NUREG/CR--4550-Vol.1-Rev.1

TI90 006253

Analysis of Core Damage Frequency: Internal Events Methodology

Manuscript Completed: December 1989
Date Published: January 1990

Prepared by
D. M. Ericson, Jr., Editor,* T. A. Wheeler, T. T. Sype, M. T. Drouin,**
W. R. Cramond, A. L. Camp, K. J. Maloney, F. T. Harper

Sandia National Laboratories
Albuquerque, NM 87185

*ERC Environmental and Energy Services Company
1717 Louisiana Boulevard, NE
Albuquerque, NM 87110

**Science Applications International Corporation
2109 Air Park Road, S.E.
Albuquerque, NM 87106

Prepared for
Division of Systems Research
Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission
Washington, DC 20555
NRC FIN A1228

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

DISCLAIMER

Portions of this document may be illegible in electronic image products. Images are produced from the best available original document.

ABSTRACT

NUREG-1150 examines the risk to the public from a selected group of nuclear power plants. This report describes the methodology that evolved as the internal event core damage frequencies for four plants were generated in support of NUREG-1150. The objective is to perform an analysis that closely approximates a state-of-the-art Level 1 Probabilistic Risk Assessment (PRA). Therefore, in principle, it is similar to those used in previous PRAs. However, this methodology, based upon previous studies and using analysts experienced in these techniques, allows the analysis to be focused upon selected areas. With this approach only the most important systems and failure modes are emphasized and modeled in detail, and the data and human reliability analyses are simplified. An analysis employing this methodology (exclusive of external reviews) can be completed in nine to twelve months using two or three full-time experienced systems analysts and part-time personnel in other areas, such as data analysis and human reliability analysis. This is significantly faster and less expensive than previous analyses, but even so, most of the insights that are obtained by the more expensive studies are still provided.

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

CONTENTS

CONTENTS (Continued)

CONTENTS (Concluded)

LIST OF FIGURES

LIST OF FIGURES (Concluded)

LIST OF TABLES

LIST OF TABLES (Continued)

LIST OF TABLES (Continued)

LIST OF TABLES (Continued)

FOREWORD

This is one of numerous documents that support the preparation of the NUREG-1150 document by the NRC Office of Nuclear Regulatory Research. Figure 1 illustrates the front-end documentation. There are three interfacing programs at Sandia National Laboratories performing this work: the Accident Sequence Evaluation Program (ASEP), the Severe Accident Risk Reduction Program (SARRP), and the Phenomenology and Risk Uncertainty Evaluation Program (PRUEP). The Zion PRA was performed at Idaho National Engineering Laboratory and Brookhaven National Laboratory.

Table 1 is a list of the original primary documentation and the corresponding revised documentation. There are several items that should be noted. First, in the original NUREG/CR-4550 report, Volume 2 was to be a summary of the internal analyses. This report was deleted. In Revision 1, Volume 2 now is the expert judgment elicitation covering all plants. Volumes 3 and 4 include external events analyses for Surry and Peach Bottom, respectively.

The revised NUREG/CR-4551 covers the analysis included in the original NUREG/CR-4551 and NUREG/CR-4700. However, it is different from NUREG/CR-4550 in that the results from the expert judgment elicitation are given in four parts to Volume 2 with each part covering one category of issues. The accident progression event trees are given in the appendices for each of the plant analyses.

Originally, NUREG/CR-4550 was published without the designation "Draft for Comment." Thus, this revision of NUREG/CR-4550 is designated Revision 1. The label Revision 1 is used consistently on all volumes except Volume 2, which was not part of the original documentation. NUREG/CR-4551 was originally published as a "Draft for Comment" so, in its final form, no Revision 1 designator is required to distinguish it from the previous documentatation.

There are several other reports published in association with NUREG-1150. These are:

NUREG/CR-5032, SAND87-2428, Modeling Time to Recovery and Initiating Event Frequency for Loss of Off-site Power Incidents at Nuclear Power Plants, R. L. Iman and S. C. Hora, Sandia National Laboratories, Albuquerque, NM, January 1988.

NUREG/CR-4840, SAND88-3102, Recommended Procedures for External Event Risk Analyses for NUREG-1150, M. P. Bohn and J. A. Lambright, Sandia National Laboratories, Albuquerque, NM, November 1989.

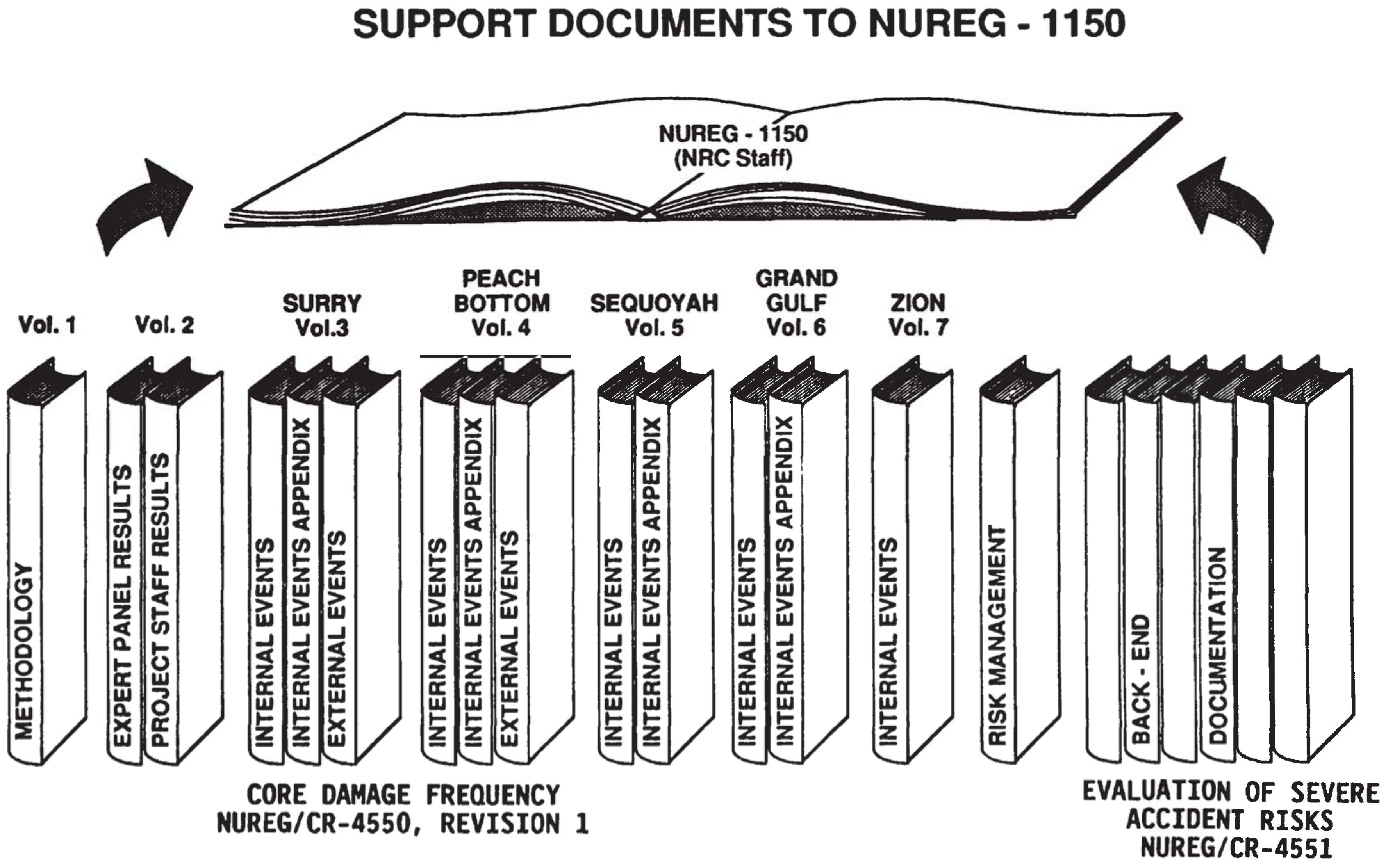


FIGURE 1. DOCUMENTATION FOR NUREG-1150.

Table 1.
NUREG-1150 Analysis Documentation

Original Documentation

NUREG/CR-4550
Analysis of Core Damage Frequency From Internal Events

Volume	1	Methodology
	2	Summary (Not Published)
	3	Surry Unit 1
	4	Peach Bottom Unit 2
	5	Sequoyah Unit 1
	6	Grand Gulf Unit 1
	7	Zion Unit 1

NUREG/CR-4551
Evaluation of Severe Accident Risks and the Potential for Risk Reduction

Volume	1	Surry Unit 1
	2	Sequoyah Unit 1
	3	Peach Bottom Unit 2
	4	Grand Gulf Unit 1
	5	Zion Unit 1

NUREG/CR-4700
Containment Event Analysis for Potential Severe Accidents

Volume	1	Surry Unit 1
	2	Sequoyah Unit 1
	3	Peach Bottom Unit 2
	4	Grand Gulf Unit 1

Revised Documentation

NUREG/CR-4550, Revision 1
Analysis of Core Damage Frequency

Volume	1		Methodology
	2	Part 1	Expert Judgment Elicit. Expert Panel
		Part 2	Expert Judgment Elicit.--Project Staff
	3	Part 1	Surry Unit 1 Internal Events
		Part 2	Surry Unit 1 Internal Events App.
		Part 3	Surry Unit 1 External Events
	4	Part 1	Peach Bottom Unit 2 Internal Events
		Part 2	Peach Bottom Unit 2 Internal Events App.
		Part 3	Peach Bottom Unit 2 External Events
	5	Part 1	Sequoyah Unit 1 Internal Events
		Part 2	Sequoyah Unit 1 Internal Events App.
	6	Part 1	Grand Gulf Unit 1 Internal Events
		Part 2	Grand Gulf Unit 1 Internal Events App.
	7		Zion Unit 1 Internal Events

NUREG/CR-4551, Evaluation of Severe Accident Risks

Volume	1		Methodology
	2	Part 1	Expert Judgment Elicit.--In-vessel
		Part 2	Expert Judgment Elicit.--Containment
		Part 3	Expert Judgment Elicit.--Structural
		Part 4	Expert Judgment Elicit.--Source-Term
		Part 5	Expert Judgment Elicit.--Supp. Calc.
		Part 6	Expert Judgment Elicit.--Proj. Staff
		Part 7	Expert Judgment Elicit.--Supp. Calc.
		Part 8	Expert Judgment Elicit.--MACCS Input
	3	Part 1	Surry Unit 1 Anal. and Results
		Part 2	Surry Unit 1 Appendices
	4	Part 1	Peach Bottom Unit 2 Anal. and Results
		Part 2	Peach Bottom Unit 2 Appendices
	5	Part 1	Sequoyah Unit 2 Anal. and Results
		Part 2	Sequoyah Unit 2 Appendices
	6	Part 1	Grand Gulf Unit 1 Anal. and Results
		Part 2	Grand Gulf Unit 1 Appendices
	7	Part 1	Zion Unit 1 Anal. and Results
		Part 2	Zion Unit 1 Appendices

NUREG/CR-4772, SAND86-1996, Accident Sequence Evaluation Program Human Reliability Analysis Procedure, A. D. Swain III, Sandia National Laboratories, Albuquerque, NM, February 1987.

NUREG/CR-5263, SAND88-3100, The Risk Management Implications of NUREG-1150 Methods and Results, A. C. Camp et al., Sandia National Laboratories, Albuquerque, NM, December 1988.

A Human Reliability Analysis for the ATWS Accident Sequence with MSIV Closure at the Peach Bottom Atomic Power Station, A-3272, W. J. Luckas, Jr. et al., Brookhaven National Laboratory, Upton, NY, 1986.

Any related supporting documents to the back-end NUREG/CR-4551 analyses are delineated in NUREG/CR-4551. A complete list of the revised NUREG/CR-4550, Revision 1 volumes and parts is given below.

General

NUREG/CR-4550, Volume 1, Revision 1, SAND86-2084, Analysis of Core Damage Frequency: Methodology Guidelines for Internal Events.

NUREG/CR-4550, Volume 2, SAND86-2084, Analysis of Core Damage Frequency from Internal Events: Expert Judgment Elicitation.

Surry

NUREG/CR-4550, Volume 3, Revision 1, Part 1, SAND86-2084, Analysis of Core Damage Frequency: Surry Unit 1 Internal Events.

NUREG/CR-4550, Volume 3, Revision 1, Part 2, SAND86-2084, Analysis of Core Damage Frequency: Surry Unit 1 Internal Events Appendices.

NUREG/CR-4550, Volume 3, Revision 1, Part 3, SAND86-2084, Analysis of Core Damage Frequency: Surry Unit 1 External Events.

Peach Bottom

NUREG/CR-4697, EGG-2464, Containment Venting Analysis for the Peach Bottom Atomic Power Station, D. J. Hansen et al., Idaho National Engineering Laboratory (EG&G Idaho, Inc.) February 1987.

NUREG/CR-4550, Volume 4, Revision 1, Part 1, SAND86-2084, Analysis of Core Damage Frequency: Peach Bottom Unit 2 Internal Events.

NUREG/CR-4550, Volume 4, Revision 1, Part 2, SAND86-2084, Analysis of Core Damage Frequency: Peach Bottom Unit 2 Internal Events Appendices.

NUREG/CR-4550, Volume 4, Revision 1, Part 3, SAND86-2084, Analysis of Core Damage Frequency: Peach Bottom Unit 2 External Events.

Sequoyah

NUREG/CR-4550, Volume 5, Revision 1, Part 1, SAND86-2084, Analysis of Core Damage Frequency: Sequoyah Unit 1 Internal Events.

NUREG/CR-4550, Volume 5, Revision 1, Part 2, SAND86-2084, Analysis of Core Damage Frequency: Sequoyah Unit 1 Internal Events Appendices.

Grand Gulf

NUREG/CR-4550, Volume 6, Revision 1, Part 1, SAND86-2084, Analysis of Core Damage Frequency: Grand Gulf Unit 1 Internal Events.

NUREG/CR-4550, Volume 6, Revision 1, Part 2, SAND86-2084, Analysis of Core Damage Frequency: Grand Gulf Unit 1 Internal Events Appendices.

Zion

NUREG/CR-4550, Volume 7, Revision 1, EGG-2554, Analysis of Core Damage Frequency: Zion Unit 1 Internal Events.

Acronyms and Initialisms

A	Large LOCA
AC	Alternating Current
ACC	Accumulators
ACT	Actuation
ADS	Automatic Depressurization System
AFW	Auxiliary Feedwater
AIS	Alternate Injection System
APB	Accident Progression Bin
APET	Accident Progression Event Tree
ARI	Alternate Rod Insertion
ASEP	Accident Sequence Evaluation Program
ATWS	Anticipated Transient Without Scram
BCD	Battelle Columbus Division
B&W	Babcock and Wilcox
BOP	Balance of Plant
BWR	Boiling Water Reactor
CCW	Component Cooling Water
CD	Core Damage
CE	Combustion Engineering
COP	Containment Overpressure Protection
CRD	Control Rod Drive
CS(S)	Containment Spray (System)
CSI(S)	Containment Spray Injection (System)
CSR(S)	Containment Spray Recirculation (System)
CST	Condensate Storage Tank
CtF	Containment Failure

Acronyms and Initialisms (Continued)

CtV	Containment Vulnerable
CtVt	Containment Vented
CV	Core Vulnerable
CVCS	Chemical and Volume Control System
DC	Direct Current
DEP	Depressurization
DG	Diesel Generator
EBS	Emergency Boron System
ECCS	Emergency Core Cooling System
EFW	Emergency Feedwater
EHC	Electric Hydraulic Control
EI	Energy Incorporated
ECOM	Errors of Commission
EOM	Errors of Omission
EOP	Emergency Operating Procedures
EP	Electric Power
EPG	Emergency Procedure Guidelines
EPRI	Electric Power Research Institute
ESF	Emergency Safeguard Features
ESW	Emergency Service Water
EVS	Emergency Ventilation System
EWD	Elementary Wiring Diagrams
FMEA	Failure Modes and Effects Analysis
FRA	Future Resources Associates
FSAR	Final Safety Analysis Report
F&B	Feed and Bleed

Acronyms and Initialisms (Continued)

FW	Feedwater
HEP	Human Error Probability
HPCI	High Pressure Coolant Injection
HPCS	High Pressure Core Spray
HPI(S)	High Pressure Injection (System)
HPIN	High Pressure Injection
HPR(S)	High Pressure Recirculation (System)
HPSW	High Pressure Service Water
HRA	Human Reliability Analysis
HtX	Heat Exchanger
HVAC	Heating Ventilation and Air Conditioning
IA	Instrument Air
ICS	Ice Condenser System
IE	Initiating Event
IEF	Initiating Event Frequency
INEL	Idaho National Engineering Laboratory
INPO	Institute for Nuclear Power Operation
INJ	Injection
IORV	Inadvertent Open Relief Valve
IPRDS	In-Plant Reliability Data System
IREP	Interim Reliability Evaluation Program
ISR	Inside Spray Recirculation
LER	Licensee Event Report
LOCA	Loss of Coolant Accident
LOSP	Loss of Offsite Power
LPCI	Low Pressure Coolant Injection

Acronyms and Initialisms (Continued)

LPCS	Low Pressure Core Spray
LPI(S)	Low Pressure Injection (System)
LPIN	Low Pressure Injection
LPR(S)	Low Pressure Recirculation (System)
LWR	Light Water Reactor
MCC	Motor Control Center
MFW	Main Feedwater
MOV	Motor-Operated Valve
MSIV	Main Steam Isolation Valve
MTC	Main Temperature Coefficient
NPRDS	Nuclear Plant Reliability Data System
NPSH	Net Positive Suction Head
NRC	Nuclear Regulatory Commission
NSSS	Nuclear Steam Supply System
NUS	NUS Corporation
OSR	Outside Spray Recirculation
P&ID	Piping and Instrumentation Diagrams
PCS	Power Conversion System
PL&G	Pickard, Lowe and Garrick
PORV	Power Operated Relief Valve
PRA	Probabilistic Risk Assessment
PRUEP	PRA Uncertainties Estimation Program
PWR	Pressurized Water Reactor
QCG	Quality Control Group
RCIC	Reactor Core Isolation Cooling
RCP	Reactor Coolant Pump

Acronyms and Initialisms (Continued)

RCS	Reactor Coolant System
RF	Recovery Factor
RHR	Residual Heat Removal
RMIEP	Risk Methods Integration and Evaluation Program
ROD1	Early manual rod insertion
ROD2	Late manual rod insertion
RPS	Reactor Protection System
RPSE	Reactor Protection System Electrical Failure
RPSM	Reactor Protection System Mechanical Failure
RPT	Recirculation Pump Trip
RSSMAP	Reactor Safety Study Methodology Application Program
RWST	Reactor Water Storage Tank
Rx	Reactor
SAIC	Science Applications International Corporation
SAROS	Safety and Reliability Optimization Services, Inc.
SARRP	Severe Accident Risk Reduction Program
SBO	Station Blackout
SCRM	Manual scram of reactor
SCG	Senior Consultant Group
SDG	Shutdown Cooling
SG	Steam Generator
SGTR	Steam Generator Tube Rupture
SNL	Sandia National Laboratories, Albuquerque
SLC	Standby Liquid Control
SLC1	Standby Liquid Control one pump

Acronyms and Initialisms (Continued)

SLC2	Standby Liquid Control two pumps
SLCD	Standby Liquid Control
SPC	Suppression Pool Cooling
SPMU	Suppression Pool Makeup
SRV	Safety Relief Valve
SSW	Standby Service Water
SW(S)	Service Water
SSW X-tie	Standby Service Water Cross-tie
S1	Intermediate LOCA
S2	Small LOCA
S3	Small small LOCA
T	Transient
T1	LOSP Transient
T2	Transient with loss of PCS
T2A	Transient with loss of PCS and feedwater
T2B	Transient caused by IORV
T3	Transient with PCS available
TAC	Transient caused by loss of AC vital bus
TAF	Top of Active Fuel
TDC	Transient caused by loss of DC vital bus
TMI	Three Mile Island
TS	Technical Specification
TT	Turbine Trip
UHI	Upper Head Injection
VSS	Vapor Suppression System

ACKNOWLDGEMENTS

The authors wish to acknowledge the efforts of the other analysis teamleaders, specifically Mr. Alan Kolaczkowski of SAIC and Mr. Robert Bertucio of EI and their analysis teams. Persons not listed explicitly in the report but whose efforts should be noted include Emily Preston of SNL who typed the report, and Nancy Cabber of SAIC who provided the graphics.

EXECUTIVE SUMMARY

NUREG-1150 examines the risk to the public from a selected group of nuclear power plants. In order to provide a consistent set of results and insights, a methodology for estimating the core damage frequency from internal events* was developed. This methodology, the objective of which is to produce an analysis that closely approximates a state-of-the-art Level 1 Probabilistic Risk Assessment (PRA), is known as the Accident Sequence Evaluation Program (ASEP) methodology. In principle, its methods are similar to those used in previous PRAs; however, the ASEP methodology is a focused approach using experienced analysts; it concentrates resources in areas important to risk and uses simplified techniques in other areas. It may be observed that the NUREG-1150 studies do not all follow this methodology precisely.** There are minor exceptions or differences which arise because the studies were done by independent teams and the plants are inherently different. Nevertheless, the methodology described here reflects the best judgment of the participants.

The following characteristics allow this methodology to be useful in a variety of ways:

- Its suitability to the regulatory process. There is sufficient detail in its information base, analytical methods, assumptions, uncertainties, and results for it to be readily understandable.

- Its detail, which is sufficient so that small teams of personnel with a firm grasp of engineering principles, PRA methods, and the design and operation of nuclear power plants can apply its methods.

- Its ability to identify, where appropriate, major assumptions and simplifications and describe their limitations, advantages and disadvantages.

The methodology does not attempt to model different plants and systems at the same level of detail. Rather, the level of detail and approach is established on a plant and system-specific basis. Thus, resources can be concentrated on those issues known, or expected, to be the most important.

In order to approximate a detailed Level 1 PRA, the methodology provides several specific types of analytic results. These results include:

* Internal events are defined here as those events that occur within the plant (except for fires and internal floods) plus the loss of offsite power as an initiating event.

** In particular, analysis of the Zion Unit 1 nuclear power plant did not use the methodology in this volume (see NUREG-1150 Appendix A; or NUREG/CR-4550, Volume 7, Revision 1).

- A realistic estimate of the core damage frequency and its uncertainty;

- Identification of the dominant accident sequences and their frequencies;

- Identification of the dominant plant damage states and their frequencies;

- Characterization of the important uncertainties and sensitivities;

- Identification, in the form of sequence cut sets, of those plant features (e.g., hardware failures, human errors) that are the most important to the likelihood of core damage; and

- Documented plant models for future use in analyzing particular issues as they pertain to the plant analyzed.

To meet the stated objectives, certain tasks have been identified and specific methods developed to accomplish them. The tasks included in the methodology are described below.

1. Plant Familiarization Analysis. The first task in the analysis is to develop familiarity with the plant. This is the foundation for all subsequent tasks. Information is assembled from past studies and the Final Safety Analysis Report (FSAR) to develop an initial set of event trees, fault trees, questions, and requests for information before a visit to the plant. After the plant visit, the majority of the information required is in hand and the team is knowledgeable about the design and operation of the plant. Regular contact is maintained with the plant staff throughout the study to ensure that current data and information are used.

2. Accident Sequence Initiating Event Analysis. The next step is to identify those potential accident initiating events that lead to a need for subcriticality and removal of decay heat. This analysis involves a number of steps. First, the accident initiating events [e.g., Loss of Offsite Power (LOSP)] are identified, including any that may be unique to the plant under study. Then the safety functions that are necessary to prevent core damage (e.g., remove decay heat) are defined. Based upon these initiating events and functions, the safety systems that must operate to perform the functions are identified, along with any support systems that are needed, such as service water or electric power. For each of these systems, success criteria are defined, for example, how many pumps must operate and when, so that the safety function is performed. Finally, the initiating events are combined into groups based upon the similarity of the system responses required.

3. Accident Sequence Event Tree Analysis. Accident sequence event trees are constructed for each initiating event group. The event tree structure describes the combination of system successes and failures that can result in core damage. This structure reflects system interrelationships and those aspects of accident phenomenology that can affect system success, and uses information developed in Task 2. The task also requires interface with analysts conducting the accident progression analyses (see Task 9).

4. Systems Analysis. To estimate the sequence frequencies, the success or failure probability of each event on the event tree must be established. Thus, the important contributors to failure of each system are identified by the use of system fault trees that logically represent the ways in which the undesired event (system failure) may occur. Initially fault trees are developed for all of the front-line systems. If a front-line system has support system dependencies (e.g., electric power, service water), models are developed for the support systems and integrated with the front-line system models. The Boolean solution of the fault trees defines the combinations of events that can lead to system failure.

   This task interfaces with the human reliability, dependent failure and data base analyses. Human errors associated with test and maintenance activities and certain responses to accident situations are modeled directly in the fault trees. Dependent failures arising from system interdependencies and component common cause failures are also directly modeled.

5. Dependent and Subtle Failure Analysis. Nuclear power plants are sufficiently complex that dependent failures, often very subtle in nature, can be of primary importance in determining the core damage frequency. Potential failures that are buried in the depths of the design and operation of the plant are often not easily discerned. Two different types of failures may be characterized as dependent failures. First, there are explicit functional and support system dependencies that are identified and modeled in the event trees and fault trees. This group includes the dependence of front-line systems on electric power and cooling water. This group is identified through examination of design documentation. Second, there are those types of dependent failures that have been observed previously, but which cannot be explicitly modeled, i.e., simultaneous failures from a single cause common to all of them, some of which are due to very subtle design interactions or due to the manufacturing processes, and which may require very diverse methods to identify them. A common cause event that accounts for these types of failures is added to the fault trees where appropriate.

6. Human Reliability Analysis. This analysis involves the analysis of two types of failures: pre-accident errors, including miscalibration of instrumentation and failure to restore

equipment after test or maintenance; and post accident errors, including failure to diagnose and respond appropriately to accidents. For pre-accident faults, calibration, test, and maintenance procedures and practices are reviewed for all systems. This review identifies critical instrumentation whose miscalibration could prevent system function and identifies components that could be removed from service and erroneously left in an inoperable state. For post-accident faults, emergency response procedures are reviewed for possible sources of human error that could affect the system operability. Based on these reviews, probabilities for human errors are estimated with conservative screening values being used initially. For human errors with significant impact on the core damage frequency, more realistic error rates are generated.

7. Data Base Analysis. A generic data base representing typical failure rates and their uncertainties for plant components was developed for ASEP. Because experience for the plant under study may differ significantly from the generic base, the operating history of the plant is reviewed for plant-specific failure information. Test and maintenance procedures, practices, and experience are also reviewed to establish their frequency and duration. The plant-specific information is used to supplement the generic base.

8. Accident Sequence Quantification Analysis. The models from the preceding tasks are integrated in this task to calculate point estimates of the sequence frequencies. This is an iterative process of quantification and analysis. After each quantification pass, the logic is reviewed for consistency and trends. Sequences with very low frequency are eliminated from further consideration. In general, the process proceeds as follows. First, computer input representing the logic of the system analysis fault trees is prepared, and the trees are reviewed and any logic errors corrected. Next, failure probabilities from the data base are assigned to each basic event. Fault trees representing the required support systems are combined with the safety system trees, and Boolean logic expressions for the fault trees are generated. Combinations of these Boolean expressions prescribed by the Accident Sequence Event Trees are then solved to create accident sequence expressions showing the combinations of events (i.e., cut sets) that can lead to system failure and core damage. Point estimates of the frequency of each sequence are also provided.

9. Plant Damage State Analysis. The plant damage state analysis defines the status of plant systems at the onset of core damage. These definitions include descriptions of the status of core cooling systems, containment systems, and support systems in sufficient detail to describe the state of the plant for the subsequent accident progression analysis. The plant damage states are established effectively by adding questions to the end of the accident sequence event trees. These questions are

developed through an iterative process with the accident progression analysts. In this process the accident sequence cut sets are regrouped into plant damage states, based upon the particular failures in the cut sets and answers to the selected questions. Any one accident sequence may contribute to several plant damage states, i.e., all the individual cut sets do not lead to the same plant damage state. Similarly, several accident sequences may contribute cut sets into a single damage state. However, each individual cut set is assigned to only one plant damage state. These plant damage states are quantified in the same manner as the accident sequences.

10. Uncertainty Analysis. The uncertainty analysis is accomplished using a statistical sampling approach. In the NUREG-1150 studies, a Latin Hypercube Sampling with restricted pairing was used. Values are taken from the probability distributions for the events in the Boolean logic model and combined to provide estimates of the core damage frequency. The values of the core damage frequency produced by the sampling process yield a distribution that describes the uncertainty in the frequency. This task produces the majority of the important final results, including: (1) mean, median, and other quantile values for the accident sequence and plant damage state frequencies, (2) estimates of the uncertainty in the frequencies, and (3) identification of the events driving both the magnitude of the results and the uncertainty. Both parameter value (data) and modeling uncertainties are included in the analysis.

11. Expert Judgment

    Although it is not considered to be a separate analysis task, the use of expert judgment elicitation is an integral part of the methodology to produce the PRAs in support of NUREG-1150. Expert judgment in some form is used where applicable experimental data or complete analyses are not available. The expert judgment process can address complex issues such as the behavior of components in extreme environments, or it may be used to resolve more general issues common in PRA, such as how to include operator recovery actions in the accident sequence models. It was used in both ways in these studies in the systems and data base analyses, and in the quantification of uncertainty.

12. Reporting Requirements. A significant key to success of any analysis is adequate reporting. The ASEP methodology establishes the following guidelines.

    - The dominant sequences and plant damage states are clearly identified along with the dominant contributors to each;

    - The dominant cut sets are available to reviewers;

    - Significant uncertainties and sensitivities are included;

- Events and sequences that are screened out are discussed as well as the dominant sequences;
- Any deviations from the standard methodology are clearly identified;
- Important assumptions and limitations are identified;
- The steps in the analysis are traceable and reproducible by an experienced PRA analyst.

1. INTRODUCTION

The United States Nuclear Regulatory Commission (NRC) has prepared NUREG-1150[1] to examine the risk from a selected group of nuclear power plants. In support of NUREG-1150 and as part of the Accident Sequence Evaluation Program (ASEP), Sandia National Laboratories (SNL) and its subcontractors have developed the methodology for, and produced Level 1 Probabilistic Risk Assessments (PRAs) of, the Surry, Sequoyah, Peach Bottom, and Grand Gulf nuclear power plants.[2,3,4,5] Idaho National Laboratory has developed the methodology and produced the Level 1 PRA used for the fifth plant, Zion. This report presents the methodology used for the internal events* analyses of four of the five plants analyzed.** This document serves two purposes: (1) to present the methodology used to perform four of the PRAs, and (2) to provide guidelines to analysts for the analyses of other plants. A compatible approach for analyzing external initiators is described in Reference 6. It should be noted that these four studies do not all follow this methodology precisely. There are some minor differences and exceptions which arise because the studies were done in parallel by independent teams, and the plants are inherently different. Nevertheless, this methodology reflects the best judgment of the participants as to an effective way to conduct such a study.

In previous studies such as the Interim Reliability Evaluation Program (IREP),[7] a detailed Level 1 PRA (based on internal initiators only) required a team of eight to ten individuals with various skills. Such a team can complete its work in approximately 17 months. For the NUREG-1150 work, an efficient, cost-effective approach was desired. Therefore, PRA methods were developed to produce results that closely approximate detailed Level 1 PRA results. These methods are flexible and allow for the level of detail to be determined on a plant- and system-specific basis. A team consisting of two to three experienced systems analysts and part-time data, human reliability, and computer analysts can perform a PRA and prepare a draft report in 9 to 12 months, depending on the availability of information from previous studies, the experience of the team, the complexity of the plant systems, and the degree of utility support. The manpower expenditure for each plant analysis was about 30 to 40 staff-months. Subsequent reviews and iterations will add to the resource requirements.

The four studies addressed in this document will be referred to as the NUREG-1150, or NUREG/CR-4550 analyses for the remainder of this document. The Peach Bottom analysis is used to provide examples, although examples are also taken from the other analyses, where appropriate.

* Internal events are defined here as those events that occur within the plant (except for fires and internal floods) plus the loss of offsite power as an initiating event.

** See NUREG-1150 Appendix A (or NUREG/CR-4550, Volume 7, Revision 1) for a description of the methodology used for Zion Unit 1.

1.1 Objectives and Scope of ASEP Methodology

The objective of an analysis using the ASEP methodology is to produce results approximating those obtained from a detailed state-of-the-art Level 1 PRA. The following characteristics allow this methodology to be useful to both regulators and industry. The methodology is:

- Suitable for use in the regulatory process because it contains sufficient detail in its information base, analytical methods, assumptions, uncertainties, and results to be readily understandable;
- Sufficiently detailed so that small teams of personnel with a firm grasp of engineering principles, of PRA methods, and of the design and operation of nuclear power plants can apply the methods;
- Able, where appropriate, to identify major assumptions and simplifications and describe their limitations, advantages, and disadvantages.

Note that it is not a goal of this methodology to model different systems at a consistent level of detail. Rather, the level of detail and approach is established on a system-specific basis. Thus, resources can be concentrated on those issues assessed to be the most important.

To adequately approximate a detailed Level 1 PRA, the methodology should provide several specific types of analytic results as part of its scope, including:

- A realistic distribution for the core damage frequency;
- Identification of the dominant accident sequences and their frequencies;
- Identification of the dominant plant damage states and their frequencies;
- Characterization of the important uncertainties and sensitivities;
- Identification of those plant features (e.g., hardware failures, human errors, etc.) that are the most important to the likelihood of core damage; and
- Documentation of the plant models for future use in analyzing particular issues as they pertain to the plant analyzed.

The necessary tasks for completing the ASEP PRAs are summarized in Figure 1.1-1. This illustrates the general flow of the analyses but not all the iterative interactions. Each task is discussed in more detail in

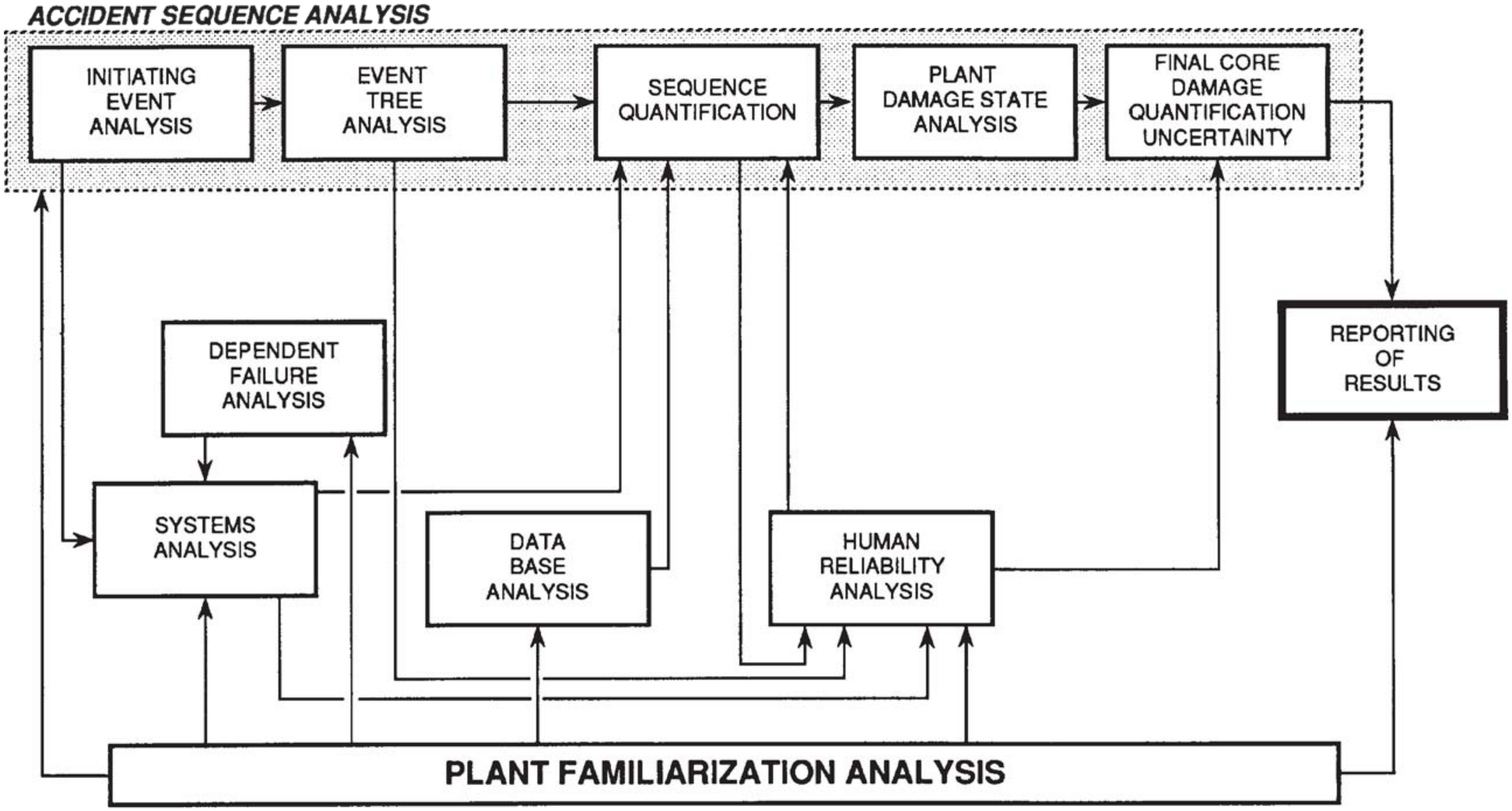

ACCIDENT SEQUENCE ANALYSIS
INITIATING EVENT ANALYSIS
EVENT TREE ANALYSIS
SEQUENCE QUANTIFICATION
PLANT DAMAGE STATE ANALYSIS
FINAL CORE DAMAGE QUANTIFICATION UNCERTAINTY
REPORTING OF RESULTS
DEPENDENT FAILURE ANALYSIS
SYSTEMS ANALYSIS
DATA BASE ANALYSIS
HUMAN RELIABILITY ANALYSIS
PLANT FAMILIARIZATION ANALYSIS

Figure 1.1-1. ASEP Task Flow Diagram.

later sections. The effort required for individual tasks varies significantly from plant to plant. Generally, the results from each task are intended to be as realistic as possible. Methods known to be conservative are not used unless they have minimal impact on the overall result. Where significant questions remain regarding the methods and subsequent results, they can be examined using uncertainty and sensitivity analysis techniques. A comprehensive uncertainty analysis that treats both parameter value and modeling uncertainties is an important part of any Level 1 PRA.

The insights from each NUREG/CR-4550 analysis are similar, and in many areas superior, to those of the IREP PRAs. While some plant-specific subtle interactions may be missing, the vast majority of the dominant contributors to the internal event core damage frequency are identified.

It is important to note that all of these simplified PRA techniques are based on experience, that is, insights gained from previous PRA studies and from PRA specialists. This approach should not be applied by analysts unfamiliar with PRAs.

1.2 Summary of ASEP Methodology

The ASEP methodology consists of 10 major tasks or analyses. These are illustrated in Figure 1.1-1. This section briefly discusses each major task and the interrelationships among the tasks. Also, the level of detail for each task is discussed. More detailed information and procedures for conducting each task are presented in the remainder of the report.

As stated in Section 1.1, the objective of the NUREG/CR-4550 analyses is to perform PRAs that are as near to the state of the art as practical. In a few cases, advances in the state of the art were required in order to complete NUREG-1150. To give the reader an idea of the level of detail of the work, explanations of what is done in the analysis are given. To simplify things, the level of detail for each task is described as: (1) an advance in state of the art, (2) state of the art, (3) slightly abbreviated, (4) abbreviated, or (5) not included. In general, a "state-of-the-art" PRA is defined as one typical of the mid-1980s, when most of this work was being performed. While it is recognized that a number of advances in PRA methods (e.g., external event modeling, common cause modeling) are being pursued under both industry and government sponsorship, these have not been assembled into a single, unified methodology for PRA. The NRC-sponsored LaSalle PRA (now scheduled for publication in 1990) will represent the most significant advance in this regard. In fact, some aspects of that methodology were employed in the NUREG/CR-4550 analyses. Nevertheless, some methods, even though they are developed and have had limited application, are considered to extend the state of the art if they are not in widespread use. Such an approach does, admittedly, involve subjective judgment, but even so, it provides a readily understood frame of reference within which the ASEP methodology may be discussed.

1.2.1 Plant Familiarization Analysis

The initial task of an ASEP analysis is to develop familiarity with the plant. This task forms the foundation for the development of plant models in subsequent tasks. Information is assembled from past studies and the Final Safety Analysis Report (FSAR) to develop an initial set of event trees, fault trees, questions, and requests for, information from plant personnel. This information gathering process takes one month and precedes an initial plant visit. One week is then spent at the plant gathering detailed information first hand. Regular contact with the plant staff is maintained throughout the course of the study. The level of detail in this task is state of the art.

At the conclusion of the initial plant visit, the majority of the information required to perform the remaining tasks has been collected and discussed in some detail with utility personnel such that the analysis team is knowledgeable about the design and operation of the plant. Subsequent communications with plant personnel are used to verify the information obtained and to identify plant changes that occur during the analysis.

1.2.2 Accident Sequence Initiating Event Analysis

The next task is to identify potentially important initiating events and the plant systems required to respond to these events. Initiating events of importance are generally those that lead to a need for subcriticality and removal of decay heat by plant safety systems. This analysis includes several steps:

- Identifying initiating events to be included in the analysis, including unusual or unique events that may affect the specific plant;

- Identifying functions that need to be performed to successfully prevent core damage;

- Identifying the front-line systems performing the above functions;

- Delineating success criteria for each front-line system responding to each initiating event; and

- Grouping initiating events, based on similarity of system response.

The level of detail in this task is state of the art. At the conclusion of this task, the number and type of event trees to be constructed and the systems to be modeled are identified. Thus, the scope of the modeling effort in subsequent tasks is clearly defined.

1.2.3 Accident Sequence Event Tree Analysis

In this task, accident sequences leading to core damage are defined by constructing event trees for each initiating event group. Generally, separate event trees are constructed for each group.

Event trees are constructed which include the systems responding to each initiating event group as defined in the Accident Sequence Initiating Event Analysis. The event tree structure reflects system interrelationships and aspects of accident phenomenology that determine whether or not the sequences lead to core damage. If a full Level 3 PRA is being conducted, the back-end analysts supply some of the phenomenological information necessary to construct these trees. If only a Level 1 PRA is being generated, then those analysts must develop the phenomenological information.

The level of detail in this task is advanced over the state of the art typically seen in Level 1 PRAs. At the conclusion of this task, models have been constructed which identify all of the sequences to be assessed in the Accident Sequence Quantification Analysis task.

1.2.4 Systems Analysis

In order to estimate the sequence frequencies, the success and failure probabilities must be determined for each question on the event trees. Thus, the important contributors to failure of each system must be identified and quantified. The models to facilitate this quantification are system fault trees. A fault tree represents ways in which a certain undesired event may occur. Fault trees are constructed that reflect the success criteria identified and refined in the three previous tasks. Each success criterion is transformed into a failure criterion that is the top event for a given fault tree. Initially, fault trees are developed for all of the front-line systems included in the event trees. If these front-line systems depend on support systems, such as electric power or service water, then models are also developed for those systems. In a subsequent task, the support system trees are combined with the respective front-line system fault trees to describe the ways, including support system faults, that the undesired event may occur. Thus, support system dependencies are an integral part of the models and the quantification process.

This task interfaces with the human reliability, dependent and subtle failure, and data base analyses. Human errors associated with test and maintenance activities and certain responses to accident situations are modeled directly in the fault trees. Dependent and subtle failures as a result of system interdependencies and component common cause failures are also directly modeled. The fault trees are developed to a level of detail consistent with the data base utilized for quantifying failure probabilities.

The level of detail in this task ranges from state of the art to abbreviated, depending on the system being modeled. In a state-of-the-art systems analysis, each system is modeled in detail, and all failure modes and components are examined. Selection of the level of modeling detail for each system is one of the most important steps in the analysis, and will, to a great extent, determine the amount of effort required to complete the Level 1 PRA. The majority of the models in the methodology are detailed fault trees, supplemented with a few simplified fault trees, Boolean equations, or black box models (event probabilities or failure rates), as appropriate. Selection of the level of detail is guided by consideration of such things as the relative importance of the system, complexity of the system, dominant failure modes, and availability of data. Most of the front-line fluid systems will be modeled with detailed fault trees, as will all critical support systems. The outputs of this task are models for each question found in the event trees.

1.2.5 Dependent and Subtle Failure Analysis

Nuclear power plants are sufficiently complex that dependent and subtle failures may be very important to the core damage frequency. Failures that are buried in the depths of the design and operation of the plant are not easily identifiable. Dependent and subtle failures are categorized separately because they are very distinct types of failures.

The dependent failures include:

- Explicit functional dependencies which involve initiators, support systems, and shared equipment; and

- Common cause faults involving simultaneous failure or unavailability of components or systems.

The subtle failures include:

- Peculiar or unusual interactions of system design and interfaces, or system component operation; and

- Subtle interactions identified in previous studies and PRAs or by PRA experts.

The dependent failures are identified in the analysis process. When the subtle failures are identified, they are added to the sequence event trees or fault trees, as appropriate. In rare cases, such events may be modeled by changes to failure data or the cut set expressions. The level of detail in this task ranges from slightly abbreviated to state of the art. A significant effort is made to identify, model, and quantify dependent failures.

At the conclusion of this task, the above dependencies have been identified and modeled.

1.2.6 Human Reliability Analysis

This task involves the analysis of two types of potential human errors: (1) pre-accident errors, including failure to restore equipment to operability following test and maintenance, and (2) post-accident errors, including failure to diagnose and respond appropriately to accidents. In the evaluation of pre-accident faults, calibration, test, and maintenance procedures and practices are reviewed for each front-line and support system. The evaluation includes identifying: (1) sensors that require calibration and if miscalibration precludes system operation or prevents the operator from diagnosing system condition, and (2) systems and components removed from service during test or maintenance but which could erroneously be left in an inoperable state. The human error rates are quantified based upon the Accident Sequence Evaluation Program Human Reliability Analysis Procedure.[35]

For post-accident faults, procedures to be followed in response to accidents modeled in the event trees are identified and reviewed for possible sources of human errors that could affect the operability or function of systems for the accident sequences. In order to support eventual sequence quantification, human error rates are estimated. Screening values are used for initial calculations. For human errors found to be significant in the screening analysis, nominal human error probabilities are evaluated, reflecting plant-specific characteristics.

The level of detail in this task (both pre- and post-accident) ranges from state of the art to abbreviated. For the boiling water reactor (BWR) plants in NUREG-1150, the situation was such that a detailed Human Reliability Analysis (HRA) was performed on the post accident human faults for the Anticipated Transient Without Scram (ATWS) sequences. For the other BWR sequences and for all of the sequences for the pressurized water reactors, an initial screening procedure was used for the post-accident faults. In this methodology, an HRA specialist is present during the plant visit, interviewing operators, emphasizing the sequences and procedures most important to the analysis. The screening procedure is conservative; however, any operator actions that yield high accident sequence results are identified and reconsidered in greater detail with more realistic values.

1.2.7 Data Base Analysis

This task involves the development of a data base for quantifying basic events (other than human errors) appearing in the system fault trees, and initiating events. A generic data base representing typical initiating event frequencies and component failure rates and their uncertainties was developed for ASEP. However, plant-specific data may differ significantly from industry-wide data. In this task, the operating history of the plant is reviewed to ascertain plant specific initiating event frequencies and whether any plant components have unusual failure rates. Test and maintenance practices and plant experiences are also reviewed to determine the frequency and duration of these activities. This information is used to supplement the generic data base.

The level of detail in this task is abbreviated from that normally seen for a Level 1 PRA. A data specialist is present during the plant visit and obtains plant-specific data for the components that are most important to the analysis. The analysis is abbreviated in the sense that all components are not included in the analysis and particular failures are not investigated in detail. Where plant-specific data are unavailable or inadequate, generic data are used.

1.2.8 Accident Sequence Quantification Analysis

The models from each previous task are integrated in the accident sequence quantification analysis task to calculate point estimates for the accident sequence frequencies. This is done using any one of a number of computer codes for Boolean reduction and quantification of fault trees and event trees. Quantification is a time-consuming and iterative task generally performed at various stages during the analysis. For example, the analyst will typically estimate partial sequence frequencies early in the study in order to screen out large numbers of event tree sequences and decide if certain systems do not need to be modeled. The complexity of the analysis can be reduced without losing significant sequences by careful truncation during steps in the Boolean reduction, where the size of the fault tree becomes unmanageable. Usually, probability values for sequence truncation are 1E-8 or 1E-9. As the event tree and fault tree modeling proceeds, the analyst will continue to develop the sequence quantification, while continually screening out low probability sequences. For the sequences that remain, a detailed quantification is performed in several steps:

- Prepare final computer input representing the logic of the systems analysis fault trees;

- Identify and correct errors in the fault trees;

- Assign failure probabilities to each basic event in the fault tree;

- Combine support system fault trees with the appropriate front-line system fault trees;

- Develop logic expressions and their complements, if used, for events not included on fault trees; and

- Develop accident sequence expressions with combinations of component faults or cut sets with point estimates of their probabilities.

The results of this task include computerized accident sequence models for the plant. These models describe the possible plant response to all important accident sequences. Point estimate quantification provides an initial estimate of the frequency of each important sequence. The level of detail in this task is equivalent to the state of the art for a Level 1 PRA.

1.2.9 Plant Damage State Analysis

The plant damage state analysis provides the information necessary to complete the accident progression analysis in a comprehensive Level 3

PRA. The overall Level 3 PRA structure is discussed in Section 1.4. The plant damage state definitions provide the status of plant systems at the onset of core damage. These definitions include descriptions of the status of core cooling systems, containment systems, and support systems in sufficient detail to describe the state of the plant for the accident progression analysis. The definition of the plant damage states is accomplished by adding additional questions to the end of the accident sequence event trees. However, in many cases it is not necessary to actually draw the plant damage state event tree, but rather, the questions can be dealt with in a matrix format, as discussed in Section 11.

The questions that define the plant damage states are selected during an iterative process with the accident progression analysts. During the actual analysis, the accident sequence cut sets are regrouped into plant damage states, based on the particular failures in the cut sets and the answers to the selected questions. Any particular accident sequence may contribute to several different plant damage states, i.e., all the individual cut sets do not lead to the same plant damage state. Similarly, several different accident sequences can contribute cut sets to the same plant damage state. There are also cases where a single accident sequence cut set is divided into multiple cut sets that go into different plant damage states.

Once the new plant damage state cut set groups are formed, they are quantified in the same manner as the accident sequences. Point estimates are determined, and then an uncertainty analysis is performed, as discussed below. This analysis represents an advance in the state of the art for PRAs.

1.2.10 Uncertainty Analysis

The Uncertainty Analysis task produces most of the important final results, including: (1) mean, median, and other quantile values for the individual sequence, plant damage state, and total plant core damage frequencies, (2) estimates of the uncertainty in the frequencies, and (3) identification of the events driving both the magnitude of the results and the uncertainty. Both parameter value (data) and modeling uncertainties are included in the analysis. This analysis involves several steps:

- Assign a probability distribution to each basic event in the logic models;

- Prepare an uncertainty distribution for those issues or parameters for which insufficient information is available by eliciting expert judgment;

- Determine the correlation between events in the logic models;

- Input the logic models and the probability distributions, including correlation factors, to an appropriate computer code package to perform the sampling and importance calculations; and

- Perform additional sensitivity studies on key issues.

This analysis will produce a distribution for the frequencies from which mean values and other statistical measures can be inferred. Matrix analysis techniques are used to process the results and rank the basic events according to their contribution to the core damage frequency and the uncertainty. By combining parameter value and modeling uncertainty, and using advanced techniques for eliciting expert judgment where necessary, the uncertainty analyses performed for NUREG-1150 represent a significant advancement in the state of the art over most previous Level 1 PRAs.

1.2.11 Expert Judgment

Although it is not considered to be a separate analysis task, the use of expert judgment elicitation is an integral part of the methodology to produce the PRAs in support of NUREG-1150. Expert judgment in some form is used where applicable experimental data or complete analyses are unavailable. The expert judgment process can address complex issues such as the behavior of specific components in extreme environments, or it may be used to resolve more general judgments common in PRA, such as how to include operator recovery actions in the accident sequence models. It was used in both ways in the current studies in the systems and data base analyses, and in the quantification of uncertainty.

1.2.12 Reporting Requirements

A key to the success of any analysis is the reporting of the results. PRAs are notoriously difficult to document in a form that facilitates outside review. However, we have established some guidelines to assist in the process.

- The dominant sequences and plant damage states should be clearly identified, along with the dominant contributors to each;

- The dominant cut sets should be available;

- Significant uncertainties and sensitivities should be included;

- The report should discuss the disposition of events and sequences that were screened out, as well as the dominant sequences;

- Any deviations from the standard methodology should be clearly identified;

- Experienced PRA analysts should be able to readily review and understand the results, and trace through the dominant sequences; and

- Important assumptions and limitations should be clearly identified.

It is important to recognize that documentation should be done throughout the process, rather than be deferred to the end of the analysis. Otherwise, key assumptions and subtleties of the analysis may be lost.

1.3 Analysis Limitations

In addition to the above discussions comparing this analysis to a state-of-the-art PRA, it is helpful to identify some things that PRAs do not normally treat. The following list of items not treated in NUREG-1150 or, at most, treated very simply, is taken with some modification from NUREG-1115:[9]

L Partial Failures;

L Design Adequacy;

L Construction Errors;

L Adequacy of Test and Maintenance Practices;

L Effect of Aging on Component Reliability (also burn-in phenomena);

L Adequacy of Equipment Qualification;

L Operator Errors of Commission; and

L Sabotage.

1.4 Integrated Level 3 PRA Framework

The results produced using the ASEP methodology are intended to be part of an integrated Level 3 PRA framework. This section describes how the ASEP analyses fit into that overall framework. In simple terms, the three levels of PRA can be defined as follows:

Level 1: Identification of potential core damage events and analysis of their frequency of occurrence (the ASEP methodology is used for the internal events portion of the Level 1 analysis);

Level 2: Analysis of the possible radionuclide releases (source terms) resulting from the core damage events; and

Level 3: Analysis of the health and economic consequences of radioactive releases.

The integrated PRA framework is depicted in Figure 1.4-1. The Level 1 analysis is also referred to as the front-end analysis, while Levels 2 and 3 are usually referred to as the back-end analysis. The internal event portion of the Level 1, or front-end analysis, is the focus of this report. The complete Level 3 framework includes analyses of internal and external event* frequencies, accident progression and containment response, radionuclide releases (source terms), and health and economic consequences. At each step in the process there are interactions, sometimes iterative, with one or more of the other steps. Further, all of the steps provide input to an integrated uncertainty analysis.

* External events include, for example, earthquakes, internal fires, internal and external flooding and winds.

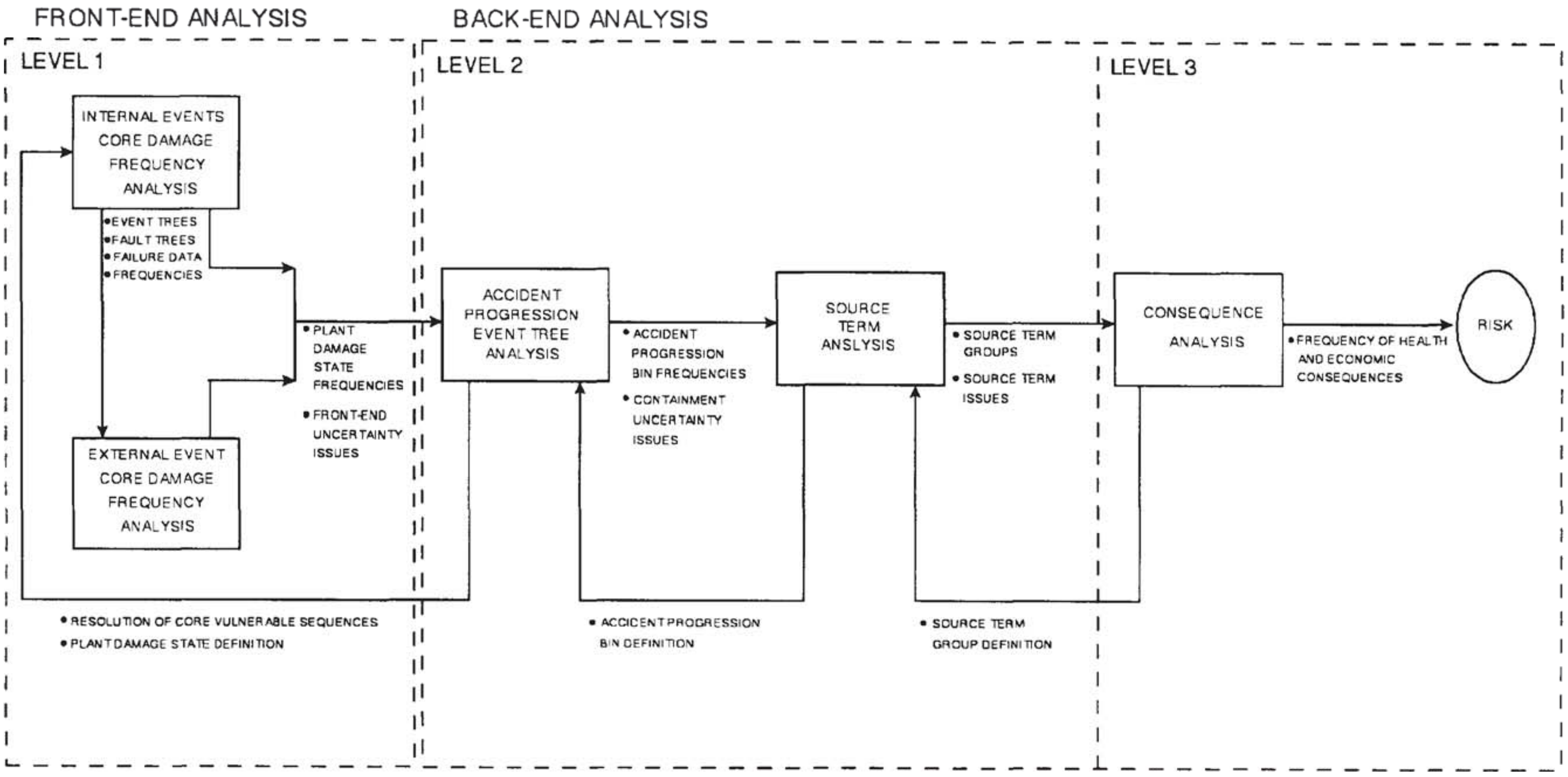

FRONT-END ANALYSIS
BACK-END ANALYSIS
LEVEL 1
LEVEL 2
LEVEL 3
INTERNAL EVENTS CORE DAMAGE FREQUENCY ANALYSIS
•EVENT TREES
•FAULT TREES
•FAILURE DATA
•FREQUENCIES
EXTERNAL EVENT CORE DAMAGE FREQUENCY ANALYSIS
• PLANT DAMAGE STATE FREQUENCIES
• FRONT-END UNCERTAINTY ISSUES
ACCIDENT PROGRESSION EVENT TREE ANALYSIS
• ACCIDENT PROGRESSION BIN FREQUENCIES
• CONTAINMENT UNCERTAINTY ISSUES
SOURCE TERM ANSLYSIS
• SOURCE TERM GROUPS
• SOURCE TERM ISSUES
CONSEQUENCE ANALYSIS
• FREQUENCY OF HEALTH AND ECONOMIC CONSEQUENCES
RISK
• RESOLUTION OF CORE VULNERABLE SEQUENCES
• PLANT DAMAGE STATE DEFINITION
• ACCICENT PROGRESSION BIN DEFINITION
• SOURCE TERM GROUP DEFINITION

Figure 1.4-1. Integrated Level 3 PRA Framework

At each major step in Figure 1.4-1, intermediate results can be produced. In general, there are a very large number of possible outcomes at each stage. Therefore, the problem is simplified by grouping the outcomes based on their similarity, and in some cases screening out outcomes of negligible probability. There are three major transition points at which groupings are made:

1. Plant Damage States. Sequence cut sets are combined into groups described by the combinations of failures that lead to core damage and result in similar reactor coolant system and containment response.

2. Accident Progression Bins. The outcomes from (or paths through) the accident progression event tree that would produce similar radionuclide source terms are grouped together.

3. Source Term Groups. Source terms that would produce similar consequences are grouped together.

There are various measures of risk that can be generated in a Level 3 PRA but, in general, risk is determined by using the following equation.

$$R_M = R_h R_i R_j R_k \; F_h \; P(PDS_{ih}) P(APB_{ji}) \; P(S_{kj}) C_{Mk} \qquad (1.1)$$

where:

R_M = risk (expected value) for risk measure M (consequence/ yr),

F_h = frequency of initiating event h,

$P(PDS_{ih})$ = probability that initiating event h leads to plant damage state i,

$P(APB_{ji})$ = probability that plant damage state i will lead to accident progression bin j,

$P(S_{kj})$ = probability that accident progression bin j will lead to source term group k,

C_{Mk} = value of consequence measure M, conditional on the occurrence of source term group k.

This section briefly discusses how the elements identified in Figure 1.4-1 provide the terms included in the above equation, with particular emphasis on the interfaces and integration needs affecting the internal event sequence frequency analysis.

The first important interface to note is the one between the internal and external events analyses. The external events analysis methods described in Reference 6 rely on the internal events analysis to provide sequence event trees, fault trees, and basic event random failure data. The external event analysts then modify these models to include the failures that result from the particular external events. Because they begin with the identical models used in the internal events analysis and include the same random failures, the internal and external results may be compared on a consistent basis. Section 5 discusses some considerations that should be addressed when preparing the plant models so that they may be used later in the external events analysis.

The internal and external sequences are evaluated separately to estimate their respective core damage frequencies and to identify the dominant contributors for each category. Both sets are essentially large Boolean expressions that can be evaluated using a sampling approach. This approach is discussed in more detail in Section 12. The results of the two uncertainty analyses include the mean value and uncertainty estimates for the total core damage frequency and for each plant damage state. Importance measures identifying the contributions of particular events are also included.

The internal and external event core damage frequency analyses represent the front-end portion of the Level 3 PRA. There are several important interfaces between the front-end analyses and the overall risk or back-end analyses (Levels 2 and 3). The back-end analysts are responsible for helping to resolve core vulnerable sequences. These are sequences where core cooling is initially successful, but containment cooling is inadequate, and eventual containment failure or venting could impact the continued success of the core cooling functions. Issues such as containment failure pressure, leak size, location of the failure, and the resulting environment outside containment are resolved by the back-end analysts.

The most important product that the front-end analysis supplies to the back-end analysis is the quantification of the plant damage state probabilities, the values for $P(PDS_{ih})$ in Equation 1. The plant damage state definitions contain information that help answer the initial questions on the accident progression event tree. These definitions deal with both systems questions (e.g., availability of containment sprays) and the phenomenological status at the time of core damage (e.g., reactor coolant system pressure). The frequency of each plant damage state is produced as part of the front-end uncertainty analysis. Plant damage states are discussed in more detail in Section 11.

The final product that the front-end analysis supplies to the back-end analysis is the set of dominant front-end random variables to be included in the overall Level 3 PRA uncertainty analysis and the probability distributions associated with those issues. Because of computing limitations and the enormous number of parameters associated with a Level 3 PRA, only the front-end issues most important to core damage frequency are selected. Other, less important, variables are fixed at their mean values for incorporation into the risk calculation. The important uncertainty issues are identified during the front-end uncertainty analysis, based on selected importance measures, as discussed in Section 12.

The plant damage states define a unique set of initial and boundary conditions to the accident progression analysis. Once these have been defined, the accident progression event tree (APET) can be constructed. The APET consists of a series of questions whose answers define the different branches of the tree. These branches determine the direction of the accident progression conditional on the answers to the previous questions. The output of the APET is grouped into accident progression bins (APBs) which define sets of unique plant state and phenomenological characteristics for the source term analysis. The APET is evaluated conditional on the plant damage state frequency. The conditional probability of each APB, $P(APB_{ji})$, is the sum of the probabilities of all the accident progression paths that lead to that bin, and the probability of each path is the product of the probabilities of all the branches determining the path. The plant damage state definitions determine the particular probability distributions used to quantify many of the branches in the initial questions on the accident progression event tree. Other questions are quantified by either assigning probability distributions to parameters (e.g., pressure, hydrogen concentration) which are then used to calculate the probabilities of the various branches of a question or the question branches are directly assigned probability distributions. These distributions are sampled at the same time as the plant damage state frequencies and other Level I variables that appear in the APET. The APET is then evaluated in a sampling mode for each plant damage state.

For each important accident progression bin, source terms, and their associated uncertainties are estimated. Source term groups are then determined for the plant damage state, and consequences for risk measure ℓ are estimated for each source term $C_{\ell k}(s)$. These risk measures can include both health effects, such as latent cancer fatalities, and economic effects, such as offsite property damage.

In order to estimate the uncertainty in risk, Equation 1.1 is solved numerous times using a sampling approach. In a complete uncertainty analysis, every important element would be assigned a probability distribution representative of its uncertainty, and all elements would be sampled over their range of probabilities. In practice, there are far too many variables for all of them to be included. Therefore, based on uncertainty and sensitivity analyses performed for each of the steps shown in Figure 1.4-1, only those parameters most important to the risk and its uncertainty are included. These parameters are sampled using stratified statistical sampling to produce an overall estimate of the uncertainty in various risk measures. The NUREG-1150 studies used Latin Hypercube Sampling with restricted pairing in this process. The actual details of the integration of the risk analysis are very complex and some variations in this approach are possible. For more information regarding the details of the back-end analysis methodology, the reader should consult Reference 10.

1.5 Analysis Team and Schedule

1.5.1 The Analysis Team

The success of an ASEP-type analysis (i.e., Level 1, front-end, internal events) using these methods depends strongly on the ability of an organization to assemble the required expertise and coordinate the diverse activities. People with the following expertise are recommended for this team:

- One team leader experienced in PRA;
- Two to three systems analysts (at least one of whom is familiar with the necessary computer codes);
- One human reliability analyst (part-time); and
- One data analyst (part-time).

1.5.2 The Team Leader

The team leader manages and integrates the analysis and should have the requisite authority to do so effectively. This individual is responsible for the technical content of the analysis and for ensuring adherence to the procedures and consistency among different analysts. Thus, the team leader should be experienced in PRA and able to provide perspective and direction to the effort. In addition, PRAs require considerable judgment, since many issues as yet unresolved in the technical community must be treated in the analysis. The team leader must weigh differing viewpoints and decide how the analysis is to be performed, depending on the objectives of the study and the portions that need to be emphasized. In the course of the analysis, questions involving subtleties in modeling arise; guidance is needed as to the level of detail at which to develop each model. In order to make these and other judgments, the team leader must have been involved in previous PRAs where similar problems have been faced; that experience will be invaluable in resolving new problem areas.

1.5.3 Analytical Expertise Required

The major portion of a Level 1 PRA analysis is performed by systems analysts. The analysts should be familiar with system design and operation and analysis of systems, although they do not all need to be PRA experts. The systems analysts are responsible for many tasks, including development of the event-tree and system fault tree models for the plant. Therefore, analysts who can provide the accident sequence progression and systems integration that is needed for event tree construction and who can analyze both fluid and electrical systems are needed.

Persons with expertise in human reliability and data analysis are important members of the team. The human factors analyst assists the systems analyst in identifying the human errors to be included in the analysis and provides the insights needed to quantify those errors. The data analyst accumulates and analyzes generic and plant-specific data on component and system failure rates for the quantification of accident sequences. This person should have experience in analyzing data using current statistical techniques and selecting the proper failure rate for the event in question.

A Level 1 PRA analysis produces logic models that are generally impractical to evaluate without use of a Boolean algebra manipulating code. The team should include personnel familiar with the operation of the chosen code.

1.5.4 Utility Involvement

Over the years, it has become clear that there are nearly as many different plant designs as there are plants, particularly with respect to balance-of-plant systems. Thus, the success of the project requires thorough familiarity with the plant being analyzed. This familiarity is best obtained through interactions with utility personnel. The utility can provide people capable of making unique contributions to the analysis. Among them should be someone thoroughly familiar with the operation of the plant. This individual should understand how the plant will be operated under accident conditions and should be familiar with control room operations, plant equipment, and the plant layout. Utility personnel can also provide the necessary knowledge of testing and maintenance procedures, as well as the accompanying administrative controls. The analysis team should also have access to plant personnel familiar with specialized aspects of plant design, such as instrumentation and control.

In addition to providing unique capabilities to the team, utility personnel serve as focal points for the gathering and transmittal of information from the plant and for receiving information pertaining to the analysis. They also ensure that the assumptions made in the analysis accurately reflect the design of the plant and help to ensure that the analysis is realistic. The precise structure for communicating with a utility can be set up on a case-by-case basis; however, in all cases the communication should be reasonably formal. Records should be kept of key transmittals from the utility, and such information should be available to reviewers, although it need not be included in the formal reports. Also, it is important that some interactions occur with both the actual plant personnel and utility headquarters staff.

1.5.5 Manpower Estimates and Schedule

Staff estimates for each task are presented in Table 1.5-1, and a representative schedule is presented in Figure 1.5-1. These are discussed briefly below. Program review is included in the table and figure, and is discussed in the next section. The actual analyses for NUREG-1150 took considerably more effort than indicated here because of the numerous reviews and iterations involved. Nevertheless, the estimates below reflect a realistic indication of the effort required to achieve a draft report including internal review.

Table 1.5-1
Manpower Estimates by Task

	TASK	MANPOWER ESTIMATE STAFF-MONTHS
1.	Plant Familiarization Analysis	3
2.	Accident Sequence Initiating Event Analysis	1
3.	Accident Sequence Event Tree Analysis	3
4.	Systems Analysis	10
5.	Dependent and Subtle Failure Analysis	2
6.	Human Reliability Analysis	3
7.	Data Base Development	2
8.	Accident Sequence Quantification Analysis	2
9.	Plant Damage State Analysis	1
10.	Uncertainty Analysis	2
11.	Draft Report Preparation	6
12.	Program Review	6
	Total	41

* Expert judgment elicitation is not listed as a separate task because it may be used in many tasks.

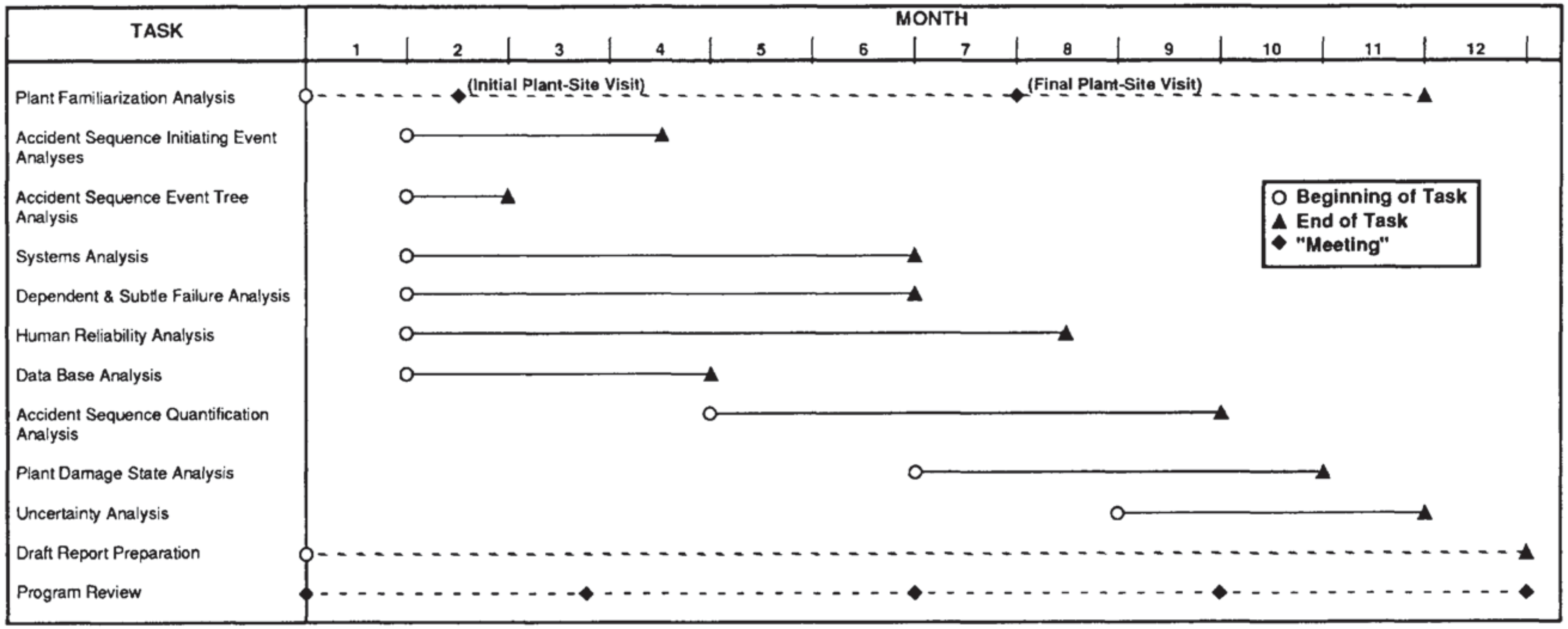


Figure 1.5-1. Schedule for ASEP Analysis

The Plant Familiarization Analysis task precedes all others and forms the basis for construction of the event tree and fault tree models. This task takes about four to six weeks initially (communication with utility personnel is continuous throughout the project) and involves about three staff-months of effort.

The Accident Sequence Initiating Event Analysis, Accident Sequence Event Tree Analysis, and Systems Analysis tasks proceed in parallel, and there are considerable interactions between them. A substantial portion of the Event Tree Analysis task is actually performed in the Accident Sequence Initiating Event Analysis task of identifying the initiating events and responding systems. A limited amount of thermal-hydraulic analysis may be required. As a result, these two tasks are estimated to take about two and one-half months to complete and four staff-months of total effort. The construction of detailed models for all front-line systems and selected support systems requires considerably more time, approximately three to five calendar months and ten staff-months of effort.

The Dependent and Subtle Failure Analysis task proceeds in parallel with the Systems Analysis task. Portions of this task are performed as part of both the plant familiarization and system work. Therefore, this task takes about three to five months and requires two staff-months of effort.

The Human Reliability Analysis and the Data Base Analysis tasks also proceed concurrently with the modeling efforts since both support the modeling. The Human Reliability Analysis task occurs over a longer period of time, since this tends to be an interactive process. Refinements in both data and human error rates are made during the accident sequence quantification analysis when the more important events have been identified. The two tasks are estimated to require about five staff-months of work.

The Accident Sequence Quantification Analysis task is a time-consuming, iterative process that produces point estimates of the core damage frequency. Much of the activity is devoted to ensuring integration of the models, ensuring they are correct and consistent, and then quantifying them. This task takes about three to five months and involves about two staff-months of effort.

The Plant Damage State Analysis involves regrouping the accident sequence cut sets according to selected characteristics that influence subsequent accident progression. This process involves iteration with the back-end analysts and production of point estimates for each plant damage state. The task should begin when the sequence event trees are complete and will take about one staff-month of effort.

The Uncertainty Analysis task produces the final results, including mean values, uncertainty estimates and importance measures. The results must be carefully checked for validity and consistency. The task takes about two months and about two staff-months of effort. If a formal expert judgment elicitation process is included, then this time can increase by a factor of four or more.

The reporting associated with an ASEP analysis is substantial and is a time-consuming task. Major portions of the report should be prepared while the analysis is proceeding. Reporting requires about six staff-months of effort. However, this is time well spent. A well-prepared report will serve as a reference for future analyses and decisions to be made by the utility. Note that the total effort of 41 staff-months produces a draft report that has been reviewed only within the analysis team. Submittal of such a report to outside review generally results in one or more iterations of indeterminate length.

1.6 Program Review

A Level 1 PRA involves a number of assumptions and judgments on the part of the analysis team. To ensure the quality and validity of the work, one or more groups should be chartered with the responsibility for reviewing the work and providing timely feedback. Because the time available to complete the analyses is usually short, these reviews are intense, and analyst response should be rapid. Two review groups were used in the ASEP analyses as described below.

1.6.1 Senior Consultant Group

The purpose of the Senior Consultant Group (SCG) was to provide a broad-scope review of the objectives, assumptions, methods, and results of the four PRAs. This high-level review further assured the validity and applicability of the products. The SCG was not expected to provide detailed quality control or assurance of the products. This high level of review is optional for future analyses since the methodology has now received numerous high-level reviews.

The membership of the SCG changed over the life of the program, but at various times included:

1. Dennis C. Bley, Pickard Lowe and Garrick
2. Michael P. Bohn, SNL
3. Robert J. Budnitz, Future Resources Associates
4. Gregory J. Kolb, SNL
5. Joseph A. Murphy, NRC
6. William E. Vesely, Science Applications International Corporation (SAIC).

1.6.2 Quality Control Group

The Quality Control Group (QCG) provides an in-depth technical review of the methods and results. A group such as this is essential to the credibility of any future Level 1 PRA. The goals of the QCG are to:

1. Provide guidance regarding methods utilized in the PRAs;
2. Ensure the consistent application of methods by all PRA teams; and
3. Ensure the technical adequacy of work.

For the NUREG-1150 analyses, these goals were met via periodic review meetings with the PRA teams and the review of information packages in between the meetings. At the review meetings, the QCG discussed the methods and reviewed, in detail, all technical work performed. This included review of fault trees, cut sets, failure data, etc. Records were kept to document the QCG comments and their eventual resolution. It is essential that such reviews occur during the analysis, as opposed to waiting until a draft report is complete.

The ASEP QCG membership changed over the life of the program, but at various times included the individuals listed below. Also shown are each individual's technical specialties.

1. Barbara J. Bell, Battelle Columbus Division--human reliability analysis;

2. Gary J. Boyd, Safety and Reliability Optimization Services Inc.--systems analysis;

3. Gregory J. Kolb, SNL--systems analysis;

4. Eddie A. Krantz, Idaho National Engineering Laboratory (INEL)--systems analysis;

5. David M. Kunsman, SNL--systems analysis;

6. Gareth W. Parry, NUS Corporation--uncertainty analysis, systems analysis, data analysis, containment and consequence analysis interface;

7. Arthur C. Payne, Jr., SNL--systems analysis, reliability data;

8. John Wreathall, SAIC--human reliability analysis.

1.6.3 Outside Peer Review

Draft NUREG-1150 and its supporting contractor documents were reviewed in considerable detail by numerous outside groups. These reviews have resulted in some significant changes to the present NUREG-1150 methodology. Many of the important comments received are presented in Appendix D of NUREG-1150, so they will not be repeated here. Perhaps more than anything else, these comments have underscored the need to report the results and to explicitly include discussions of the crucial assumptions and limitations of the study. The fact that there have been so many thorough reviews of this work should provide any future user with a good understanding of the capabilities of the methods and the questions that are likely to arise during any accompanying peer reviews.

2. PLANT FAMILIARIZATION ANALYSIS

This section describes the Plant Familiarization Analysis task. Before the technical analysis can begin, it is imperative that the analysis team becomes familiar with all aspects of the plant. The quality of information gathered in this task and the manner in which it is managed is critical to the success of the entire analysis effort. This information gathering process provides assurance that the possible core damage accident sequences are correctly defined and realistically describe the possible plant responses.

2.1 Plant Familiarization Assumptions and Limitations

Because this task provides the basic plant information needed to perform the analytical work, the accuracy of the information gathered is crucial. If inaccurate information is used (e.g., a plant drawing that is out of date: a pump has been removed from the system, but not reflected in the drawing), the potential exists for the final results to inaccurately reflect the plant. It is therefore important that the information be verified. However, verification of the accuracy of the information can be difficult. Using utility designated Controlled Documentation can reduce the potential impact of this limitation. Additionally, some information that is needed to perform the analysis can only be gathered by actually visiting the plant site. This required information is not available in any documentation (e.g., accessibility of a component--a valve is in a location the operator can or cannot readily reach). However, access to a particular area in the plant to determine information may not be possible. In this type of situation, the analyst has two options. The opinions of the plant staff as to accessibility can be used or the analyst may assume some level of accessibility. Either of these options has the potential to inaccurately reflect the plant.

The plant that is being analyzed may not be a fixed entity; that is, during (and after) the period of the analysis, design and operational changes at the plant can occur. Many of the changes will not have a risk or safety impact; however, some of the changes will have the potential to significantly affect the final results of the analysis. The team leader will decide at the start of the project on a configuration freeze date; that is, the date after which plant changes will not be included in the analysis. Therefore, close communication must exist between the team leader and the utility staff member responsible for scheduling plant changes. This minimizes the potential for the analysis to be outdated before completion, and ensures that the analysts are not dealing with a moving target in terms of plant configuration.

2.2 Plant Familiarization Analysis Development

In the Plant Familiarization Analysis task, an understanding of the plant is established. This understanding or knowledge provides the foundation for subsequent technical analyses and modeling activities. This process involves several steps that are illustrated in Figure 2.2-1 and are described below.

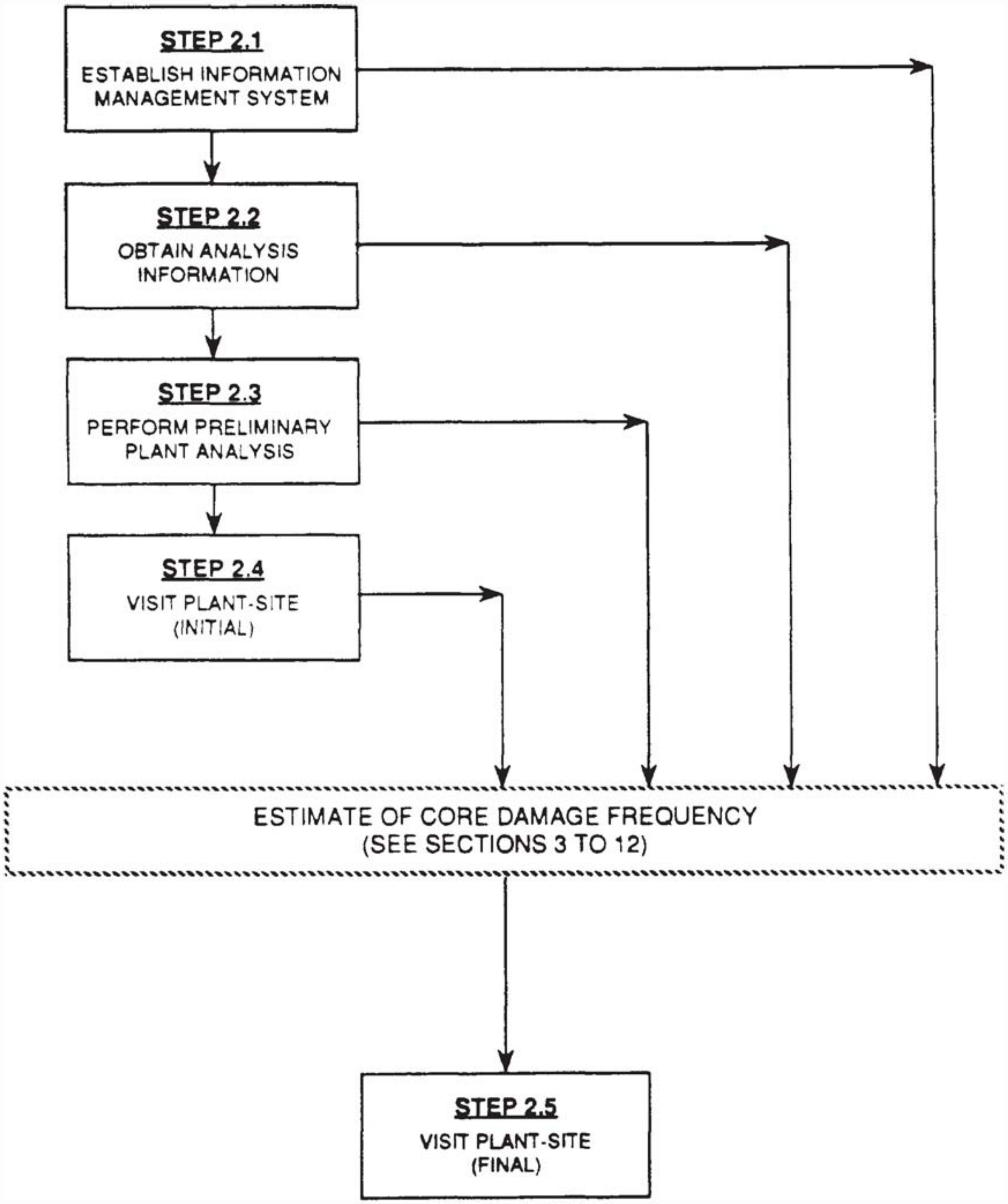

STEP 2.1
ESTABLISH INFORMATION MANAGEMENT SYSTEM
STEP 2.2
OBTAIN ANALYSIS INFORMATION
STEP 2.3
PERFORM PRELIMINARY PLANT ANALYSIS
STEP 2.4
VISIT PLANT-SITE (INITIAL)
ESTIMATE OF CORE DAMAGE FREQUENCY (SEE SECTIONS 3 TO 12)
STEP 2.5
VISIT PLANT-SITE (FINAL)

Figure 2.2-1. Step Relationship for Plant Familiarization Analysis.

Step 2.1. Establish Information Management System

In this step the team leader establishes a system for acquiring and tracking the information gathered throughout the study. A large amount of plant information is collected from almost every department and discipline within the utility (i.e., licensing, engineering, operations, training) and then organized for the analysis team to perform the subsequent analytical tasks. To verify that the information is properly integrated and documented, a formal system for information and data acquisition and tracking is established. The team leader has overall responsibility for cataloging data and controlling the information within the project, as well as documenting all requests for additional information from the various departments. Similarly, a corresponding person at the utility is identified to be responsible for responding to all information requests from the team leader. In addition, the team continuously communicates with the appropriate departments and the utility site throughout the entire analysis. With this procedure in place, plant familiarization work begins.

Step 2.2. Obtain Analysis Information

In this step the analysis team prepares for plant-site visits by obtaining plant information to be studied before any visits. Much of the information required to perform the analysis is obtained from plant documentation and does not require an actual visit to the plant site. However, verification and clarification of the information will be required and can, in some cases, only be accomplished by a plant-site visit. To ensure that this visit proceeds in an efficient manner with the least possible disruption to plant personnel, the team should be prepared. The team should know what questions to ask, what documentation is required, where clarification is needed, what areas and equipment need to be seen in the plant, etc. This preparation involves obtaining: (1) plant documentation and (2) previous Probabilistic Risk Assessments (PRAs) and related studies applicable to the plant. The plant documentation initially required generally consists of the following:

- System descriptions;

- Piping and Instrumentation Diagrams (P&IDs) and Functional Control Diagrams (FCDs) for all front-line systems and their corresponding support systems;

- Elementary wiring diagrams (one lines);

- Layout drawings (the reactor, control, auxiliary, etc. buildings and the control room including layout of instrumentation on the panels);

- Emergency, operating, training, administrative and test and maintenance procedures;

- Component performance information (maintenance logs, Licensee Event Reports (LERs)); and

- Post-Three Mile Island (TMI) and PRA modifications.

Step 2.3. Perform Preliminary Plant Analysis

In this step the team performs preliminary analyses from the information obtained in Step 2.2. This includes developing preliminary accident sequence event trees, system schematics, dependency diagrams and system models and establishing system success criteria (see Section 3 through 10 for descriptions of these activities). This preliminary work is performed only for selected accident initiators and systems. The entire list of systems that are to be examined in the course of the study is not finished until some of the subsequent tasks are complete. However, based on past analyses, a preliminary list of accident initiators and systems can be compiled. These accident initiators and systems that have been shown to be important to safety and risk in past studies are selected. Table 2.2-1 gives this preliminary list for both boiling water reactors (BWRs) and pressurized water reactors (PWRs).

The preliminary analysis also identifies specific areas where additional information is needed to perform the subsequent tasks and for accurate models. Based on these initial activities, the plant-specific information and documentation that are still required are identified. Depending on the utility preference, this may be a single package or several with the appropriate information request being sent to individual departments. Additionally, questions that the team will ask personnel at the plant site concerning system design and plant operation should be prepared before the visit. At this point in the analysis, the team should be adequately prepared for the plant-site visit.

Step 2.4. Visit Plant Site (Initial)

In this step the analysis team visits the plant site to obtain information still required to perform the analytical tasks. It should be recognized that the information still required does not necessarily need to be obtained on a single visit. It may be more efficient to schedule a series of visits depending on the information required and the personnel the team wishes to visit. Additionally, as the PRA progresses, new questions will most likely arise which might require additional plant-site visits. The purpose of this initial plant visit is to acquire the detailed information that is lacking on those aspects of the plant that have been identified at this point as important to safety or risk. If a single visit is scheduled, the visit usually lasts from three to five days. The analysis team consists of the overall program leader, the team leader, the systems analysts, a data analyst, a containment analyst, and a human reliability analyst. The team usually meets with the manager of engineering, his staff and various personnel in operations, training, and maintenance.

Table 2.2-1
Preliminary BWR and PWR Accident Initiators and Systems

BWR	PWR
Accident Initiators	Accident Initiators
Loss of Coolant Accidents (LOCA)	LOCA
Transients	Transients
Station Blackout	Station Blackout
Anticipated Transients Without Scram (ATWS)	ATWS
Front Line Systems	Front Line Systems
High Pressure Core Spray (HPCS)	High Pressure Injection (HPI)
High Pressure Coolant Injection (HPCI)	High Pressure Recirculation
Reactor Core Isolation Cooling (RCIC)	Power Operated Relief Valves (PORV)
Safety Relief Valves (SRV)	Low Pressure Injection (LPI)
Automatic Depressurization (ADS)	Low Pressure Recirculation (LPR)
Low Pressure Core Spray (LPCS)	Accumulators
Low Pressure Coolant Injection (LPCI)	Power conversion
Residual Heat Removal (RHR) --	Auxiliary Feedwater (AFW)
Suppression pool cooling	Containment Spray Injection (CSI)
Containment spray	Containment Spray Recirculation (CSR)
Shutdown cooling	RPS
Reactor Protection System (RPS)	Alternate Injection*
Alternate Rod Insertion (ARI)	
Standby Liquid Control (SLC)	
Power Conversion System (PCS)	
Alternate injection*	
Support Systems	Support Systems
Electric Power	Electric Power
Actuation	Actuation
Instrument Air (IA)	IA
Heating Ventilation Air Conditioning (HVAC)	HVAC
Service water (SW)**	SW**

* At some plants, one example of an alternate injection system would be the Firewater system.

** Service water is used generically here to imply any "cooling water" system that is required for successful operation of the front-line and other support systems

This initial plant visit generally consists of the following.

1. Discussions* with plant engineering and operational staff concerning:

   - Normal and emergency configurations of the various systems of interest;
   - Normal and emergency operation of the various systems during various accidents as outlined by the analysts;
   - System interdependencies;
   - Design changes implemented at the plant;
   - Automatic and manual actions taken in response to various emergency conditions;
   - Operational problem areas identified by plant personnel that might impact the analysis;
   - Subtle interactions and failures identified by the analysts that might be applicable; and
   - Detailed discussions regarding emergency procedures (e.g., walk-through of various accident scenarios).

2. Discussions* with plant engineering and maintenance staff concerning:

   - Data (maintenance logs, LERs, etc.) on specific items provided by the team leader to the data analyst; and
   - implementation of test and maintenance procedures.

3. Discussions* with plant training staff concerning training practices for various emergency conditions.

4. If possible, a visit to the plant simulator where the operators perform various accident scenarios as outlined by the analysis team.

5. Tour of the plant focusing on the modeled systems noting such things as:

   - Location of equipment (e.g., elevation);
   - Enclosed rooms with or without doors;
   - Type of doors (e.g., flood, fire);
   - Size of room;
   - Possibility of establishing natural ventilation; and
   - Travel time for operators.

* Discussions are documented where required. It should be noted that not all analysts participate in every discussion nor visit every plant area, e.g., control room access is usually very restricted.

6. Tour of the control room noting such things as

- Relative location of panels,
- Layout of instrumentation on the panels,
- Type of instrumentation on the panels,
- Relative location of emergency procedures in the control room,
- Type of controls for system and component actuation on the panels (e.g., buttons, switches, key-locked switches, etc.),
- Type of annunciators and location on panels, and
- Annunciator indication (e.g., white light ON means...).

Each of above discussions always centers on its impact and integration into the various analytical tasks. Additionally, plant trip notes are written and sent to the various personnel visited. This allows the utility personnel to clarify any misunderstandings and provides a formal trace of the information received.

Step 2.5. Visit Plant Site (Final)

The purpose of the final plant-site visit is to present to appropriate utility personnel the preliminary results (i.e., after the Level 1 analysis is complete, but before results are published) of the analysis and assess the team's perception of the plant. The visit lasts from one to three days. For the final plant-site visit, the team should at least consist of the overall program leader and the team leader. Additional personnel attending from the analysis team will depend on the final results; that is, if the team leader judges that the discussions will center primarily on the human reliability analysis task, the human reliability analyst might attend. The team generally meets with the manager of engineering, his staff, and various personnel in operations, training, and maintenance.

The final plant visit generally consists of the following:

- Presentation of preliminary results;

- Discussions with engineering staff on major contributors and assumptions;

- Discussions with operational staff on "gray" areas concerning operator actions; and

- Tour of the plant to look at systems and components to clarify any possible misunderstandings, assumptions, etc.

Additional information may be supplied to the analysis team by plant-site personnel in response to issues raised during this final plant visit. Plant trip notes are also written for this visit.

During the entire analysis, regular communication and contact with both plant-site personnel and other utility staff are maintained so that as questions arise, they are resolved and incorporated into the analysis as quickly and efficiently as possible.

2.3 Plant Familiarization Recommended Reporting

This task involves both learning the design and operation of the plant and managing the information that is gathered. The information that is obtained regarding the design and operation of the plant is used to perform the subsequent technical tasks. This information is reported in each of the analytical tasks it supports. The reader should refer to the subsequent sections for the reporting of this information. However, how the information is gathered and managed is important and is generally reported in this task. This information includes the following:

- Analysis Team. The personnel comprising the analysis team consisted of the overall program leader, the team leader, system analysts, a data analyst, a containment analyst and human reliability analysts. The team visited with mechanical engineering staff members and various personnel in operations, training and maintenance at the plant.

- Plant Visits. Any visits to the plant site or other plant offices are reported. This report includes: (1) the dates of the visit, (2) the project staff included on each visit, (3) the purpose of each visit, (4) the personnel that were visited, (5) a general description of each visit (e.g., information discussed such as the Emergency Operating Procedures; walkdowns of the plant systems under examination), and (6) any major findings of each visit.

- Plant Changes. During the period of the analysis, the plant will most likely undergo changes (e.g., adding redundancy to the actuation logic of the reactor protection system). The changes that are incorporated into the analysis are discussed.

An example of the information that is reported in this part of the analysis is given in the following subsection.

2.4 Example of Plant Familiarization Analysis

One of the four plants analyzed in this program was selected to illustrate the methodology for each of the tasks. The plant selected is Peach Bottom, Unit 2.

Peach Bottom, Unit 2 is a BWR-4 reactor type with a Mark I containment. Peach Bottom is basically a four-division plant. Pressure relief is provided through 11 SRVs. Five of these SRVs are part of the ADS. The PCS provides core cooling and heat removal in normal operations. In case the core cooling function of PCS is lost, the emergency core cooling is provided by the HPCI system (turbine-driven single train with no AC dependence) and two low pressure motor-driven systems (i.e., LPCI and LPCS). Core cooling can also be provided by a RCIC system, a High by either: (1) the RHR system with several operational modes--suppression pool cooling, containment spray and shutdown cooling; or (2) the containment venting system. The Emergency Service Water (ESW) system provides cooling water for emergency system pump-motor cooling, room cooling and diesel generator cooling. A High Pressure Service Water (HPSW) system provides the heat sink for the RHR system. Figure 2.4-1 gives an overall schematic of the plant.

Where the methodology may differ because of the differences between BWRs and PWRs or because of uniqueness of Peach Bottom, examples are given to illustrate these differences.

An example of a BWR Plant Familiarization Analysis is presented below.

Step 2.1. Establish Information Management System

There are many ways to manage the information gathered for a PRA. The project team leader should establish a system to document the following information:

- Questions that arise during the analysis and their resolution;

- Assumptions made throughout the analysis;

- Initiators examined in the analysis (including any screened out);

- The success criteria established for each initiating event group;

- The accident sequences developed for each initiating event group--those that are dominant and non-dominant--and the reasons for the differences;

- System information that is used in the development of the system models;

- Estimation of basic event probabilities and initiating event frequencies;

- Operator actions considered in the analysis, and the information used to determine the human failure rates;

- Comments from the various review groups and their incorporation into the models.

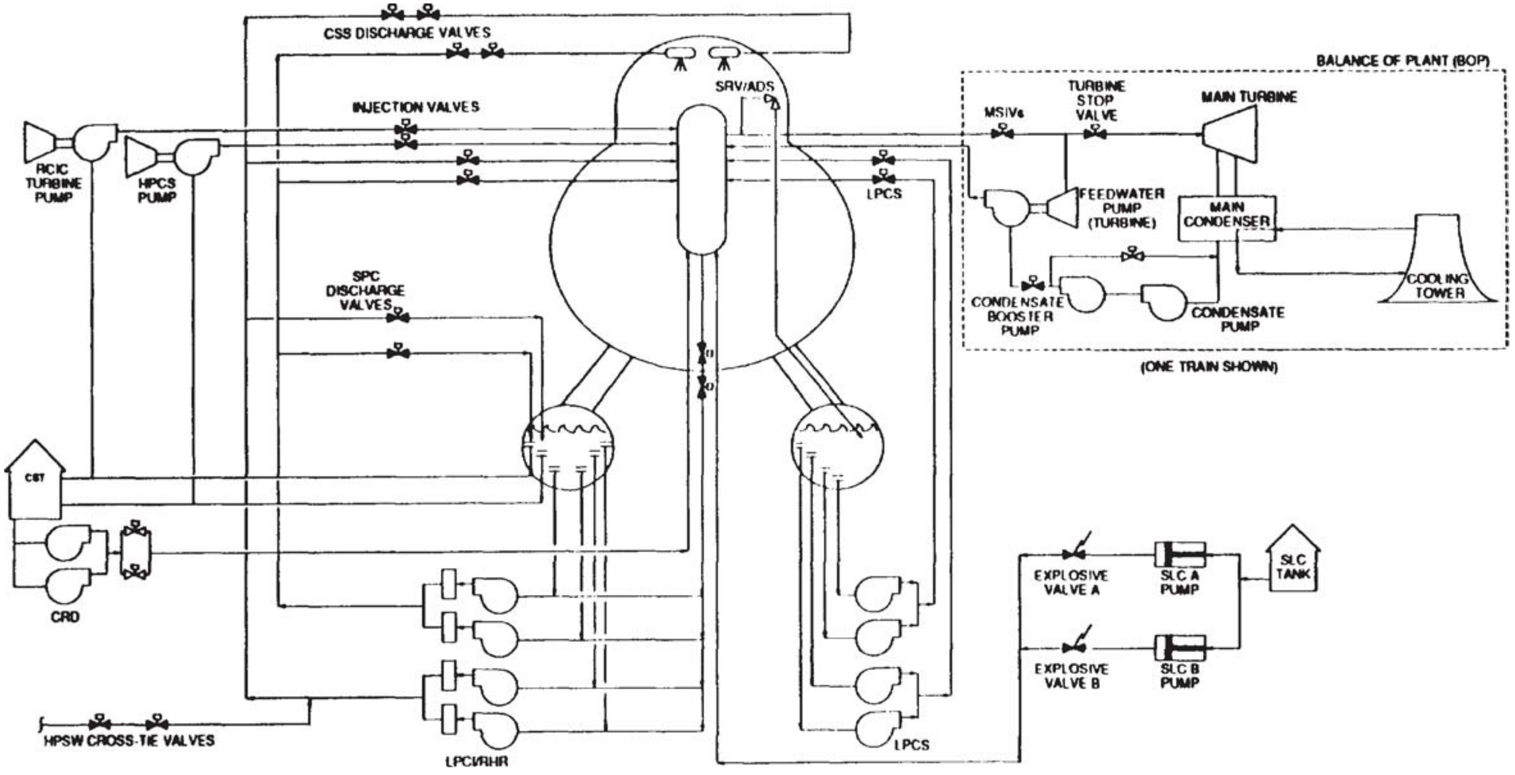


Figure 2.4.1 Plant Schematic of Peach Bottom, Unit 2

Step 2.2. Obtain Analysis Information

An example of the plant information request is shown in Table 2.4-1.

Step 2.2. Perform Preliminary Plant Analysis

An example of the plant visit information request and questions sent to the plant personnel is shown in Table 2.4-2. The individual analyses are discussed in Sections 3 through 10 of this report.

Step 2.2. Visit Plant Site (Initial)

Detailed plant trip notes are taken on the individual plant visits. An example of plant trip notes is not given. The notes generally consist of information gathered during discussions, documentation received, and a list of action items (either for team or other utility personnel).

Step 2.5. Visit Plant Site (Final)

An example of a final plant visit presentation is not given. The presentation generally includes the final results and basic assumptions.

Table 2.4-1
Example of Plant Information Request

Procedures

- LOSP
- Station Blackout
- Loss of One AC Bus (Safety)
- Loss of One DC Bus (Safety)
- Loss of PCS (Feedwater, etc.)
- Turbine Trip
- Loss of Service Water (SW)
- Loss of One 120 V AC Vital Bus
- Administrative
- Training
- Loss of HVAC
- Loss of IA
- Inadvertent SRV Opening
- Main Steam Isolation Valve (MSIV) Closure Event
- Containment Venting
- LOCA
- Any other specific procedure or guideline impacting the plant-specific implementation of the Emergency Procedure Guidelines (EPGs)
- Maintenance and test (human reliability expert will elaborate).

Elementary Wiring Diagrams

- AC/DC Distribution System
- Emergency AC (including DC power for diesels)
- Systems for which P&IDs are needed except HVAC, IA, PCS.

P&IDs, FCDs and System Descriptions

- Nuclear Steam Supply System Instrumentation
- RHR (including LPCI)
- HPCI
- RCIC
- LPCS
- ADS
- PCS
- CRD
- SLC
- SW
- HVAC systems that support above systems
- IA

Technical Specifications (TS)

List of Post-TMI Modifications (and Post-PRA)

Layout Drawings

- Reactor Building, Control, Auxiliary, etc. Building (to determine accessibility to areas for recovery and potential common cause from a HVAC point of view).

- Control room including instrumentation layout on panels.

Table 2.4-1
Example of Plant Information Request (Concluded)

Plant Personnel that the Team Needs to Meet with During the Site Visit

- System engineers
- Instrumentation and electrical engineers
- Test and maintenance personnel
- Operators
- Anyone utility recommends to answer types of questions listed below

Types of Questions to be Addressed on Plant Visit

- General system layout;
- Specific component dependencies (AC/DC power by distribution bus, SW, IA, etc.);
- Loads--particularly for support systems (power, IA, SW, HVAC, etc.);
- Success criteria under different conditions;
- Actuation specifics--what automatically starts system, what stops or isolates system, what can be controlled from control room, what is locally operated, etc.;
- Timing considerations--how long can component run without cooling, how long do batteries last without charging, etc.;
- Are there other success paths not known to us?
- Maintenance and operational tendencies--staggered, preventive, specifics of system operation, e.g., what is normally running, what is normally standby.

Table 2.4-2
Example of Plant Visit Request

Individuals the Team Needs to See

- Persons familiar with system success criteria for various initiators;
- Engineers familiar with design, testing, maintenance and operational aspects of systems;
- Data base specialist;
- Test and maintenance personnel familiar with test (staggered versus non-staggered) and maintenance (scheduled versus non-scheduled) philosophies, tagging procedures, etc.;*
- Operational staff familiar with plant procedures, actions they would take under certain accident conditions, other recovery possibilities, etc.*
- ATWS sequence experts;*
- Containment response analyst.

Typical Questions

1. Pre-existing containment leakage could affect containment pressurization rate, etc. What leakage rate is allowed and how is leakage detected from the drywell? Wetwell?

2. What do the procedures call for to attempt early scram given failure of auto scram? Possibilities would seem to include:

   - Manual scram buttons in control room?
   - Provisions for single rod scram in auxiliary control room?
   - Vent air from scram pilot valve operators? How?
   - Perform scram reset and try manual scram? (Will this function if scram condition persists?)
   - Manual insertion of rods using rod sequence control system? How will operator select maximum worth rods to put in first? Must he override interlocks to do so? How difficult is it to override the interlocks?

3. Is the ARI system implemented. If not when?

4. ARI Design

   a. Does the ARI system use separate sensors, logic, and scram air header exhaust valves from the RPS?

* Particularly at the plant with the ability to talk through scenarios, see the equipment locations (in or out of control room, close or far, etc.), observe test and maintenance practices, etc.

Table 2.4-2
Example of Plant Visit Request (Continued)

b. Does the ARI use equipment (sensors, valves...) similar in design, maintenance, and testing requirements to that used in the RPS?

c. Is the ARI "fail-safe" like RPS; i.e., deenergize to trip?

d. Is the ARI system 1-of-2-taken-twice logic? Does the logic monitor all the same parameters as RPS?

5. Recirculation Pump Trip (RPT)

a. Are there any cases where RPT is not needed?

b. What signals actuate RPT automatically?

c. Is there any analysis establishing time or conditions when RPT must occur?

6. MSIVs

a. What signals cause MSIV closure? Which ones can be bypassed and how?

b. Is the current MSIV low level setpoint at Level 1 or 2?

c. Is the feedwater runback implemented? When does it actuate? What is the resulting flow? What is the effect on the number of MSIV closure events?

d. How much cladding failure must occur before MSIVs close on high radiation?

e. Do procedures specifically call for attempting to keep the MSIVs open if they didn't initially close or re-open the MSIVs given an ATWS with MSIV closure? If so, are operators aware of the difficulties such as the possible need to jumper isolation signals?

7. Turbine Bypass

a. Is the turbine bypass capability at Peach Bottom 25% of full power?

b. Have there been any instances of turbine bypass failure at Peach Bottom?

Table 2.4-2
Example of Plant Visit Request (Continued)

8. Drywell Coolers

   a. What signals trip the drywell coolers and would they be restarted by procedure?

9. SLC

   a. Is the current configuration a manual 43 gpm system?

   b. When is the 86 gpm system to be implemented? Will it be auto or manual?

   c. What are the necessary conditions to start SLC? Are any special administrative approvals required?

   d. How does the operator know when sufficient boron has been injected so as to increase coolant injection flow per the EPGs?

10. Level Control

   a. What instruments will be relied upon to indicate the water level when it is near the Top of Active Fuel (TAF)?

   b. Are operators aware of the potential discrepancies and errors in level readings from calibration differences? What effect is expected from rerouting of the level instrumentation compensating legs?

   c. Please clarify the relationships of Coolant Levels 2 and 1 to the TAF.

11. High Pressure Cooling

   a. What is your perception of the adequacy of RCIC and CRD to prevent core damage during an ATWS? Sufficient flow?

   b. Are you aware of any analyses that may contradict the assumption that HPCI and RCIC will fail with suction water temperatures of 200 to 240°F?

   c. It is understood that HPCI switches suction to the suppression pool on high level in the pool or on low condensate storage tank (CST) level and that RCIC now just switches on low CST. Is this true? Are operators trained to manually switch RCIC if HPCI switches and to manually switch HPCI if its auto-switch systems would be prevented? Is such prevention possible? Can the systems be switched back to the CST and how?

Table 2.4-2
Example of Plant Visit Request (Continued)

d. At what turbine exhaust backpressures will the HPCI and RCIC turbines fail?

12. Depressurization

a. What is the approximate relief capacity (in terms of percentage of full power) of the ADS valves? All the SRVs?

b. Does the ADS still use a high drywell pressure signal?

c. What indications are used to show SRV position?

d. Is the plant following the suggested EPGs calling for depressurization to avoid pool heat capacity temperature limits? How will this be performed?

e. Won't the auto ADS timer keep restarting (with operator reset) during the time that level control is near TAF?

f. What are the required differential pressures between the drywell pressure and the service air pressure to sustain an SRV open or to open an SRV? What is the maximum service air pressure and do procedures call for maximizing this pressure during high containment pressure conditions? Will the service air be isolated during ATWS and can it be reopened?

13. Low Pressure Cooling

It is understood that the plant procedures call for use of low pressure systems during ATWS, if required.

a. Will the condensate system still be potentially available to inject flow into the vessel (depending on the initiating event) and in fact, will it automatically inject if pressure in the vessel is low enough? (i.e., condensate is not locked out?)

b. Is it true that LPCS/LPCI must be manually shut off once they start (there is no Level 8 auto trip, for example)?

c. Is it true that LPCS/LPCI will auto restart on a sustained Level 1 signal unless they are locked out?

d. Is it true that LPCS/LPCI do not trip on low suction pressure?

e. Can LPCS/LPCI systems pump saturated water?

f. Are there any procedures for LPCS/LPCI switch to CST for suction?

Table 2.4-2
Example of Plant Visit Request (Concluded)

g. Does the operator training include awareness of the potential for large, sudden injections using the low pressure systems especially if depressurization is called for to avoid pool heat capacity temperature limits?

h. Will the suppression pool cooling mode of RHR switch to the LPCI mode at Level 1 or high drywell pressure? If so, does the operator training include the potential difficulties associated with maintaining suppression pool cooling since switching to LPCI will divert flow from the pool when reactor pressure is low enough?

i. Can condensate/LPCS/LPCI be throttled to keep level at TAF?

14. Containment Venting

a. What are the procedural requirements for containment venting?

b. Is it correct that the procedures call for venting the drywell and wetwell first with the 2-in. lines, the 6-in. lines, and then the 18-in. lines?

c. What power is required to open the vent lines and monitor the containment pressure?

d. Are there analyses available to show the adequacy of the vent lines under ATWS conditions?

e. Must isolation interlocks be overridden to vent? How and where are they overridden? Are the procedures clear on this point?

f. Under what conditions are the vent valves reclosed? Do procedures specify these conditions?

15. General

Many simultaneous operator actions could be required during an ATWS (rod insert, SLC start, level monitoring, emergency core cooling system pump control, depressurization...). The human reliability analysis experts will probably be very interested in seeing the control room layout for the relative locations of the above equipment and discussing the ATWS scenario with operators and/or training staff. How many operators would need to be involved, and how they would communicate, etc. may have an impact in the ATWS analysis. This is one scenario (among others) that will warrant discussion in considerable detail while at the plant site. Therefore, any assistance you could provide us in better understanding the planned operator response to an ATWS during the plant visit will be appreciated.

3. ACCIDENT SEQUENCE INITIATING EVENT ANALYSIS

In a Probabilistic Risk Assessment (PRA), those events that disrupt the normal conditions in the plant and lead to the need for reactor subcriticality and decay heat removal are referred to as accident sequence initiating events. This section describes the methodology used to identify and group the initiating events examined in the analysis.

3.1 Initiating Event Assumptions and Limitations

The identification of the initiating events is limited to those events associated with plant equipment and the loss of offsite power. External events such as winds, fires, flooding, and earthquakes are not considered in this analysis. For external event analysis, the reader is referred to Reference 6. Additionally, this analysis is performed for 100% power conditions; events occurring at low power or cold shutdown are not included.

The objective of the PRA is a realistic analysis; excessive conservatism is avoided where possible. Where resources permit, specific analyses (e.g., thermal-hydraulic calculations) are performed to establish realistic success criteria. However, where schedule and resources do not allow for specific calculations, the success criteria may be based on Final Safety Analysis Report (FSAR) information or valid thermal-hydraulic calculations from other sources.

3.2 Initiating Event Analysis Development

Initiating events applicable to the plant must be identified. Once the events have been identified, they are grouped to make the subsequent tasks more efficient. This grouping is performed because the plant responds in exactly the same manner for several initiating events. These tasks are performed in several steps as illustrated in Figure 3.2-1 and as described below.

Step 3.1. Obtain Information

In this step, the information that is required to identify and group the applicable initiating events is identified and gathered. A significant portion of this information is obtained in the Plant Familiarization Analysis task. The required information generally includes the following:

- Plant logs;
- Licensee Event Reports (LERs);
- Nuclear Regulatory Commission LER data summaries;[11,12]
- Electric Power Research Institute initiating event reports;[13,14]
- Idaho National Engineering Laboratory, EG&G Idaho Inc. initiating event report;[15]

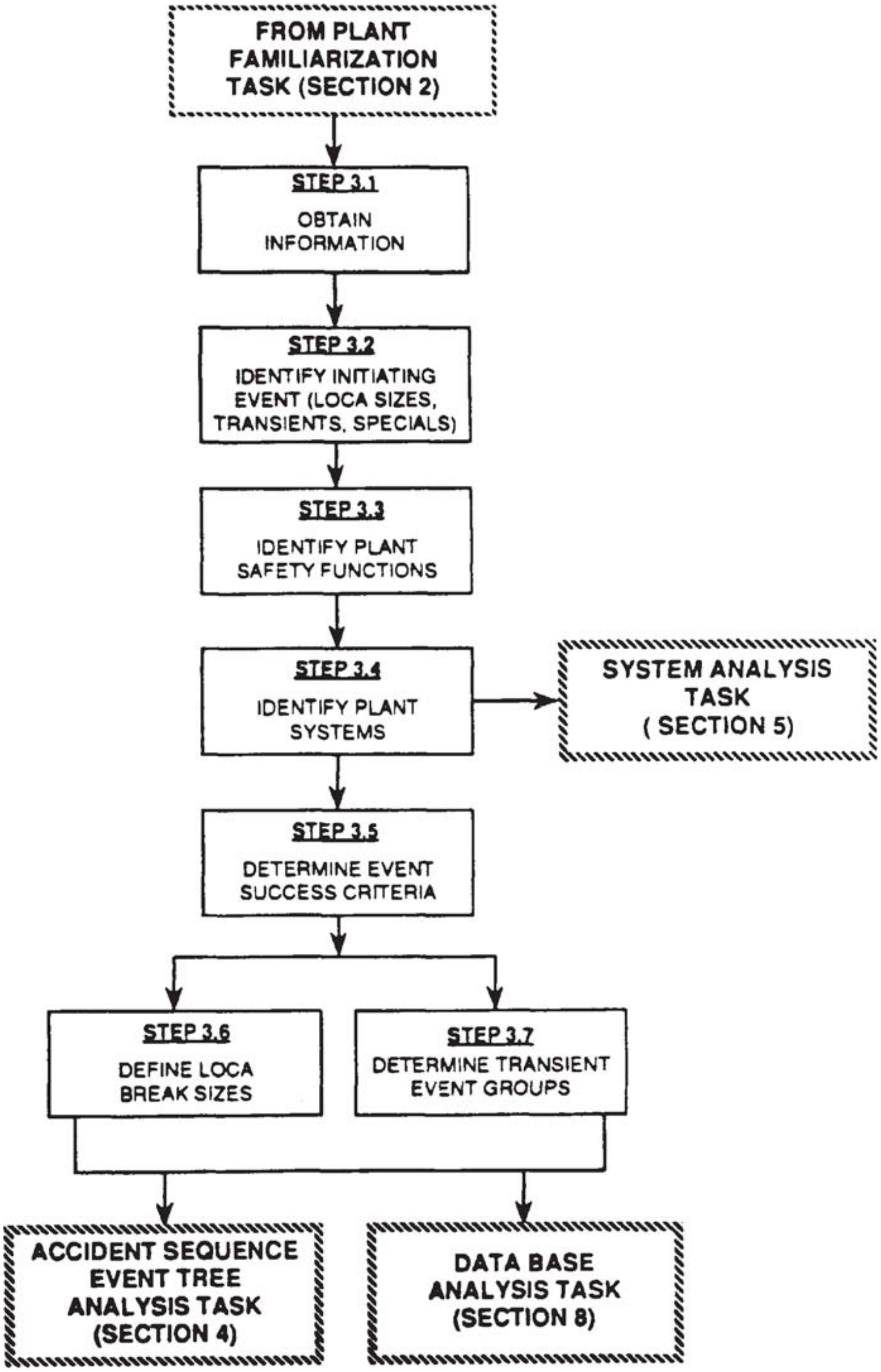

FROM PLANT FAMILIARIZATION TASK (SECTION 2)
STEP 3.1
OBTAIN INFORMATION
STEP 3.2
IDENTIFY INITIATING EVENT (LOCA SIZES, TRANSIENTS, SPECIALS)
STEP 3.3
IDENTIFY PLANT SAFETY FUNCTIONS
STEP 3.4
IDENTIFY PLANT SYSTEMS
SYSTEM ANALYSIS TASK (SECTION 5)
STEP 3.5
DETERMINE EVENT SUCCESS CRITERIA
STEP 3.6
DEFINE LOCA BREAK SIZES
STEP 3.7
DETERMINE TRANSIENT EVENT GROUPS
ACCIDENT SEQUENCE EVENT TREE ANALYSIS TASK (SECTION 4)
DATA BASE ANALYSIS TASK (SECTION 8)

Figure 3.2-1. Step Relationship for Accident Sequence Initiating Event Analysis

- Final Safety Analysis Report (FSAR);
- Appropriate vendor (i.e., Westinghouse, General Electric, Combustion Engineering, or Babcock and Wilcox) Loss of Coolant Accident (LOCA) reports;[16,17,18,19]
- Plant information (such as system descriptions) to evaluate "special initiators";
- Plant layout and elevation drawings; and
- Other miscellaneous reports the analysis team identifies as applicable to the analysis.

The manner in which data is collected and catalogued varies from plant to plant. The above list is generic. The analyst should consult with plant personnel to determine if any other type of documentation exists that will assist in identifying plant-specific initiating events.

Step 3.2. Identify Initiating Events

In this step the analyst identifies the initiating events that can disrupt the normal conditions in the plant and potentially result in an accident sequence. These events are classified as either transient events or LOCAs. Transient events generally involve events related to the Balance Of Plant (BOP), while the LOCAs involve pipe breaks within the high pressure primary coolant system piping. Numerous initiators of these types have been catalogued in previous PRAs. However, recent analyses have shown there are other types of events that can be important to risk and safety. These events are referred to as special initiators. Each of these is discussed separately.

Step 3.2a. Identify LOCA Sizes

In this step the analyst defines the ranges of LOCA break sizes. The primary system contains a variety of piping sizes which, if breached, could require different systems to function for prevention of core damage. Nevertheless, the range of LOCA sizes can be divided into groups for which plant response, in terms of required system operability, is the same or very similar. This information is obtained from the plant FSAR (modified if necessary for realism, as opposed to conservative licensing criteria) or it may be established from thermal-hydraulic analyses of the particular events. The LOCA sizes for boiling water reactors (BWRs) and pressurized water reactors (PWRs) are usually defined as follows:

A large LOCA is a break that depressurizes the reactor to the point where the low pressure systems can inject automatically providing sufficient core cooling to prevent core damage.

An Intermediate LOCA is a break that does not depressurize the reactor quickly enough for the low pressure systems to automatically inject and provide sufficient core cooling to prevent core damage. However, the loss from the break is such that high capacity systems (i.e., 1500 to 5000 gpm) are needed to makeup the inventory depletion.

A small LOCA is a break that does not depressurize the reactor quickly enough for the low pressure systems to automatically inject and provide sufficient core cooling to prevent core damage. However, low capacity systems (i.e., 100 to 1500 gpm) are sufficient to makeup the inventory depletion.

A small-small LOCA is defined as a seal leak from the recirculation pump for a BWR and the reactor coolant pump for a PWR.

Step 3.2b. Identify Transient Events

In this step the analyst identifies the transient initiating events. Analyses that have identified generic event initiators are reviewed and those events applicable to the plant are identified. Generic transient events for BWRs and PWRs from the EG&G initiating event report [15] are identified below in Table 3.2-1. The plant history is reviewed to identify any additional plant-specific transient initiating events.

Step 3.2c. Identify Special Events

If the loss of a plant system (excluding BOP systems and offsite power) disrupts the normal operation of the plant, this event is referred to as a special initiator. Such special initiators, although relatively low in frequency, may contribute significantly to the core damage frequency and therefore ought to be examined. Failure Modes and Effects Analysis is one method for determining whether a system should be included as a special initiator. In this method, each component within the system is identified; then for each component the analyst determines: (1) its function, (2) the possible failure modes, (3) the failure mechanisms, (4) the effects on the system, and (5) the method of failure detection. This process is performed in part in the Systems Analysis task.

Some examples of systems where loss should be examined as special initiators are listed below:

- Vital AC or DC buses;
- Cooling water or service water systems, that is, any cooling water system that is required in a support function, but not as a direct core cooling system;
- Instrument air; and
- Heating, ventilation and air conditioning

There may be other systems that are unique to a given plant. The analyst should conduct a thorough evaluation of plant systems to determine which, if any, should be included as initiators.

There are some events that do not involve the loss of a system, but rather specific components. That is, for normal transients a component failure causes a system to fail, which then in turn results in a reactor

Table 3.2-1
Generic Transient Events for BWRs and PWRs

BWR Events	PWR Events
1. Electric load rejection	1. Loss of Reactor Coolant System (RCS) flow (one loop)
2. Electric load rejection with turbine bypass valve failure	2. Uncontrolled rod withdrawal
3. Turbine trip	3. Control Rod Drive (CRD) mechanical problems and\or rod drop
4. Turbine trip with turbine bypass valve failure	4. Leakage from control rods
5. Main Steam Isolation Valve (MSIV) closure	5. Leakage in primary system
6. Inadvertent closure of one MSIV	6. Low pressurizer pressure
7. Partial MSIV closure	7. Pressurizer leakage
8. Loss of condenser vacuum	8. High pressurizer pressure
9. Pressure regulator fails open	9. Inadvertent safety injection signal
10. Pressure regulator closed	10. Containment pressure problems
11. Inadvertent Open Relief Valve (IORV)	11. Chemistry and Volume Control System (CVCS) malfunction -- boron dilution
12. Turbine bypass fails open	12. Pressure, temperature, power imbalance -- rod position error
13. Turbine bypass or control valves cause increased pressure (closed)	13. Startup of inactive coolant pumps
14. Recirculation control failure, increasing flow	14. Total loss of RCS flow
15. Recirculation control failure, decreasing flow	15. Loss or reduction in Feedwater (FW) flow (one loop)
16. One recirculation pump trip	16. Total loss of FW flow (all)
17. Recirculation pump trip (all)	17. Full or partial closure of MSIV (one loop)
18. Abnormal startup of idle recirculation pump	18. Closure of all MSIVs
19. Recirculation pump seizure	19. Increase FW flow (one loop)
20. Feedwater (FW) increasing flow at power	20. Increase FW flow (all loops)
21. Loss of FW heater	21. FW flow instability -- operator error
22 Loss of all FW flow	22. FW flow instability -- miscellaneous mechanical
23. Trip on one FW or condensate pump	23. Condensate pumps loss (one)
24. FW, low flow	24. Condensate pumps loss (all)

Table 3.2-1
Generic Transient Events for BWRs and PWRs (Concluded)

BWR Events		PWR Events	
25.	Loss FW flow during startup or shutdown	25.	Loss of condenser vacuum
26.	High FW flow during startup or shutdown	26.	Steam generator leakage
27.	Rod withdrawal at power	27.	Condenser leakage
28.	High flux from rod withdrawal at startup	28.	Miscellaneous leakage in secondary system
29.	Inadvertent insertion of rods	29.	Sudden opening of steam relief valves
30.	Detected fault in Reactor Protection System (RPS)	30.	Loss of circulating water
31.	Loss of offsite power	31.	Loss of component cooling
32.	Loss of auxiliary power (transformer)	32.	Loss of service water
33.	Inadvertent startup High Pressure Coolant Injection (HPCI) or Core Spray (HPCS)	33.	Turbine trip, throttle valve closure, EHC problems
34.	Scram from plant occurrences	34.	Generator trip or generator caused faults
35.	Spurious trip via instrumentation RPS fault	35.	Loss of offsite power (LOSP)
36.	Manual scram, no out-of-tolerance condition	36.	Pressurizer spray failure
37.	Cause unknown	37.	Loss of power to necessary plant systems
		38.	Spurious trips, cause unknown
		39.	Auto trip, no transient
		40.	Manual trip, no transient
		41.	Fire within secondary system

trip. But, for these special initiators, the component loss directly results in a reactor trip and the need for decay heat removal. These types of failures disrupt the normal operation of the plant and have a potential for severe risk consequences. The events that need to be examined as special initiators include:

- Steam Generator Tube Rupture (SGTR). SGTR is defined as a tube break that results in a loss of primary coolant of approximately 50 gpm or greater;

- Interfacing LOCA. This LOCA is defined as backflow of high pressure coolant from the primary system back through low pressure injection system piping which results in the breach of the piping or components.

- Vessel Rupture. This event is defined as a rupture in the vessel such that it leads directly to core damage.

In determining whether the loss of a plant system or component should be treated as a special initiating event, the frequency and the expected level of degradation to other plant systems must also be considered. If the estimate of the event frequency is below a preselected screening level, the event does not necessarily require further examination. But, before eliminating any event, the analyst must also consider whether or not initial estimates of the frequencies of any accident sequences caused by the event are below a preselected screening value, typically 1E-8 per reactor year If they are, the event probably does not require further examination. However, in selecting this latter screening value, the analyst does not want to eliminate any initiators that could result in dominant accident sequences. That is, the final accident sequences retained for full quantification should represent approximately 95 to 99% of the core damage frequency. Therefore, the process is iterative and may involve significant engineering judgment.

Finally, if (1) the event has the same effect on plant systems as a previously defined LOCA or BOP transient event and (2) the estimated frequency of the event is less than either the LOCA or the BOP transient event, then the special event can be subsumed in either the LOCA or BOP transient.

Step 3.3. Identify Plant Safety Functions

In this step the analyst identifies the plant functions (e.g., core cooling) that are required to mitigate the initiating events and to prevent core damage* and radionuclide release. Identification of these safety functions forms the preliminary basis for grouping initiating events.

* For BWRs in this study, the core is considered to be in a damaged state when the reactor water level is less than two feet above the bottom of the active fuel. For PWRs, the core is considered to be in a damaged state once the top of the active fuel assemblies is uncovered.

Safety functions can be defined many different ways, depending on the plant type, system design, the timing of system responses, and the preference of the analyst. The safety functions used for both the BWRs and PWRs (as shown in Table 3.2-2) are based on the Interim Reliability Evaluation Program Procedures Guide.[7]

Step 3.4. Identify Plant Systems

In this step the analyst identifies all the plant systems that can perform each of the safety functions above. The capacities of each system and the conditions under which the system can operate are also identified (e.g., system can provide 5000 gpm with reactor at high pressure, but cannot provide any makeup with reactor at low pressure, < 300 psig). This information is obtained from plant documentation such as system descriptions and the FSAR.

Step 3.5. Determine Event Success Criteria

In this step the analyst establishes the success criteria required to mitigate the effects of the initiating events, that is, the minimum requirements of each safety function in order to prevent core damage. However, before the analyst can determine what these requirements are, the point at which core damage occurs must be defined (see Step 3.3 for definition of core damage). For BWRs in this study, the core is considered to be in a damaged state when the reactor water level is less than 2 ft above the bottom of the active fuel. However, a more accurate definition can be used: core damage occurs when the peak allowable cladding temperature is reached. This definition was not used in the BWR NUREG/CR-4550 front-end studies because it would have required detailed thermal-hydraulic calculations beyond the scope and resources of the work. For PWRs, the core is considered to be in a damaged state once the top of the active fuel assemblies is uncovered. The difference in these definitions is a result of the inherent differences between BWRs and PWRs. In a BWR, partial core uncovery does not result in damage, because a BWR is designed for in core boiling and steam cooling.

In establishing the basic requirements for each safety function to prevent core damage, the analyst (1) determines the effects of the safety functions on each other, (2) identifies the different time periods of the accident (e.g., $0 < t < 1$ h, $1 < t < 4$ h, etc.) during which the success criteria for each function changes, (3) identifies the phenomenological conditions created by the accident sequence, and then (4) determines the combination of the systems (identified in Step 3.4) needed to perform each function.

In performing this four-step analysis, the definition of the success criteria becomes rather complex because, depending on how well a particular function is accomplished, the success criteria can change for the other safety functions. Therefore, the success criteria of the safety functions is considered within a hierarchical type framework.

Reactor subcriticality affects the power (i.e., heat) production which affects the amount of pressure relief, coolant inventory, and heat

Table 3.2-2
BWR and PWR Plant Safety Functions

Reactor/Event	Safety Function	Purpose/Description
BWRs		
LOCAs	• Reactor subcriticality	• Shut reactor down to reduce power (heat) production
	• Emergency Core Cooling (ECC)	• Maintain coolant medium around core
	• Early containment overpressure protection	• Protect containment from failure due to energy release of the LOCA blowdown
	• Late containment overpressure protection	• Protect containment from failure due to heat transferred from the coolant
Transients	• Reactor subcriticality	• Shut reactor down to reduce power (heat) production
	• RCS overpressure protection	• Protect the RCS from power and pressure surge caused by the turbine trip
	• ECC	• Maintain coolant medium around core
	• Containment overpressure protection	• Remove the heat transferred from the coolant to the containment to control pressure
PWRs		
Transients and LOCAs	• Reactor subcriticality	• Shut reactor down to reduce power (heat) production
	• Core heat removal	• Maintain fuel temperature limits by transfer of heat from fuel to coolant and ultimately outside of RCS boundary
	• RCS integrity	• Maintain the integrity of the reactor coolant boundary in order to preserve coolant inventory
	• Containment overpressure suppression	• Protect containment from failure due to heat discharged from the RCS

removal required. The success criteria of this function depends upon how well reactor subcriticality is accomplished. Therefore, this function is the first one considered. If the energy release (i.e., blowdown from LOCA or power imbalance from a transient) is not prevented, it can: (1) potentially result in core damage, that is, the remaining safety functions have no impact; or (2) also affect the success criteria of the remaining functions. This hierarchical framework (i.e., type of logic) is followed throughout. It illustrates the reasoning used in determining the success criteria for each safety function for the various initiating events and the ordering of the functions.

In most cases, the success criteria for the LOCAs and the transients have been well defined in past PRAs or from thermal-hydraulic calculations performed either by the utility (i.e., FSAR calculations) or by the vendor. However, if the analyst feels that these sources are excessively conservative, plant-specific calculations may be required. Once the basic success criteria have been defined, the analyst identifies systems (from Step 3.4) that satisfy the requirements.

Step 3.6. Define LOCA Break Sizes

In this step the actual break sizes for the LOCAs are defined. The break size range depends on the specific plant. Differentiation of LOCA sizes is required since the plant specific response varies according to the size of a break. Therefore, the break is defined by the size that is required to give the conditions identified in Step 3.2a (including both steam line and fluid line breaks).

The following LOCA groups were used in the NUREG/CR-4550 studies:

BWR LOCA Sizes

- Large LOCA, labeled A, steam or liquid break sizes of approximately 0.1 ft^2 or larger;

- Intermediate LOCA, labeled S1, liquid breaks of approximately 0.004 to 0.1 ft^2 and steam breaks of approximately 0.05 to 0.1 ft^2;

- Small LOCA, labeled S2, liquid breaks less than 0.004 ft^2 and steam breaks less than 0.05 ft^2;

- Small-small LOCA (defined to include special recirculation pump seal leaks), labeled S3, for leaks up to a maximum of approximately 50-100 gpm on a per pump basis although less than 5 gpm is more typical;

- Interfacing system LOCAs; or the so-called "V" sequence, are a breach of a high pressure to low pressure interface with the primary system.

PWR LOCA Sizes

- Large LOCA, labeled A, break sizes with diameters greater than 6 in.;

- Intermediate LOCA, labeled S1, break sizes with diameters between 2 to 6 in.;

- Small LOCA, labeled S2, break sizes with diameters between 1/2 to 2 in.;

- Small-small LOCA, labeled S3, break sizes with diameters less than 1/2 in. or flows of approximately 50 to 100 gpm (seal LOCA); and

- Interfacing system LOCAs, breaks caused by a breach of a high pressure to low pressure interface with the primary system. (This break will only be included based on the results of Step 3.2c.)

Step 3.7. Determine Transient Event Groups

In this step the analyst classifies the initiating events into transient groups differentiated by their effect on the Power Conversion System (PCS) or offsite power.

For the BWRs considered in NUREG-1150, the groups were differentiated by offsite power failure and whether the PCS failures are causing loss of core cooling, heat removal or both. The following transient groups were then identified:

BWR Groups

- Events resulting in an immediate LOSP;

- Events resulting in an immediate loss of the PCS (offsite power initially available) such that coolant makeup (i.e., feedwater) and heat removal (i.e, condenser) are lost;

- Events that do not cause any loss of the PCS (offsite power initially available);

- Events resulting in partial loss of PCS, that is, loss of feedwater, but with the condenser available for heat removal, offsite power is initially available; and

- Events resulting in an IORV in the primary system (offsite power initially available).

- Those events caused by a special initiator that cannot be classified into one of the above groups. More than one special initiating event group may be required.

For the NUREG/CR-4550 PWRs, the groups were differentiated by offsite power failure and whether the PCS is available or unavailable. The following transient groups were then identified:

PWR Groups

- Events resulting in an immediate LOSP;
- Events resulting in an immediate loss of the PCS (offsite power initially available);
- Events that do not cause any loss of PCS (offsite oower initially available); and
- Those events caused by a special initiator that can not be classified into one of the above groups. More than one special initiating event group may be required.

The events listed in Table 3.2-1 are grouped into the above NUREG/CR-4550 categories as shown below in Table 3.2-3. The grouping is reviewed to determine if any plant-specific information would cause the generic events to be regrouped. A generic event is removed if it cannot occur at the plant. However, similar events (i.e., similar to the generic events) which may occur at the plant are included. For example, at a plant the generic event, loss of an AC bus, cannot occur; therefore, it is not included in the grouping. But, plant-specific information indicates that the similar event, loss of a DC bus (which was not in the generic event groups) can occur and should be included. Otherwise, the analyst is falsely lowering the frequency.

If plant-specific data are not available to estimate the initiating event group frequencies (see Section 8), then the analyst must rely on generic data. The frequency for each initiating event from Reference 15 is also listed below in Table 3.2-3.

In Step 3.2c, the analyst determined whether or not there were any special initiators. If a special initiator has the same effect on the plant as one of the above transients, it is included in that grouping. If not, it forms a new transient group.

3.3 Initiating Event Nomenclature

The nomenclature for the initiating events is listed below.

BWR Events

T1 -- Transient caused by LOSP.
T2 -- Transient without PCS available (and offsite power initially available).
T3a -- Transient with PCS available (and offsite power initially available).
T3b -- Transient with feedwater lost, but condenser available (and offsite power initially available).

Table 3.2-3
BWR and PWR Generic Transient Groups

Reactor/Group	Table 3.2-1 Event	Initiating Event	Frequency/ Reactor Year
BWR Groups*			
LOSP**	31.	LOSP	0.08
	32.	Loss of auxiliary power (transformer)	0.02
		Total	0.10
Loss of PCS	2.	Electric load rejection with turbine bypass failure	0.004
	4.	Turbine trip with turbine bypass valve failure	0.004
	5.	MSIV closure	0.27
	6.	Inadvertent closure of one MSIV	0.21
	7.	Partial MSIV closure	0.06
	8.	Loss of condenser vacuum	0.41
	9.	Pressure regulator fails open	0.08
	10.	Pressure regulator fails closed	0.10
	12.	Turbine bypass fails open	0.04
	13.	Turbine bypass or control valves increase pressure (closed)	0.42
	37.	Cause unknown	0.06
		Total	1.66
IORV	11.	IORV	0.14
PCS Available	1.	Electric load rejection	0.45
	3.	Turbine trip	0.87
	14.	Recirculation control failure, increasing flow	0.18
	15.	Recirculation control failure, decreasing flow	0.05
	16.	One recirculation pump trip	0.06
	17.	Recirculation pump trip (all)	0.03
	18.	Abnormal startup of idle recirculation pump	0.02
	19.	Recirculation pump seizure	0.004
	20.	FW--increasing flow at power	0.14

Table 3.2-3
BWR and PWR Generic Transient Groups (Continued)

Reactor/Group	Table 3.2-1 Event	Initiating Event	Frequency/ Reactor Year
BWR Groups*			
PCS Available (Cont.)	21.	Loss of FW heater	0.02
	23.	Trip of one FW or condensate pump	0.20
	27.	Rod withdrawal at power	0.01
	29.	Inadvertent insertion of rods	0.06
	30.	Detected fault in RPS	0.05
	33.	Inadvertent startup of HPCI/HPCS	0.01
	34.	Scram from plant occurrences	0.58
	35.	Spurious trip via instrumentation, RPS fault	1.11
	36.	Manual scram, no out-of-tolerance condition	0.87
		Group Total	4.71
FW Lost but Condenser Available	22.	Loss of all FW flow	0.07
	24.	FW, low flow	0.49
		Group Total	0.56
PWR Groups*,*			
LOSP**	35.	Loss of offsite power	0.15
			0.15
Loss of PCS	9.	Inadvertent safety injection signal	0.05
	16.	Total loss of FW flow (all loops)	0.16
	18.	Closure of all MSIV	0.04
	20.	Increase in FW flow (all loops)	0.02
	21.	FW flow instability--operator error	0.29
	22.	FW flow instability--miscellaneous mechanical cause	0.34
	24.	Loss of all condensate pumps	0.01
	25.	Loss of condenser vacuum	0.14
	30.	Loss of circulating water	0.05
		Group Total	1.10

Table 3.2-3
BWR and PWR Generic Transient Groups (Continued)

Reactor/Group	Table 3.2-1 Event	Initiating Event	Frequency/ Reactor Year
PWR Groups*,* **			
PCS Available	1.	Loss of RCS flow (one loop)	0.28
	2.	Uncontrolled rod withdrawal	0.01
	3.	CRD mechanical problems and/or rod drop	0.50
	4.	Leakage for control rods	0.02
	5.	Leakage in primary system	0.05
	6.	Low pressurizer pressure	0.03
	7.	Pressurizer leakage	0.005
	8.	High pressurizer pressure	0.03
	10.	Containment pressure problems	0.005
	11.	CVCS malfunction--boron dilution	0.03
	12.	Pressure/temperature /power imbalance--rod position error	0.13
	13.	Startup of inactive coolant pump	0.002
	14.	Total loss of RCS flow	0.03
	15.	Loss or reduction in FW flow (one loop)	1.50
	17.	Full or partial closure of MSIV (one loop)	0.17
	19.	Increase in FW flow (one loop)	0.44
	23.	Loss of Condensate pumps (one loop)	0.07
	26.	Steam generator leakage	0.03
	27.	Condenser leakage	0.04
	28.	Miscellaneous leakage in secondary system	0.09
	29.	Sudden opening of steam relief valves	0.02
	33.	Turbine trip, throttle valve closure, EHC problems	1.19
	34.	Generator trip or generator caused faults	0.46
	36.	Pressurizer spray failure	0.03
	38.	Spurious trips--cause unknown	0.08
	39.	Auto trip--no transient condition	1.49
	40.	Manual trip--no transient condition	0.47
		Group Total	7.20

Footnotes for Table 3.2-3

* The core damage frequency is estimated for those times when the reactor (i.e., plant) is at power and only considering internal initiators. Therefore, those events that occur at other times and that are external events are not included. These events include the following:

BWR 25. Low FW flow during startup or shutdown;
26. High FW flow during startup or shutdown; and
28. High flux from rod withdrawal at startup.
PWR 41. Fire within plant.

** In estimating the frequency of LOSP, an analysis has been performed evaluating data more recent than Reference 15. This evaluation (reported in Reference 20) has established that the differences experienced site to site preclude the establishment of a generic LOSP frequency. Typical results for a plant specific analysis (in this case, Peach Bottom) are shown in Figure 3.2-2.

*** Certain of the PWR events cannot be classified into any of the above groups. They are, in actuality, more of a special initiator. These include the following:

31. Loss of component cooling,
32. Loss of service water system, and
37. Loss of power to necessary plant systems.

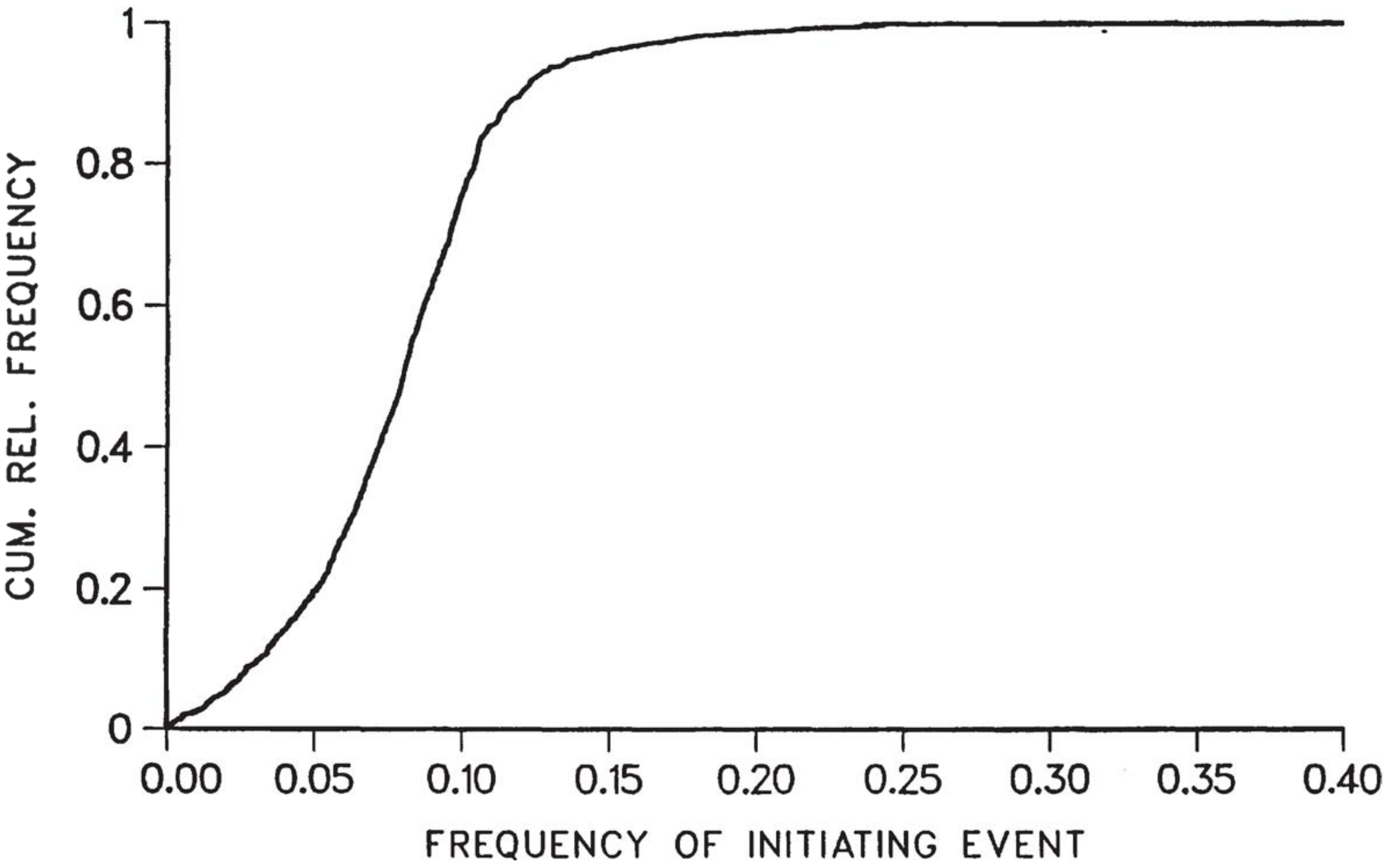


Figure 3.2-2. Distribution of LOSP Initiating Frequency for Peach Bottom (Reference 20)

T3c -- Transient with an IORV in the primary system (and offsite power initially available).

TAC/x-- Transient with loss of AC bus ‘x’.

TDC/x-- Transient with loss of DC bus ‘x’.

Tx -- Transient caused by some other plant system failure.

A -- Large LOCA.

S1 -- Intermediate LOCA.

S2 -- Small LOCA.

S3 -- Small Small LOCA.

‘V’ -- Interfacing LOCA.

‘R’ -- Vessel rupture.

PWR Events

T1 -- Transient caused by LOSP.

T2 -- Transient without PCS available (and offsite power initially available).

T3 -- Transient with PCS available (and offsite power initially available).

TAC/x-- Transient with loss of AC bus ‘x’.

TDC/x-- Transient with loss of DC bus ‘x’.

Tx -- Transient caused by some other plant system failure.

A -- Large LOCA.

S1 -- Intermediate LOCA.

S2 -- Small LOCA.

S3 -- Small Small LOCA.

V -- Interfacing LOCA.

‘R’ -- Vessel rupture.

If, after examining plant-specific information, new transient or LOCA categories are added, the analyst should follow the general nomenclature, that is, using ‘T’ to designate a transient and ‘S’ to designate a LOCA. For example, SGTR does not fall into any of the regular PWR transient categories; therefore, it requires its own grouping. A possible transient category added to represent SGTR would be ‘T4’.

3.4 Initiating Event Recommended Reporting

There are four items in this task that are generally reported. These include the following:

- Sources of Information. A list or general description of the documentation/information that was used in the task is discussed.

- Assumptions. Any assumptions that were made in performing the initiating event analysis are discussed. Their potential impact on the final results should also be addressed.

- Events. The initiating events examined are discussed. This discussion should address both the events retained for further examination and those that were eliminated and the rationale.

- Success Criteria. The success criteria established for each initiating event group should be presented including the basis for the criteria.

- Event Frequencies. The frequencies estimated for each initiating event group are presented.

3.5 Example of Accident Sequence Initiating Event Analysis

An example for the development of a BWR initiating event analysis is presented in this subsection. The Peach Bottom NUREG/CR-4550[4] analysis is used to illustrate the steps in this task.

Step 3.1 Obtain Information

Information sources utilized to identify and group the accident sequence initiating events of Peach Bottom include:

- ASEP prior work
- WASH-1400[39]
- Grand Gulf RSSMAP[60]
- IREP Browns Ferry[29]
- Limerick PRA[66]
- Shoreham PRA
- GE-NEDO 24708A[16]
- PECO monthly "hi-spot" reports
- Peach Bottom Updated FSAR
- BWR Event "V" presentation by J. Minarick to ASEP Senior Consultant Group

Part of the above information, coupled with information gained during the initial plant visit and subsequent telephone conversations, was used to identify possible special initiators, which are events not typically included in generic lists of initiating events.

Step 3.2 Identify Initiating Events

Initiating events disrupt normal conditions in the plant and can potentially result in a number of accident sequences. The initiating events were defined as discussed in Step 3.2 of Section 3.2.

Step 3.2a Identify LOCA Sizes

From a review of the information sources identified in Step 3.1, it was found that the three LOCA sizes identified in Section 3.2 were appropriate. These sizes were based on different mitigation success criteria as was done in the original WASH-1400 study of Peach Bottom. No further work was required on the primary system LOCAs at this point in the analysis. The potential for interfacing system LOCAs was also examined in this study. Based on actual operating experience, the high to low pressure interface in the LPCS and RHR systems was reviewed to identify sources for a V sequence. Such a sequence has been examined and is included in the event tree analysis section.

An examination of possible LOCAs within mitigating systems was also performed. One LOCA source appeared more likely since it could cause a plant trip and affect multiple safety systems. This was a LOCA in the Normal Service Water (NSW) system piping where the piping interfaces with the Emergency Service Water (ESW) system piping to feed a number of core cooling loads and the diesel generators. A pipe break in this location could disturb normal service water flow so as to cause a plant trip and possible loss of the NSW system. Subsequent ESW initiation would feed the break instead of cooling certain safety system loads. However, since (a) operation of the High Pressure Service Water (HPSW) system is unaffected (no dependency on the NSW or ESW system), (b) HPCI and RCIC are only indirectly affected by room cooling (systems could run 10 or more hours without NSW or ESW), (c) such a break could be isolated, and (d) the probability of a LOCA occurring in a specific location in a low pressure system is considered relatively low (<1E-6), this initiator was determined to be less important than other initiators of interest. This conclusion is consistent with the scope of LOCAs analyzed in other PRAs.

Step 3.2b Identify Transient Events

Peach Bottom Units 2 and 3 have approximately 14 years of operating history; therefore, the generic data on initiating events presented in Section 3.2 was replaced where appropriate. The operating history of the two units was reviewed, and events that had occurred at either plant that resulted in a plant trip (whether automatic or manual) were identified. These events were defined as the initiating transient events.

Step 3.2c Identify Special Events

Special initiators and support system failures acting as initiators were identified for inclusion in the Peach Bottom analysis. During the review of the Peach Bottom electrical design, it was noted that safety and non-safety loads are eventually shared off buses that ultimately derive their power from the 4160 VAC and 125/250 VDC safety buses. Loss of these buses potentially could cause a plant trip and simultaneous degradation of safety systems. An actual occurrence of a plant trip due to the de-energization of a 4160 VAC safety bus and the sharing of safety and non-safety loads at Peach Bottom was used as sufficient argument to treat the loss of any buses of this type as a special initiator. These two special initiators were identified and named TAC and TDC initiators.

A search for other special initiators was performed which included three major categories: loss of a service water system, loss of instrument air, and loss of heating and ventilation equipment. Potential failures in the NSW system, the Turbine Building Cooling Water (TBCW) system, the Reactor Building Cooling Water (RBCW) system, the ESW system, and the HPSW system were reviewed as possible special initiators. Pipe breaks, the potential for causing a plant trip, and effects on the safety systems were considered in the review. No special initiators worthy of further examination involving these systems were identified, based in part on the generally sharp separation between the safety and non-safety cooling water systems (ESW, HPSW, and RBCW are standby safety systems; NSW and TBCW are normally operating, non-safety systems) and, thus, the unlikely possibility of a simultaneous plant trip and degradation of plant systems. The probability of flooding is small based on the low pressure operation of these systems and their locations with respect to most other safety systems.

Loss of instrument air/nitrogen can cause a plant trip through the dependency of the Power Conversion System (PCS), drywell coolers, and area ventilation systems on air supplies. Air or nitrogen is also supplied to the following accident mitigation systems: (1) the Automatic Depressurization system (ADS) valves, (2) the Emergency Ventilation system (EVS) dampers which provide room cooling for the diesel generators, switchgear, and DC systems, (3) the CRD full flow path, (4) some containment vent valves used for containment venting, and (5) the MSIVs. However, none of these systems presents a problem, for the following reasons. The ADS and MSIV valves can remain open for significant periods of time since they are backed-up by accumulators and other air/nitrogen supplies. The critical EVS dampers fail open. The CRD system can achieve near full flow conditions without air through an alternate passive path. Containment vent valves each have a separate air bottle which can be used to operate the valve locally. The HPCI, RCIC, LPCI, LPCS, and HPSW systems are available to operate given a loss of instrument air. These points, along with the expected low probability of loss of air/nitrogen as an initiator, were used to eliminate loss of air/nitrogen as a special initiator on probabilistic grounds.

Heating and ventilation systems were reviewed but discarded as possible special initiators. This is based on the degree of separation in the design of these systems at Peach Bottom, the low heat loads in critical equipment areas such as the AC bus rooms, and the generally slow effects of loss of heating and ventilation equipment which allow time for corrective action before a plant trip would occur. Additionally, PECO performed analyses as part of the original FSAR to show that, for example, equipment in the control room would not reach equipment qualification limits, even with total loss of HVAC.

Those special initiating events that were reviewed and eliminated from the analysis are given in Table 3.5-1.

Step 3.3. Identify Plant Safety Functions

Plant safety functions required to mitigate initiating events for Peach Bottom are the same as those defined in Table 3.2-2. No additional analyses are required. Those functions are:

- For LOCAs; Reactor Subcriticality, Emergency Core Cooling; Early Containment Overpressure Protection, and Late Containment Overpressure Protection

- For Transients; Reactor Subcriticality, Reactor Coolant System Overpressure Protection, Emergency Core Cooling, and Containment Overpressure Protection

Step 3.4 Identify Plant Systems

Peach Bottom plant documentation was reviewed and discussions with utility personnel were held to identify systems capable of performing each safety function. The capacity and operating conditions of each of these systems were then established to ensure they could meet the functional needs. This information is summarized in Table 3.5-2.

Step 3.5 Determine Success Criteria

The criteria that must be met to successfully mitigate the effects of the Peach Bottom initiating events were developed in several steps. Past PRAs and other related studies (e.g., Shoreham and Limerick[66] PRAs and General Electric NEDO studies[16], etc.) were reviewed for applicability. A significant number of the success criteria for core cooling and containment overpressure protection were established based upon the thermal-hydraulic calculations from those references. However, because one objective of the overall study was to perform a realistic analysis, it was appropriate to give credit for all systems where possible. Therefore, some plant-specific calculations were performed to determine if specific systems met the success criteria.

For example, from past studies, the core cooling success criterion for transients was approximately 300 gpm. A calculation was performed to determine if the control rod drive system which could provide 210 gpm was, in fact, sufficient. Another example involves containment venting. Calculations were performed to define what venting capacity was required for LOCAs, transients, and ATWS, respectively, in order to protect the containment from overpressurizing.

The success criteria are summarized in Table 3.5-3.

Step 3.6 Determine LOCA Break Sizes

Using the LOCA definitions from Step 3.2a, the success criteria from Step 3.5 and information from past studies, the break sizes for Peach Bottom LOCA initiating events were defined. The resulting break sizes were as follows:

- Large LOCA - greater than 0.1 sq. ft.

- Intermediate LOCA - 0.004 to 0.1 sq. ft. - liquid
  0.05 to 0.1 sq. ft. - steam

- Small LOCA - less than 0.004 sq. ft. - liquid
  less than 0.05 sq. ft. - steam

- Small-Small LOCA - 50 to 100 gpm (seal LOCA)

- Interfacing LOCA - breach of a high to low pressure interface

Step 3.7 Determine Transient Event Groups

The transient groups (i.e., T1, T2, T3a, etc.) were defined in Step 3.7 of Section 3.2. The initiating events that were identified in Step 3.2b of this section were reviewed to determine to which group they belonged. For example, one such event that had tripped the plant at Peach Bottom was loss of one feedwater pump. This initiating event resulted in a turbine trip with partial loss of feedwater, but PCS was still available; therefore, this event was placed in T3a (PCS available) group. All other events were similarly examined and classified.

The final list of initiating events requiring further analysis for Peach Bottom and associated frequencies is given in Table 3.5-4.

Table 3.5-1

Initiators Reviewed and Eliminated From Further Analysis

INITIATOR TYPE	PRIMARY REASONS FOR ELIMINATION
LOCAs in Secondary Side of Plant	• Isolation potential
LOCAs in Mitigating Systems	• Probability of occurrence • Isolation potential • Redundancy provided by other systems to prevent core damage
Reactor Vessel Rupture*	• Qualitative discussion only
Loss of Service Water Systems	• Redundancy of systems • Functional and spatial separation of normally operating vs. standby systems • Probability of occurrence • Isolation potential
Loss of Instrument Air/ Nitrogen	• Ability of most key systems to adequately perform without air/nitrogen • Probability of occurrence
Loss of HVAC	• Redundancy in equipment • Relatively low heat loads in critical areas • Slow effects allow recovery before plant trip • PECO analyses and historical performance

* This event was initially screened out based on low frequency of occurrence. However, because of the high risk potential of the event, that decision is now the subject of debate and should be reconsidered in future PRAs.

Table 3.5-2
Safety Function System Requirements

Safety Function	Plant System	Capacity/Operating Conditions
Reactor Subcriticality	Reactor Protection System	
Reactor Coolant System Overpressure Protection (Transient only)	Safety Relief Valves	
Emergency Core Cooling	High Pressure Coolant Injection	5000 gpm/high pressure
	Reactor Core Isolation Cooling	600 gpm/high pressure
	Low Pressure Coolant Injection	10,000 gpm per pump/low pressure
	Low Pressure Core Spray	3125 gpm per pump/low pressure
	Control Rod Drive	210 gpm, reactor pressurized/high pressure 300 gpm, reactor depressurized/ high pressure
	Condensate	10870 gpm/low pressure
	High Pressure Service Water	4500 gpm per pump/low pressure
Containment Overpressure Protection	Suppression Pool Cooling	10,000 gpm per pump/low pressure
	Shutdown Cooling	10,000 gpm per pump/low pressure
	Containment Spray	10,000 gpm per pump/low pressure
	Primary Containment Venting	

Table 3.5-3
Success Criteria Summary Information

INITIATOR	REACTOR SUBCRITICAL	EMERGENCY CORE COOLING	EARLY CONTAINMENT OVERPRESSURE PROTECTION	LATE CONTAINMENT OVERPRESSURE PROTECTION
A	RPS or ARI & RPT or Manual Rods and RPT	1 of 4 LPCI or any 2 LPCS pumps	VSS	1 of 4 RHR & HtX (SPC or Spray modes) and associated HPSW or Containment Venting
S1	RPS or ARI & RPT or Manual Rods and RPT	HPCI (2 hours only) or DEP w/3 valves* and Any 2 LPCS pumps or DEP w/3 valves* and 1 of 4 LPCI or DEP w/3 valves* and 1 HPSW (inject mode)	VSS	1 of 4 RHR & HtX (SPC or Spray modes) and associated HPSW or Containment Venting

* Conservative for most breaks.

Table 3.5-3
Success Criteria Summary Information (Continued)

INITIATOR	REACTOR SUBCRITICAL	EMERGENCY CORE COOLING	EARLY CONTAINMENT OVERPRESSURE PROTECTION	LATE CONTAINMENT OVERPRESSURE PROTECTION
S2	RPS or ARI & RPT or Manual Rods and RPT or Timely SLC and RPT (for steam break)	HPCI or RCIC or 1 FW or DEP w/3 valves and Any 2 LPCS pumps or DEP w/3 valves and 1 of 4 LPCI or DEP w/3 valves and 1 Condensate or DEP w/3 valves and 1 HPSW (inject mode)	VSS	1 of 4 RHR & HtX (SPC or Spray Modes) and associated HPSW or Containment Venting or PCS
S3	If detected and isolated, treat like T3. If not isolated, treat like S2 liquid LOCA.			

Table 3.5-3
Success Criteria Summary Information (Continued)

INITIATOR	REACTOR SUBCRITICAL	RCS OVERPRESSURE PROTECTION	EMERGENCY CORE COOLING	CONTAINMENT OVERPRESSURE PROTECTION
T1	RPS or ARI & RPT or Manual Rods and RPT or Timely SLC and RPT	SRVs open & close	HPCI or RCIC or CRD (~full flow) or 1 FW [see Note (a)] or DEP w/3 valves and Any 2 LPCS pumps or DEP w/3 valves and 1 of 4 LPCI or DEP w/3 valves and 1 Condensate [see Note (a)] or DEP w/3 valves and 1 HPSW (inject mode)	1 of 4 RHR & HtX (SDC, SPC, Spray Modes) and associated HPSW or PCS [see Note (a)] or Containment Venting

NOTE:
(a) Only available if offsite power is restored.

Table 3.5-3
Success Criteria Summary Information (Continued)

INITIATOR	REACTOR SUBCRITICAL	RCS OVERPRESSURE PROTECTION	EMERGENCY CORE COOLING	CONTAINMENT OVERPRESSURE PROTECTION
T2	RPS or ARI & RPT or Manual Rods and RPT or Timely SLC and RPT	SRVs open & close	HPCI or RCIC or CRD (~full flow) or 1 FW [see Note (a)] or DEP w/3 valves and Any 2 LPCS pumps or DEP w/3 valves and 1 of 4 LPCI or DEP w/3 valves and 1 Condensate or DEP w/3 valves and 1 HPSW (inject mode)	1 of 4 RHR & HtX (SDC, SPC, Spray Modes) and associated HPSW or PCS [see Note (b)] or Containment Venting

NOTES:

(a) Since feedwater is likely lost as part of the T2 initiator, feedwater must first be restored.

(b) T2 is a loss of the PCS so the PCS must first be restored.

Table 3.5-3
Success Criteria Summary Information (Continued)

INITIATOR	REACTOR SUBCRITICAL	RCS OVERPRESSURE PROTECTION	EMERGENCY CORE COOLING	CONTAINMENT OVERPRESSURE PROTECTION
T3 types	RPS or ARI & RPT or Manual Rods and RPT or Timely SLC and RPT	PCS or SRVs open & close	HPCI or RCIC or CRD (~full flow) or 1 FW or DEP w/3 valves and Any 2 LPCS pumps or DEP w/3 valves and 1 of 4 LPCI or DEP w/3 valves and Condensate or DEP w/3 valves and 1 HPSW (inject mode)	1 of 4 RHR & HtX (SDC, SPC, Spray modes) and associated HPSW or PCS or Containment Venting

Table 3.5-3
Success Criteria Summary Information (Concluded)

INITIATOR	REACTOR SUBCRITICAL	RCS OVERPRESSURE PROTECTION	EMERGENCY CORE COOLING	CONTAINMENT OVERPRESSURE PROTECTION
TAC/X	Like T2 except Emergency Core Cooling & Residual Heat Removal have fewer AC pumps available to operate.			
TDC/X	Like T2 except Emergency Core Cooling & Residual Heat Removal have fewer AC pumps available to operate and HPCI or RCIC may be unavailable depending on which DC bus is affected.			

NOTE: Any transient with a stuck open relief valve will be treated as:

One valve stuck open ------- S2 steam LOCA

Two valves stuck open ------- S1 steam LOCA

Three valves stuck open ----- A steam LOCA

Table 3.5-4

Peach Bottom Initiating Events and Frequencies

INITIATOR NOMENCLATURE	DESCRIPTION	MEAN FREQUENCY (per year)
T1	Loss of offsite power (LOSP) transient	0.079
T2	Transient with the Power Conversion System (PCS) unavailable	0.05
T3A	Transient with the PCS initially available	2.5
T3B	Transient involving loss of feedwater (LOFW) but with the steam side of the PCS initially available	0.06
T3C	Transient due to an Inadvertent Open Relief Valve (IORV) in the primary system	0.19
TAC/x	Transient caused by loss of safety AC Bus "x"	5.0E-3
TDC/x	Transient caused by loss of safety DC BUS "x"	5.0E-3
A	Large LOCA	1.0E-4
S1	Intermediate LOCA	3.0E-4
S2	Small LOCA	3.0E-3
S3	Small-small LOCA	3.0E-2
"V"	Interfacing system LOCA	<1E-8

4. ACCIDENT SEQUENCE EVENT TREE ANALYSIS

The methodology used to perform the Accident Sequence Event Tree Analysis task is described in this section. A typical Probabilistic Risk Assessment (PRA) includes the evaluation of accident sequences which present the occurrence of initiating events followed by combinations of successful and unsuccessful responses of functions or systems. The combinations of systems, and the functions they perform, determine the status of the core (i.e., core damage), containment (i.e., containment failure), or both (i.e., core damage prior to containment failure). Event tree models (bimodal logic diagrams) are constructed to represent logically the above combinations of functional and systemic responses of the plant to the initiating events. Each unique set of responses is called a sequence.

4.1 Accident Sequence Event Tree Assumptions And Limitations

In general, both functional and systemic event trees are developed in a PRA. The construction of functional event trees provides additional traceability of the analysis. However, for an abbreviated analyses, the functions are identified (see Section 3), but the corresponding functional event trees are not explicitly drawn.

The delineation of the accident sequence ends with the determination of the status of the core as safe or damaged. The core is defined to be in a safe condition when the consequences of the radionuclide releases from the damaged fuel would be negligible. Realistically, core damage occurs when the allowable peak fuel cladding temperature is reached. However, using this definition involves detailed analyses beyond the scope of many studies, so a more conservative definition is often employed. For the Boiling Water Reactors (BWRs) in NUREG-1150, core damage is assumed to occur when the reactor water level is less than two feet above the bottom of the active fuel. Because Pressurized Water Reactors (PWRs) are not designed to allow steam cooling, core damage is assumed to occur at the time at which the top of the active fuel is uncovered. As knowledge of accident progression in the core evolves, less conservative assumptions concerning core damage may be used.

Plant system components modeled in a PRA are assumed to be fully operational or non-operational. Differentiation is not made between full and partial operation of a component. Therefore, PRA methodology does not usually take into account degraded (e.g., valve partially open) or enhanced performance of a system component (e.g., pump operating near runout conditions), only operation at nominal performance or inoperable.

The front-line systems used as event tree headings include only those systems present in the plant emergency operating procedures for responding to the initiating events defined for the analysis.

The Anticipated Transient Without Scram (ATWS) accident sequences for the BWRs are not always fully delineated. ATWS sequences in which the functions; reactor subcriticality, Reactor Coolant System (RCS) overpressure protection and inventory control, and core heating are successful, are assumed to be mitigated. Even if failure of the containment overpressure protection function occurs in an ATWS sequence following success of the other functions, the sequence frequency is often below the risk-significant cut-off value, and thus the sequence would be screened from the analysis.

ATWS sequences for PWRs are treated similar to those for BWRs. As with the BWRs, low sequence probabilities for ATWS scenarios prior to the need for containment overpressure protection would produce non-dominant sequences even if failure of containment overpressure protection was considered.

4.2 Accident Sequence Event Tree Development

The event trees are logic diagrams at the system level of detail that describe the possible sequences of events that follow each initiator. The objective in developing the accident sequence event trees is to define all the possible combinations of successful and unsuccessful system responses to an initiating event. The event tree analysis tracks individual system successes and failures until it is decided whether the core is safe or damaged. The analysis may also display the status of other systems (e.g., containment overpressure protection) so as to help describe the state of the plant for the subsequent accident progression and consequence analyses. Therefore, the event trees developed will reflect system responses that can prevent or mitigate core damage and containment failure, and in some instances influence the actual consequences of the accident. The construction of the event trees involves several steps that are illustrated in Figure 4.2-1 and described below.

Step 4.1. Obtain Information

In this step the analyst identifies and gathers the information required to delineate the accident sequences. It should be noted that the majority of the information are outputs of the Accident Sequence Initiating Event Analysis task (see Section 3). The information required is as follows:

- List of Loss of Coolant Accident (LOCA) and transient initiating event groups (see Section 3),
- System success criteria for responding to LOCA and transient initiating event groups (see Section 3), and
- Various plant documents (e.g., system descriptions, operating procedures, etc.) and analyses (e.g., thermal-hydraulic analyses* concerning core, containment responses) information.

* Actual thermal-hydraulics calculations are performed when past studies do not provide adequate information.

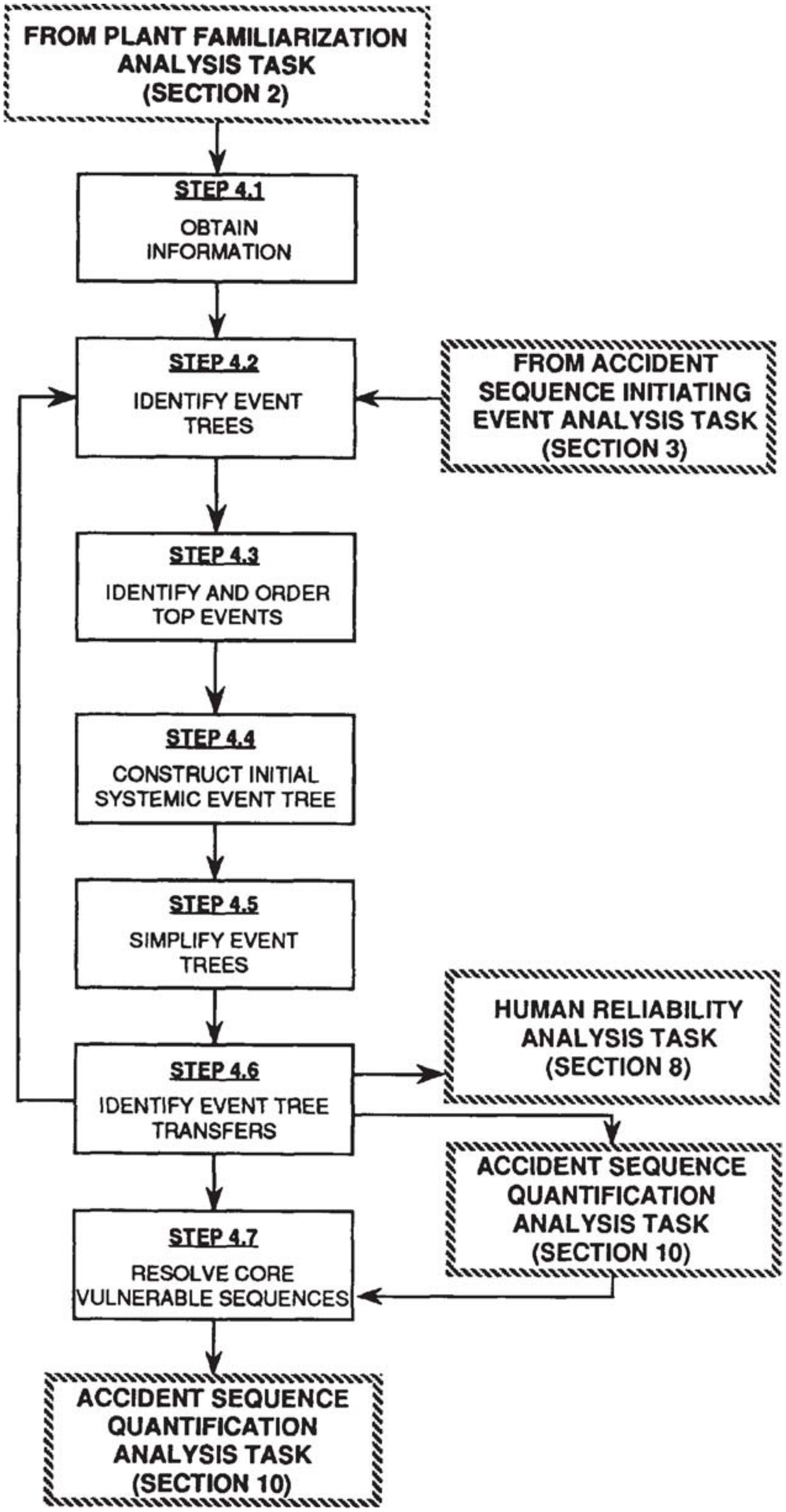

FROM PLANT FAMILIARIZATION ANALYSIS TASK (SECTION 2)
STEP 4.1
OBTAIN INFORMATION
STEP 4.2
IDENTIFY EVENT TREES
FROM ACCIDENT SEQUENCE INITIATING EVENT ANALYSIS TASK (SECTION 3)
STEP 4.3
IDENTIFY AND ORDER TOP EVENTS
STEP 4.4
CONSTRUCT INITIAL SYSTEMIC EVENT TREE
STEP 4.5
SIMPLIFY EVENT TREES
HUMAN RELIABILITY ANALYSIS TASK (SECTION 8)
STEP 4.6
IDENTIFY EVENT TREE TRANSFERS
ACCIDENT SEQUENCE QUANTIFICATION ANALYSIS TASK (SECTION 10)
STEP 4.7
RESOLVE CORE VULNERABLE SEQUENCES
ACCIDENT SEQUENCE QUANTIFICATION ANALYSIS TASK (SECTION 10)

Figure 4.2-1. Step Relationship for Accident Sequence Event Tree Analysis

Step 4.2. Identify Event Trees

In this step the analyst identifies the initiating events for which separate event trees must be developed and the accident sequences delineated. In general, a separate event tree will be developed for each LOCA initiating event group, identified in Step 3.6 in Section 3. Separate event trees are also developed for each transient initiating event group and for each special initiator identified in Step 3.7 of Section 3.

Step 4.3. Identify and Order Top Events

In this step the analyst identifies and orders the top events for each event tree based on the functions, and their success criteria, required to mitigate the initiating event. The systems that are required to accomplish each function become the top events. These events (systems) are identified in Step 3.5 of Section 3 as part of the success criteria evaluation.

Once the top events have been identified, the analyst must order them. Generally, this order is temporal. In ordering the events, the analyst first considers the functions. These functions are ordered by the time at which each function is initially required to be accomplished. For example, consider a transient at a BWR. The functions that must be accomplished are:

- Emergency Core Cooling,
- Containment Overpressure Protection,
- RCS Overpressure Protection, and
- Reactor Subcriticality.

These functions are ordered by considering the time at which conditions are generated that require the function to be accomplished. For example, consider a BWR transient event resulting from a Main Steam Isolation Valve (MSIV) closure. The first response after the initiator (at approximately 1 second) is a turbine trip followed by a reactor scram. The reactor scram accomplishes the reactor subcriticality function. Due to the MSIV closure, there is a pressure surge (at approximately 1-to-30 seconds) which requires the RCS overpressure protection function to be accomplished. In addition, coolant makeup (i.e., feedwater) is lost as a result of the MSIV closure. Water level in the vessel decreases and coolant makeup providing the core cooling function is required at about 10-to-20 minutes. Finally, the decay heat is transferred to the containment since the MSIVs are closed. The containment heat removal function is required anywhere from approximately 10 minutes to 7-to-9 hours.

Based upon the above development, the functions are then ordered as follows:

(1) Reactor Subcriticality,
(2) RCS Overpressure Protection,
(3) Emergency Core Cooling, and
(4) Containment Overpressure Protection.

With the functions ordered, the analyst can then order the top events per those safety functions. The events within each safety function are ordered while keeping the functions as ordered earlier. Therefore, the first set of top events in the event tree will be those required to accomplish the function ordered first. The second set of top events will be those for the second function, and so on until all the functions are taken into account.

In the transient example above, the first function is reactor subcriticality. The first set of events appearing in this transient tree would then be those required to achieve subcriticality. This order is also determined temporally, and the ordering is based upon the time any of the events would be required or expected to initiate, either automatically or by operator action. This information is derived from plant-specific documentation which gives the conditions for automatic initiation and manual actuation. However, if a condition actuates more than one event simultaneously, the ordering of these events is generally decided based on the plant procedures -- which event the procedure instructs the operator to actuate first.

With the identification and ordering of the top events for each event tree, the analyst is now ready to delineate the accident sequences.

Step 4.4. Construct Initial Systemic Event Tree

In this step the analyst constructs an event tree for each initiating event group by delineating the accident sequences. An event tree is constructed for each initiating event group or category since each group is based on an unique set of success criteria. Therefore, each tree has an unique structure that reflects the different mitigating system requirements (i.e. success criteria). To develop the accident sequences, the success criteria (from Step 3.5 of Section 3) and system dependencies are incorporated into success and failure decision branches using the appropriate top events until the initiating event is either mitigated or results in core damage or core vulnerability.

The methodology used is based on the 'large fault tree - small event tree' approach. The event trees provide a logical framework for the sequence progression, but the details of specific system failures are developed in the fault trees (see Section 5, Systems Analysis). The fault tree headings should be precisely related to the system success criteria specified for the event tree. It should be noted that the order of the events in the tree may be modified through the dependency analysis to more accurately reflect the sequence of events. Modification of the ordering of events may also produce a smaller number of sequences to be evaluated.

The delineation of the accident sequences includes the incorporation of three types of dependencies into the success criteria of the initiator under consideration.

Type 1 -- This dependency incorporates the functional success criteria into an event tree structure. A functional event tree is constructed to incorporate this type of dependency. At each decision point in the tree, the functional success criteria are considered in determining whether or not an event should be included within the function. That is, all the events for one function may or may not be considered because the failure of a previous function either (1) causes the accident sequence to result in core damage regardless of the function under consideration, or (2) changes the success criteria of the remaining functions.

In the former case, those functions that have no effect in preventing core damage once another function has failed are identified. For these situations, events associated with these 'ineffective functions' are not considered in the delineation of the accident sequence. In the latter case, for a transient example, one failure of RCS overpressure protection results in Stuck Open Relief Valves (SORVs). The success criteria of core cooling is different for a transient than for an SORV since inventory is now being lost. In this situation, the success criteria changes and the accident sequence is not further delineated on this event tree. The sequence transfers to another tree (see Step 4.6.).

At this point, a functional event tree has been constructed. This tree is next expanded to include explicitly the systems required. This is done by incorporating two other types of dependencies into the success criteria.

Type 2 -- This dependency incorporates the systemic success criteria of each safety function into the event tree structure. At each decision point, the systemic success criteria are considered in determining whether the event should be included within the function. If the top event under consideration meets the success criteria, then the remaining events of the function are not considered. For example, consider the top events for the core cooling function. If the first event meets the success criteria, the remaining events of that function are not considered. The first event of the next function is the next decision point.

At this point, the analyst has expanded the functional event tree into a systemic event tree. However, there is a third dependency that must be addressed for the accident sequences to accurately represent the plant response.

Type 3 -- This dependency incorporates the phenomenological conditions created by the accident sequence into the event tree structure. How a function is accomplished or the failure of a function has the potential to effect the continued success of a previous event. This type of dependency is identified and incorporated into the accident sequence. These dependencies are identified by defining the conditions that (1) can cause each event to fail, and (2) are created by the success or failure of the events of the accident sequence. At each decision point, the analyst establishes the accident sequence conditions (e.g., vessel pressure, containment temperature, etc.) and any adverse effects they may have on previously successful events. If the event providing core cooling fails because of accident sequence conditions, the sequence does not necessarily result in core damage. Other systems may be available to continue the cooling function. Such a sequence is said to be a core vulnerable sequence.

The core vulnerable sequences are not resolved in this step. Those events which must occur at this point to mitigate the core vulnerable sequence (i.e., prevent core damage) are not included. The core vulnerable sequences are only resolved if they have the potential to result in dominance (see Section 10). Therefore, each accident sequence (at this point) is identified by one of the following:

O.K. -- core damage is successfully prevented,

CD -- core damage occurs, or

CV -- the core is vulnerable.

For each accident sequence, the analyst also identifies the status of the containment as follows:

CtF -- containment failure occurs,

CtVt -- containment venting occurs, or

CtV -- the containment is vulnerable.

The status of the containment at the time of core damage is important in determining the plant damage state (see Section 11) and ultimately the source term. Therefore, it is important that the analyst identify the state of the containment at the time of core damage. For example, the designator CtF-CD signifies that containment failure occurs prior to core damage, whereas CD-CtF signifies that core damage occurs prior to any containment failure.

The core vulnerable designation (CV) is a temporary designation for sequences in which injection is initially successful, but containment heat removal has failed. Subsequent containment failure may or may not lead to injection failure and core damage, depending on the response of the injection systems to the containment failure event. The containment vulnerable designation (CtV) is used when the containment is intact at the time of core damage but its integrity might be challenged by the damaged core.

Other types of dependencies are included in the Systems Analysis task, as discussed in Sections 5 and 6. This involves consideration of the support systems (e.g., electric power, service water) that are required for the front-line systems to succeed. Such dependencies are included in the front-line system models to properly account for their potential contribution to the core damage frequency. Also included is consideration of the potential for failure related to common causes such as manufacturing defects.

Step 4.5. Simplify Event Trees

In this step the analyst reviews each event tree to ascertain whether the structure could be simplified while retaining system dependencies. This simplification is usually performed by the reordering of the top events. It should be noted that this is not an arbitrary decision. Care is taken so that if simplification is performed, the sequence development is still the same.

For example, at a BWR the operator must first ensure that the low pressure systems are operating before he is allowed to depressurize the reactor vessel. Therefore, the low pressure injection system top events would be placed before the reactor depressurization event. However, if the reactor depressurization event is ordered first, the number of sequences depicted by the event tree is reduced without any unique combinations of system successes and failures (i.e., sequences) being lost.

Additionally, if the analyst can determine that the frequency of a partially developed sequence has a low probability (i.e., its contribution is probabilistically insignificant), it need not be further developed.

Step 4.6. Identify Event Tree Transfers

In this step the analyst identifies transfers to different event trees. In some cases, after the initiating event and failure of other events, the success criteria for the sequence changes from that originally defined for the initiating event. At this point, the sequence will transfer to a different event tree. If the changed success criteria are the same as that required for one of the other initiating events, the sequence is transferred to that tree. If the success criteria are not the same as for any other initiator, then an entirely new event tree is required. In delineating the sequences for this new event tree, the analyst follows the same steps described earlier.

For instance, consider a BWR and a transient initiator with a sequence involving a subsequent stuck open relief valve. The original success criteria for the remaining functions no longer apply. The new success criteria for this sequence are the same as for a LOCA event, therefore, this sequence is transferred to that tree. However, for a transient where the reactor protection system has failed, the new success criteria are not the same as those for any of the initiators. A new event tree (i.e., ATWS) is required for this sequence.

Step 4.7. Resolve Core Vulnerable Sequences

In this step the analyst resolves core vulnerable sequences which have the potential to result in dominance. After the initial quantification (see Section 10), those sequences that are identified as having the potential to result in dominance are resolved. The analyst decides if the core coolant function, which was lost because of phenomenological conditions, can still be accomplished. In making this decision, the analyst first determines whether the phenomenological conditions remain constant. The analyst then determines if the core cooling systems which have not been considered previously (i.e., systems that should be available) can operate and prevent core damage from occurring, given the resolution of the phenomenological conditions.

For example, consider a BWR where the initiating event resulted in closure of the main steam isolation valves. All of the decay heat is transferred to the suppression pool. If the suppression pool cooling system of the late containment overpressure protection function fails, the temperature of the pool increases. If the system performing the core cooling function uses the pool as its suction source and the pump is not designed to handle such high temperature water, the system fails. If (1) the pool temperature does not decrease, (2) all other available systems also depend on the pool, and (3) these systems can not pump such hot water, then core damage occurs. However, if there are other systems that are not dependent on the suppression pool or can pump hot water, then the core vulnerability might be mitigated.

4.3 Accident Sequence Event Tree Nomenclature

The nomenclature used in the accident sequence event tree analysis is listed in Table 4.3-1.

4.4 Accident Sequence Event Tree Recommended Reporting

Three items are generally reported which result from an Accident Sequence Event Tree Analysis. These include the following:

- Assumptions. Any assumptions made in developing the accident sequence event trees are discussed including how they could effect the final results.

- Event Tree. Event trees for each initiating event are presented in graphic form to show all sequences that could potentially be dominant.

- Accident Sequences. Each sequence or group of similar sequences are described. Sequences not completely developed should be explained.

4.5 Example of Accident Sequence Event Tree Analysis

This section presents a step by step development of an accident sequence event tree for the Peach Bottom plant using the small LOCA as an example initiating event.

Table 4.3-1
Accident Sequence Event Tree Nomenclature

EVENT	DESCRIPTION*	EVENT	DESCRIPTION*
PWR	BWR		
C	CSIS	RPSM	RPSM
D1	HPIS	M	SRVs to open
D2	HPIS for feed & bleed	P	SRVs to close
D3	HPIS for seal injection	P1	One SRV to reclose
D4	HPIS for EBS	P2	Two SRVs to reclose
D5	ACC	P3	Three SRVs to reclose
D6	LPIS	B	Onsite electrical power
F1	CSRS-Inside containment	Q	PCS
F2	CSRS-Outside containment	U1	HPCS/HPCI
H1	LPRS	U2	RCIC
H2	HPRS	U3	CRD-2 pump mode
K	RPS	U4	CRD-1 pump mode
L	AFW	V1	Condensate
L2	AFW for ATWS	V2	LPCS
M	PCS	V3	LPCI
N	Charging from Unit 2	V4	SW cross tie
	aligned for seal injection	Z	SPMU
	flow to Unit 1	W1	RHR-SPC
N2	Charging from Unit 2	W2	RHR-SDC
	aligned for HPIS flow	W3	RHR-CS
	to Unit 1	X	Primary sys. depress.
P	PORVs for feed & bleed	R	Rupture of prim. cont.
PL	Power level	SPC	SPC
		SLC	SLC
P1	RCS for ATWS	Y	Primary cont. venting
P2	RCS pressure relief-ATWS	MSIV	MSIVs to stay open
Q	Pressurizer PORVs to close	ARI	ARI
R	Manual reactor trip	SCRM	Manual scram
S	SG steam relief-primary	ROD	Manual rod insertion
	depressurization	RPT	RPT
T	TT or MSIV closure-ATWS	FW	MSIV to stay open & FW
W	CCW to thermal barrier	RXHP	Rx at high pressure
	of RCS pumps	NADS	Rx at high pressure
Z	MTC-unfavorable	SRVs	SRVs do not stick open
Z1	MTC-very low	DEP	Operator to dep. Rx
BWR		HPIN	HP injection
		LPIN	LP injection
C	RPS	INJ	Continued injection
C1	RPS & manual scram	LEV	Level control
RPS	RPS	L	Operator to isolate leak
RPSE	RPSE		

*Each of these are "failures." In addition, many of the acronyms have not been defined in this section. The reader should refer to "Acronyms and Initialisms" for definitions.

Step 4.1. Obtain Information

The small LOCA initiating event was identified in Section 3 as requiring accident sequence event tree analysis. Success criteria determined for all modeled systems were also utilized for this event tree development. Listed below are several assumptions made which are generally applicable to all event trees developed for Peach Bottom regardless of the initiator.

1. Low Pressure Core Spray (LPCS), Low Pressure Coolant Injection (LPCI), and Residual Heat Removal (RHR, all modes) pumps are assumed to fail due to low net positive suction head (NPSH) following successful containment venting or containment failure by overpressure/temperature conditions.

2. LPCI/LPCS/RHR (all modes) pumps, which use the suppression pool for suction, will successfully operate using pool water at a temperature approaching 350°F (corresponding to saturation conditions near point of containment failure by overpressure).

3. Loss of the Vapor Suppression System (VSS) was considered but eliminated from the event tree since it is believed to be highly improbable.

4. High Pressure Coolant Injection (HPCI) and Reactor Core Isolation Cooling (RCIC) will fail at pool temperatures of 210 to 216°F.

5. Control Rod Drive (CRD) in the enhanced mode (two pumps) is assumed to fail following reactor depressurization for Shutdown Cooling (SDC) due to low NPSH.

Step 4.2. Identify Event Trees

Accident sequence event trees are generally developed for all LOCA sizes identified in Section 3. The small LOCA initiating event was chosen to illustrate the development of accident sequence event trees.

Step 4.3. Identify and Order Top Events

a) Identify Top Events

The systems required to provide the three safety functions of reactor subcriticality, Emergency Core Cooling (ECCS), and Containment Overpressure Protection (COP), identified in Section 3 for the small LOCA initiating event, are listed below. These become the top events for the small LOCA accident sequence event tree.

1. Reactor Subcriticality

    - Reactor Protection System (RPS)
    - Alternate Rod Insertion (ARI) & Recirculation Pump Trip (RPT)
    - Manual Rods & RPT
    - Timely Standby Liquid Cooling (SLC) & RPT

2. Emergency Core Cooling

    - HPCI
    - RCIC
    - Power Conversion System (PCS)
    - Automatic Depressurization System (ADS, 3 valves) & 2 of 4 LPCS pumps
    - ADS (3 valves) & 1 of 4 LPCI pumps
    - ADS (3 valves) & Condensate
    - ADS (3 valves) & High Pressure Service Water (HPSW, injection mode)

3. Containment Overpressure Protection

    - 1 of 4 RHR/heat exchanger trains [Suppression Pool Cooling (SPC) or Containment Spray (CS) modes] & corresponding HPSW
    - Primary Containment Venting (PCV)

b) Order Top Events

The top events previously identified in Step 3.5 are generally placed in a temporal order in the event tree. The order of the safety functions that must be performed for a LOCA at a BWR are:

- Reactor Subcriticality
- Emergency Core Cooling
- Containment Overpressure Protection

Following the ordering of the functions, the events (systems) within each safety function must be ordered until all functions are taken into account.

The first safety function is that of reactor subcriticality. The systems previously listed in this step that are required for this function become the first events in this LOCA tree, which are RPS, ARI, RPT, Manual Rods, and SLC. However, all of these events except RPS are part of the ATWS event tree since failure to scram represents a special category of sequences requiring a separate event tree. Only RPS appears in the small LOCA event tree, and failure of this system results in a transfer of this sequence to the ATWS event tree.

The second safety function is that of emergency core cooling. The systems required for this function listed previously become the events in the tree following the RPS event. These include the HPCI, RCIC, PCS, ADS, LPCS, LPCI, Condensate, and HPSW systems. These events are ordered based on plant-specific documentation which gives the conditions for automatic and manual initiation of systems. The PCS is put first because it performs both ECC and COP. The order of the remaining events becomes:

1. PCS
2. HPCI
3. RCIC
4. ADS
5. Condensate
6. LPCS
7. LPCI
8. HPSW

The third safety function is that of containment overpressure protection. The systems utilized to perform this function follow the HPSW event in the tree and include the CS and SPC modes of the RHR system. The shutdown cooling (SDC) mode of the RHR system is not given credit within this safety function. This is because operators, in a small LOCA scenario, are not instructed to use SDC unless the water level in the primary system is being maintained. Primary inventory is depleting from the small LOCA and SDC recirculates water in the reactor vessel, both of which are contrary to maintaining a constant water level in the core. Also, SDC initiation requires depressurization of the reactor vessel, which further reduces primary system inventory. The order of these events is determined as for the previous function and becomes:

1. SPC
2. CS
3. Venting

The identification and ordering of the top events is now complete and accident sequence delineation can now be accomplished.

Step 4.4. Construct Initial Systemic Event Tree

The systemic event tree is constructed by developing sequences until each one results in either a safe core or core vulnerability. The proper top events are determined for each sequence by considering the three types of dependencies described in Section 4.2.

The first dependency type incorporates functional success criteria into the event tree structure. If the reactor subcriticality function fails following the small LOCA initiator, the emergency core cooling and containment overpressure protection functions are inconsequential and the sequence, if it is probabilistically significant, will transfer to an ATWS tree. This is illustrated in Figure 4.5-1. This type of dependency exists for sequence 39 in the small LOCA accident sequence event tree in Figure 4.5-3 (see Step 4.6). Similarly, the containment overpressure protection function has no effect in preventing core damage if the emergency core cooling function fails. This is illustrated in Figure 4.5-1 as Sequence 3. Sequences 20 and 21 in Figure 4.5-3 also illustrate this functional dependency.

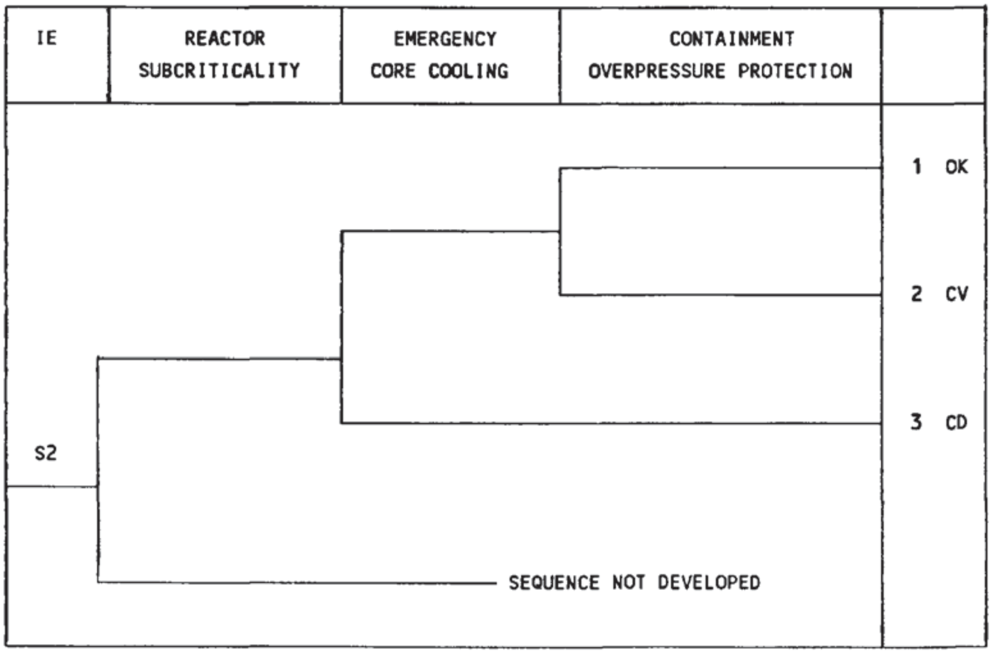


Figure 4.5-1. Example of Functional Event Tree

The second dependency type incorporates systemic success criteria into the event tree structure. If a top event meets the success criteria for a given safety function, then the remaining events for the same function are not considered. This dependency is illustrated in Sequence 1 of Figure 4.5-2 which is a systemic event tree corresponding to the functional event tree in Figure 4.5-1. The success criteria for the function of emergency core cooling is met by the PCS so the rest of the events for this function are not considered.

If PCS is unavailable, then the status of HPCI is examined. If HPCI is available, the status of the remaining emergency core cooling systems is immaterial. However, in this instance, the containment overpressure protection function must be examined. If suppression pool cooling (SPC) is available, core melt is prevented (Sequence 2, Figure 4.5-2 and Sequence 2 on Page 1 of Figure 4-5-3). On the other hand, if suppression pool cooling is not available (Sequences 3, 4, and 5, Figure 4.5-2) a core vulnerable situation exists regardless of the success or failure of containment spray or venting. This leads to consideration of a third type of dependency, one which takes into account phenomena occurring during the accident sequence. This is discussed below.

By identifying the conditions (vessel pressure, containment temperature, etc.) of a particular accident sequence, the status of the core and containment are determined and labeled. For the Peach Bottom event trees, core vulnerable sequences are generally identified by a "go to" transfer to another portion (page) of the event tree. In this manner, the outcome of all sequences in the small LOCA event tree are established as seen in Figure 4.5-3. For example, Sequences 3, 4, and 5, in Figure 4.5-2 are core vulnerable since HPCI will fail after successful initial operation, due to failure of the containment overpressure protection function, which results in a high pool temperature. Sequence 3 illustrates an implicit feature of this event tree. This sequence is core vulnerable, even though the containment overpressure protection function is successful in the CS mode. Analysis of phenomenological conditions during this sequence reveals that adverse containment conditions fail the high pressure injection systems prior to CS system initiation. This fails the emergency core cooling function, resulting in the core vulnerable condition. However, this is not the case for sequences 9, 12, 15, and 18, (Figure 4.5-3) in which the CS system provides the COP function and core vulnerability does not occur. High pressure injection fails to initiate in these sequences followed by primary system depressurization to enable low pressure cooling. Unlike the high pressure injection systems, the low pressure systems do not fail due to phenomenological conditions prior to CS system initiation, and the emergency core cooling function is maintained.

Step 4.5. Simplify Event Trees

The containment overpressure protection systems are shown early in the small LOCA tree to reduce the size of the tree. In Figure 4.5-3, the SPC and CS systems are not shown in temporal order for all sequences to decrease the total number of sequences in the tree.

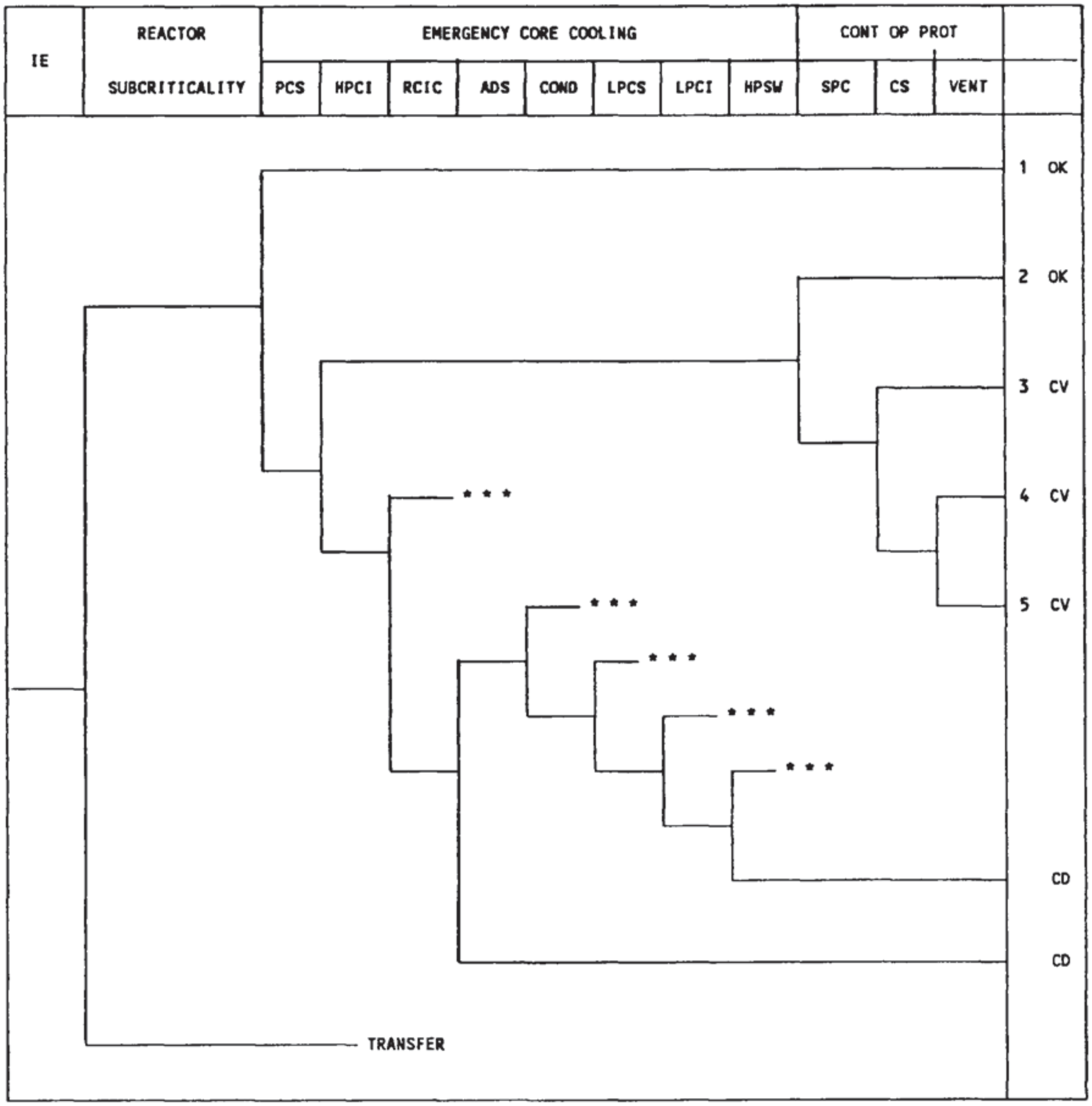


Fig 4.5-2. Example of Systemic Event Tree

Step 4.6. Identify Event Tree Transfers

No sequences transfer from the small LOCA event tree. Sequence 39 (Figure 4.5-3), which represents failure to scram following the initiating event normally would transfer to the ATWS tree. However, the low probability associated with this sequence at this point is such that it is not developed further.

Step 4.7. Resolve Core Vulnerable Sequences

All delineated sequences (see page 1 of Figure 4.5-3) not designated as core damage or core OK are core vulnerable and transfer to another portion of the tree for resolution. Phenomenological conditions in each sequence must be considered to determine if the emergency core cooling function can be restored.

Sequences 3 and 6 have lost the ECC function but the COP function is successful. High pressure injection with HPCI and RCIC, following initially successful operation, is failed due to high suppression pool temperatures obtained following SPC failure and prior to CS initiation. However, high pressure injection with CRD and all low pressure injection systems are operable. Therefore, resolution of these sequences involves incorporating into the event tree the top events of CRD, ADS (for reactor depressurization), and all low pressure cooling systems (Condensate, LPCS, LPCI, HPSW), as shown in the S2-1 branch of the event tree (page 2 of Figure 4.5-1).

Sequences 4 and 7 have lost both the ECC and COP functions. The same injection systems utilized in sequences 3 and 6 are available to satisfy the ECC function, therefore identical top events appear for sequences 4 and 7 in the initial part of the core vulnerable resolution phase. The COP function must now be restored. Since the SPC and CS modes of the RHR system have failed, the only system available to provide the COP function is the Primary Containment Venting system, which appears as a top event following the low pressure systems in the tree. Unsuccessful containment venting results in failure of the COP function. This leads to containment rupture prior to core damage, which follows the containment venting event. The containment is now depressurized, if either venting or rupture is successful. These events, since they change containment conditions, may adversely effect the ECC function. The system providing the ECC function prior to venting or rupture must also appear as a top event following venting and rupture to account for the probability that this system (CRD) failed during the containment venting or rupture process. ECC systems in plants where the vented steam is released into the equipment area are susceptible to environmental failure. The remaining low pressure systems that are still functioning (Condensate and HPSW) appear in the tree following the reactor depressurization event (ADS). The resolution of sequences 4 and 7 is shown in the S2-2 branch of the event tree (page 2 of Figure 4.5-3).

In sequence 10, high pressure injection has failed and low pressure injection provides the ECC function following primary system depressurization. The ECC function, provided by Condensate, is eventually lost due to failure of the COP function. Loss of the ECC function renders this sequence core vulnerable. Low pressure injection with Condensate is lost because failure of the SPC and CS modes of the RHR system results in pressurization of containment. High containment pressure eventually overcomes the nitrogen bottle pressure holding the primary system SRVs open, causing the SRVs to drift closed. This allows pressure in the primary system to increase which soon fails the functioning low pressure system. Resolution of this sequence requires the ECC function to be established. The first consideration is the condition in the primary system. At this point in the sequence the primary system is at high pressure. Since CRD is the only high pressure system available, this becomes the first top event in the core vulnerable resolution phase. The Primary Containment Venting system is available to provide the COP function and becomes the next event in the tree. As before, the event of rupture of containment follows the containment venting event. CRD must appear in the tree next due to the likelihood of failure during venting. The remaining injection systems follow the top event CRD in the event tree, shown in the S2-3 branch (page 3 of Figure 4.5-3).

The remaining core vulnerable sequences in the tree (13,16,19) are resolved in the same manner as the previous sequences. All are core vulnerable due to loss of the ECC function as a result of loss of the COP function. Also, all have high pressure injection available with CRD and low pressure injection available with HPSW to recover the ECC function. The Primary Containment Venting system is available to provide the COP function. These systems are utilized to resolve the three sequences as shown in the S2-4 branch of the event tree (page 3 of Figure 4.5-3).

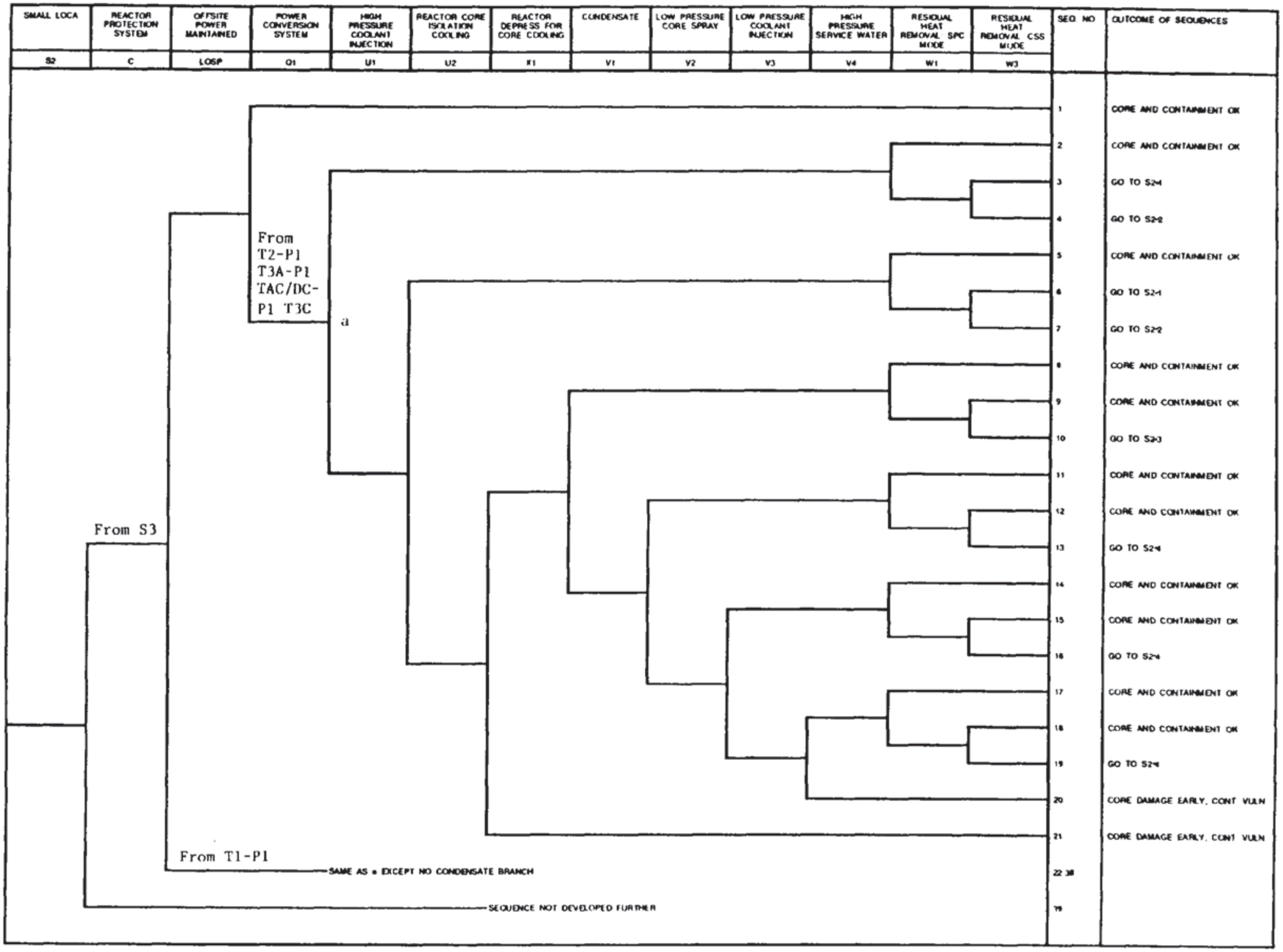

SMALL LOCA
S2
REACTOR PROTECTION SYSTEM
C
OFFSITE POWER MAINTAINED
LOSP
POWER CONVERSION SYSTEM
Q1
HIGH PRESSURE COOLANT INJECTION
U1
REACTOR CORE ISOLATION COOLING
U2
REACTOR DEPRESS FOR CORE COOLING
X1
CONDENSATE
V1
LOW PRESSURE CORE SPRAY
V2
LOW PRESSURE COOLANT INJECTION
V3
HIGH PRESSURE SERVICE WATER
V4
RESIDUAL HEAT REMOVAL SPC MODE
W1
RESIDUAL HEAT REMOVAL CSS MODE
W3
SEQ NO
OUTCOME OF SEQUENCES
From T2-P1 T3A-P1 TAC/DC-P1 T3C
a
From S3
From T1-P1
SAME AS a EXCEPT NO CONDENSATE BRANCH
SEQUENCE NOT DEVELOPED FURTHER
1 CORE AND CONTAINMENT OK
2 CORE AND CONTAINMENT OK
3 GO TO S2-1
4 GO TO S2-2
5 CORE AND CONTAINMENT OK
6 GO TO S2-1
7 GO TO S2-2
8 CORE AND CONTAINMENT OK
9 CORE AND CONTAINMENT OK
10 GO TO S2-3
11 CORE AND CONTAINMENT OK
12 CORE AND CONTAINMENT OK
13 GO TO S2-4
14 CORE AND CONTAINMENT OK
15 CORE AND CONTAINMENT OK
16 GO TO S2-4
17 CORE AND CONTAINMENT OK
18 CORE AND CONTAINMENT OK
19 GO TO S2-4
20 CORE DAMAGE EARLY, CONT VULN
21 CORE DAMAGE EARLY, CONT VULN
22 38
39

Figure 4.5-3. Small LOCA Event Tree

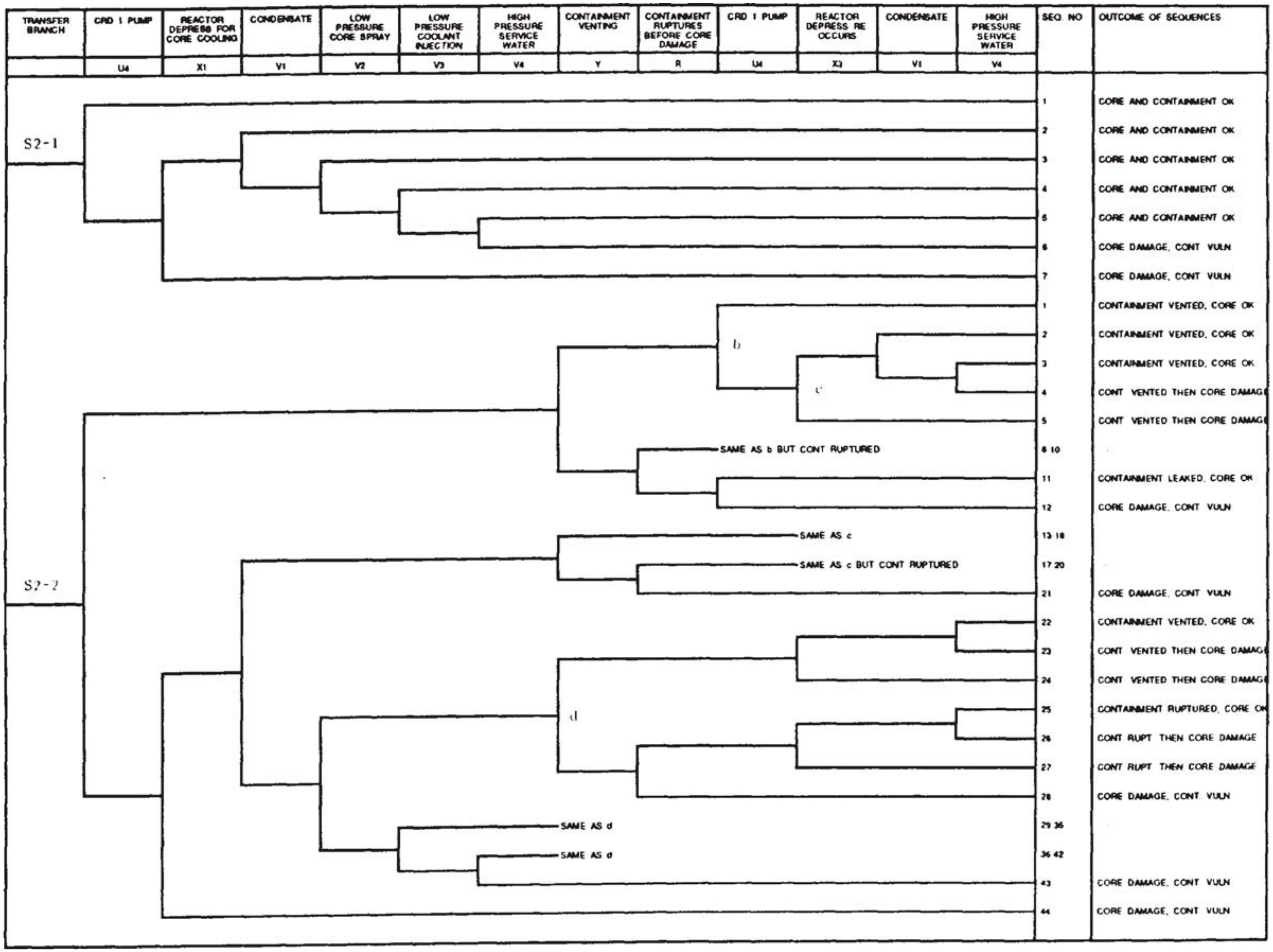

TRANSFER BRANCH
CRD 1 PUMP
U4
REACTOR DEPRESS FOR CORE COOLING
X1
CONDENSATE
V1
LOW PRESSURE CORE SPRAY
V2
LOW PRESSURE COOLANT INJECTION
V3
HIGH PRESSURE SERVICE WATER
V4
CONTAINMENT VENTING
Y
CONTAINMENT RUPTURES BEFORE CORE DAMAGE
R
CRD 1 PUMP
U4
REACTOR DEPRESS RE OCCURS
X3
CONDENSATE
V1
HIGH PRESSURE SERVICE WATER
V4
SEQ. NO
OUTCOME OF SEQUENCES
S2-1
S2-2
b
c
d
SAME AS b BUT CONT RUPTURED
SAME AS c
SAME AS c BUT CONT RUPTURED
SAME AS d
SAME AS d
1 CORE AND CONTAINMENT OK
2 CORE AND CONTAINMENT OK
3 CORE AND CONTAINMENT OK
4 CORE AND CONTAINMENT OK
5 CORE AND CONTAINMENT OK
6 CORE DAMAGE, CONT VULN
7 CORE DAMAGE, CONT VULN
1 CONTAINMENT VENTED, CORE OK
2 CONTAINMENT VENTED, CORE OK
3 CONTAINMENT VENTED, CORE OK
4 CONT VENTED THEN CORE DAMAGE
5 CONT VENTED THEN CORE DAMAGE
6 10
11 CONTAINMENT LEAKED, CORE OK
12 CORE DAMAGE, CONT VULN
13 16
17 20
21 CORE DAMAGE, CONT VULN
22 CONTAINMENT VENTED, CORE OK
23 CONT VENTED THEN CORE DAMAGE
24 CONT VENTED THEN CORE DAMAGE
25 CONTAINMENT RUPTURED, CORE OK
26 CONT RUPT THEN CORE DAMAGE
27 CONT RUPT THEN CORE DAMAGE
28 CORE DAMAGE, CONT VULN
29 36
36 42
43 CORE DAMAGE, CONT VULN
44 CORE DAMAGE, CONT VULN

Figure 4.5-3. Small LOCA Event Tree (Continued)

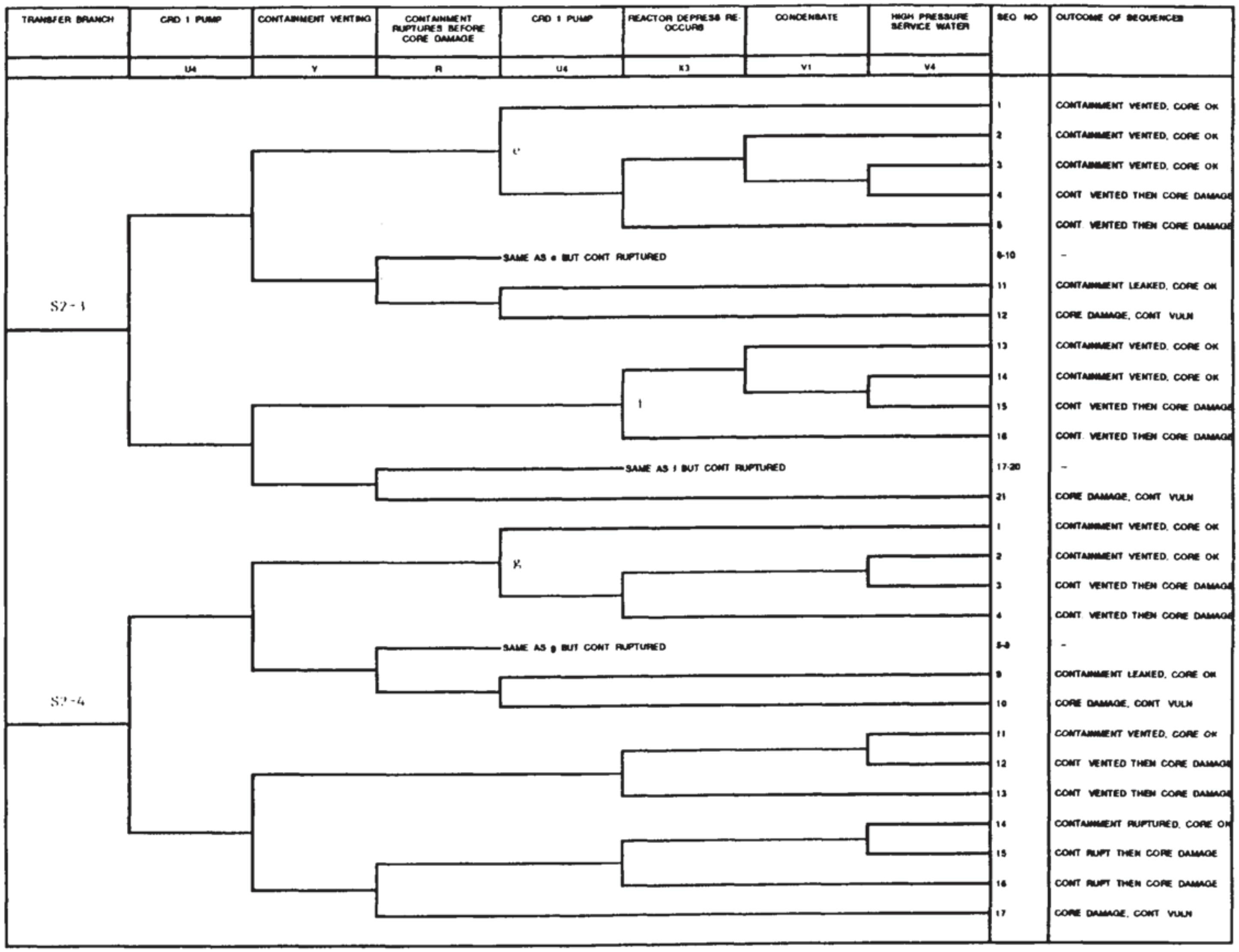

TRANSFER BRANCH
CRD 1 PUMP
U4
CONTAINMENT VENTING
Y
CONTAINMENT RUPTURES BEFORE CORE DAMAGE
R
CRD 1 PUMP
U4
REACTOR DEPRESS RE-OCCURS
X3
CONDENSATE
V1
HIGH PRESSURE SERVICE WATER
V4
SEQ NO
OUTCOME OF SEQUENCES
S2-3
e
SAME AS e BUT CONT RUPTURED
f
SAME AS f BUT CONT RUPTURED
1 CONTAINMENT VENTED, CORE OK
2 CONTAINMENT VENTED, CORE OK
3 CONTAINMENT VENTED, CORE OK
4 CONT VENTED THEN CORE DAMAGE
5 CONT. VENTED THEN CORE DAMAGE
6-10 -
11 CONTAINMENT LEAKED, CORE OK
12 CORE DAMAGE, CONT VULN
13 CONTAINMENT VENTED, CORE OK
14 CONTAINMENT VENTED, CORE OK
15 CONT VENTED THEN CORE DAMAGE
16 CONT. VENTED THEN CORE DAMAGE
17-20 -
21 CORE DAMAGE, CONT VULN
S2-4
g
SAME AS g BUT CONT RUPTURED
1 CONTAINMENT VENTED, CORE OK
2 CONTAINMENT VENTED, CORE OK
3 CONT VENTED THEN CORE DAMAGE
4 CONT. VENTED THEN CORE DAMAGE
5-8 -
9 CONTAINMENT LEAKED, CORE OK
10 CORE DAMAGE, CONT VULN
11 CONTAINMENT VENTED, CORE OK
12 CONT VENTED THEN CORE DAMAGE
13 CONT VENTED THEN CORE DAMAGE
14 CONTAINMENT RUPTURED, CORE OK
15 CONT RUPT THEN CORE DAMAGE
16 CONT RUPT THEN CORE DAMAGE
17 CORE DAMAGE, CONT VULN

Figure 4.5-3. Small LOCA Event Tree (Concluded)

5. SYSTEMS ANALYSIS

The accident sequence event trees (see Section 4) identify the various combinations of events (or accident sequence paths) that can result in a core damage state for each initiating event. To calculate the frequency of each accident sequence, a systematic method is used to identify and quantify all of the ways that each accident sequence event (or in most cases a system) can fail. This systematic search for system failures is called Systems Analysis.

There is a large selection of analytical techniques from which the analyst can choose to perform a Systems Analysis: for example, failure modes and effects analysis, logic diagrams, success trees, fault trees, etc. For the most part, the "large-fault-tree" approach is used to analyze the systems. The large-fault-tree approach defines a top event (an event that appears on the event tree) and then models in detail multiple ways for the failure of that event to occur, including the failure of required support systems. This section describes the methodology used to perform the Systems Analysis.

5.1 Systems Analysis Assumptions and Limitations

In this methodology, experienced Probabilistic Risk Assessment (PRA) analysts, who are able to identify a sufficient level of detail for the analysis of each system, are used. Not all systems are analyzed to the same level of detail. For example, if a system is potentially important, a detailed fault tree is constructed. However, past studies have shown that certain systems tend to be of minor importance to core damage frequency or risk. When an initial review shows that this conclusion is applicable, simplified models are constructed (e.g., Boolean expressions, black boxes). In some cases, the complexity of the system, not the importance, dictates that simplified methods be used. These methods are discussed in greater detail in the following sections.

As discussed in Section 2, the plant configuration and operation is not fixed; changes are constantly occurring. Some of these changes have the potential to significantly affect the safety and risk of the plant. The project leader at some time in the analysis decides on a configuration freeze date. Plant changes made after this date are not incorporated into the analysis.

5.2 Systems Analysis Development

This analysis uses the fault tree method to model most of the systems. The fault trees are a type of logic diagram that first reduces the system into segments or components. Fault logic of these segments or components is then excluded modeling all the possible failure modes. The development of these system models involves several steps that are illustrated in Figure 5.2-1 and are described below.

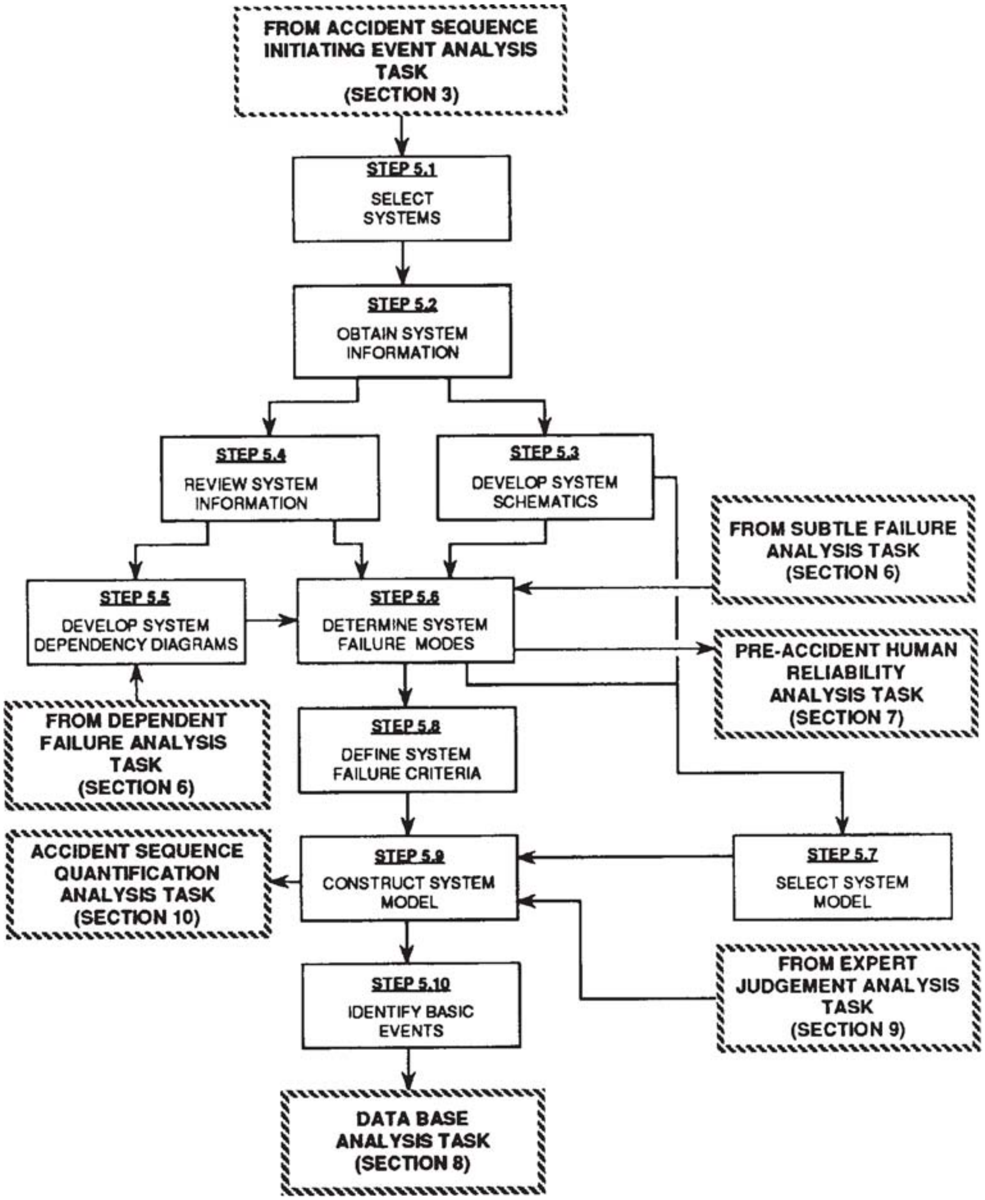

FROM ACCIDENT SEQUENCE INITIATING EVENT ANALYSIS TASK (SECTION 3)
STEP 5.1
SELECT SYSTEMS
STEP 5.2
OBTAIN SYSTEM INFORMATION
STEP 5.4
REVIEW SYSTEM INFORMATION
STEP 5.3
DEVELOP SYSTEM SCHEMATICS
FROM SUBTLE FAILURE ANALYSIS TASK (SECTION 6)
STEP 5.5
DEVELOP SYSTEM DEPENDENCY DIAGRAMS
STEP 5.6
DETERMINE SYSTEM FAILURE MODES
PRE-ACCIDENT HUMAN RELIABILITY ANALYSIS TASK (SECTION 7)
FROM DEPENDENT FAILURE ANALYSIS TASK (SECTION 6)
STEP 5.8
DEFINE SYSTEM FAILURE CRITERIA
ACCIDENT SEQUENCE QUANTIFICATION ANALYSIS TASK (SECTION 10)
STEP 5.9
CONSTRUCT SYSTEM MODEL
STEP 5.7
SELECT SYSTEM MODEL
FROM EXPERT JUDGEMENT ANALYSIS TASK (SECTION 9)
STEP 5.10
IDENTIFY BASIC EVENTS
DATA BASE ANALYSIS TASK (SECTION 8)

Figure 5.2-1. Step Relationship for Systems Analysis

Step 5.1. Select Systems

In this step the analyst identifies or selects the systems requiring models. These systems are categorized as either a front-line system or a support system. The front-line systems that require models are those identified by the success criteria in the Accident Sequence Initiating Event Analysis task (see Step 3.5 in Section 3). The support systems that must operate in order for the front-line systems to properly function require models. A preliminary list of front-line and support systems was identified in the Plant Familiarization Analysis task (see Section 2). They are listed again in Table 5.2-1. It should be noted that this is a generic list and is not necessarily applicable to all plants. In addition, there are systems that are not important to the mitigation of the initiating event (i.e., play an insignificant role in preventing core damage), but are important in that they affect the size of the source term. These systems are identified in the Plant Damage State Analysis task (see Section 11) and may also require system models.

Step 5.2. Obtain System Information

In this step the analyst identifies and collects the information necessary to develop the system models. It should be noted that a significant portion of this information is obtained in the Plant Familiarization Analysis task. Information is gathered for each system regarding its: (1) operation, (2) interfaces and dependencies, (3) test and maintenance, and (4) design. This information is usually found in the following documents:

- System descriptions;
- Piping and instrumentation diagrams and functional control diagrams for all front-line and their corresponding support systems;
- Elementary Wiring Diagrams (one lines); and
- Technical Specifications.

In addition to the above documents, some of the information is obtained from discussions with plant personnel and tours of the plant site.

Step 5.3. Develop System Schematics

A system schematic is developed for each front-line and support system. Usually the plant system drawings are very detailed, containing considerably more information than is required in the Systems Analysis task. To assist the analyst in clearly performing the system review and failure modeling, and developing the system model, a simplified system schematic is developed that defines the system as represented in the analysis.

Table 5.2-1
Preliminary Boiling Water Reactor (BWR) and Pressurized Water Reactor (PWR) Accident Initiators and Systems

BWR	PWR
Accident Initiators:	Accident Initiators:
Loss of Coolant Accident (LOCA)	LOCA
Transients	Transients
Loss of Offsite Power (LOSP)	LOSP
Interfacing Systems LOCAs	Interfacing Systems LOCAs
Anticipated Transient Without Scram (ATWS)	Steam Generator Tube Rupture (SGTR)
	ATWS
Front Line Systems:	Front Line Systems:
High Pressure Core Spray (HPCS)	High Pressure Injection (HPI)
High Pressure Coolant Injection (HPCI)	High Pressure Recirculation (HPR)
Reactor Core Isolation Cooling (RCIC)	Power Operated Relief Valve (PORV)
Safety Relief Valve (SRV)	Low Pressure Injection (LPI)
Automatic Depressurization System (ADS)	Low Pressure Recirculation (LPR)
	Accumulators (ACC)
Low Pressure Core Spray (LPCS)	Auxiliary Feedwater (AFW)
Low Pressure Coolant Injection (LPCI)	Containment Spray Injection (CSI)
Reactor Protection System (RPS)	RPS
Power Conversion System (PCS)	PCS
Alternate Rod Insertion (ARI)	Alternate injection*
Residual Heat Removal (RHR)--	Containment Spray Recirculation (CSR)
Suppression pool cooling	
Containment spray	
Shutdown cooling	
Standby Liquid Control (SLC)	
Control Rod Drive (CRD)	
Alternate injection*	
Support Systems:	Support Systems:
Electric power	Electric power
Actuation	Actuation
Instrument air (IA)	IA
Heating Ventilation Air Conditioning (HVAC)	HVAC
Service Water (SW)**	SW**

* At some plants, one example of an alternate injection system would be the firewater system.

** Service water is used generically here to imply any "cooling water" system that is required for successful operation of the front-line and other support systems.

This task is a significant element of the Systems Analysis task. The analyst is, in essence, identifying those components critical to the successful operation of the system. There are components which potentially dominate the system's unavailability. The simplification basically includes the omission of:

- Control and instrumentation from the drawing;

- Pipe segments or components that do not have a significant impact on system performance; and

- Supply lines for which credit is not taken.

However, the specific items that are either included or deleted differ depending on the type of system. The criteria used in the development of the system schematics also vary depending on the type of system as follows:

Front-line Fluid System

- All diversion paths to the first normally closed valve that are greater than or equal to one-third of the main flowpath pipe diameter are shown.

- Minimum recirculation lines are shown.

- All major components (e.g., pumps, operated valves, heat exchangers, tanks) are shown.

- All manual and check valves in the normal flow paths are shown (those in minor test lines are not shown).

- The containment boundary is shown on the schematic to indicate components potentially inaccessible during an accident sequence.

Support Fluid System

- The major components shown include (1) those immediately surrounding each cooling water load under consideration in the analysis (e.g., heat exchangers) and (2) those that affect the operation of the cooling water system (e.g., pumps, major valves).

- For a load that is not part of the accident mitigation (e.g., plant auxiliary systems), the components affecting the load are shown if the load (1) needs to be isolated for sufficient flow to the required loads or (2) its failure prevents cooling to the required loads. For example, a large load upstream such as plant auxiliary systems, needs to be isolated for the safety systems to receive adequate cooling water. If not isolated, enough flow is diverted such that insufficient cooling is provided to the safety loads.

Electric Power System

- All electrical power separation of divisions and buses (and their cross connects) and all major components (e.g., diesels, buses, batteries, chargers, inverters, buses, and selected breakers) are shown.

- Only those buses that power the loads examined are shown on the schematic (at the major bus level, not the motor control center level).

Actuation and Control System

A simplified schematic for actuation and control is not necessarily drawn. However, certain information is gathered to "black box" (see Step 5.7) the actuation and isolation signals as follows:

- For each actuation/control signal, the systems actuated or isolated are identified.

- The function for each signal is identified (e.g., actuation or isolation signal).

- The conditions for generating each signal are identified (e.g., low reactor water level).

- The sensors generating each signal are identified (e.g., Level Sensor L619A).

- Any permissives or special conditions that must exist for the systems or component to actuate (or isolate) are identified.

- The success criteria for each signal are identified.

- The supports (e.g., power) are determined for each signal and sensor.

HVAC System

- Only those HVAC loads under consideration in the analysis are drawn.

- The components (e.g., dampers, fans) affecting each HVAC load under consideration in the analysis (e.g., LPCI room cooling) are shown.

- The major components (e.g., compressors, dampers) that affect the operation of the HVAC system are also shown.

- The containment boundary is shown on the schematic to indicate components potentially unaccessible during an accident sequence.

Power Conversion System (PCS)

- For BWRs, only the following major components are shown:
  - reactor,
  - main steam lines,
  - turbine bypass line with bypass valve,
  - condenser,
  - condensate, condensate booster, and feedwater pumps, and
  - motor operated valves.

- For PWRs, only the following major components are shown:
  - steam generators,
  - main steam lines,
  - turbine bypass line with bypass valve,
  - condenser,
  - condensate, condensate booster, and feedwater pumps, and
  - motor operated valves.

Primary Pressure Relief System

- For BWRs, a simplified schematic is drawn showing the ADS valves and the pressure relief SRVs.

- For PWRs, a simplified schematic is drawn showing the PORVs, the pressure relief SRVs, and the block valves.

IA

- A simplified schematic is drawn showing (1) the major components that need to operate so that IA functions and (2) the loads that are dependent on IA.

In the initial analysis of the NUREG/CR-4550 plants, systems were divided into pipe segments. A pipe segment was defined as that portion of the system (e.g., piping and selected independent components) that could be combined for treatment in the fault tree logic. The pipe segments were indicated by nodes on the schematics. In the reanalysis, the fault tree development did not utilize the pipe segments (see Step 5.9). This change was required because of the uncertainty analysis, the correlation between components and the importance calculations were affected (see Section 12), and to provide fault trees that could be used to the external event analyses.

Step 5.4. Review System Information

In this step the analyst reviews the information gathered in Step 5.2 to eventually identify the potential failure mechanisms (i.e., modes) of each system and its associated components. In order to identify these failure modes, the analyst must understand the system:

- Operation;

- Interfaces and dependencies with other systems;

- Instrumentation and control;

- Testing and maintenance requirements including instrument calibration; and

- Historical behavior.

System Operation

It is necessary to understand the function and operation of the system under all conditions specified in the event trees:

- Which components must operate;

- Which components must change state;

- Failure position of components;

- Whether component operation is manual or automatic;

- What conditions must exist for the operator to manually actuate each component and how is the operator instructed;

- What conditions must exist for automatic actuation to occur for each component;

- Which components receive signals to change state;

- What conditions must exist for these signals to be generated; and

- How the system is automatically isolated.

Most of this knowledge can be obtained from the information gathered in Step 5.2; however, discussions with plant personnel who are familiar with the system in question provide additional insights into the operation of the system. The instrumentation associated with system operation and any associated control systems are also identified to understand manual and automatic operation.

System Interfaces and Dependencies

Because of the redundancy in most light water reactor systems, interfaces and dependencies that lead to multiple system and component failures are particularly important. Care is taken to identify all required supports and commonalities that a system or component shares with other systems or components. These interfaces and dependencies generally include:

- Power requirements;
- Cooling requirements;
- Ventilation requirements;
- Phenomenological effects such as:
  - -- steam flooding of rooms,
  - -- containment conditions (pressure and temperature),
  - -- suppression pool (BWR only) conditions (pressure and temperature), and
  - -- steam binding of auxiliary feedwater systems (PWR only);
- Actuation requirements;
- Isolation requirements; and
- Shared components (e.g., common valve).

An additional interface is the system boundary. For plants with multiple units, this boundary can have a significant impact on the results. Normally, credit is not given for using a system from an adjacent unit unless aligning the system is part of the plant procedures. If so, credit is given and this interface is clearly defined.

Again, discussions with plant personnel are helpful in identifying the system interfaces and dependencies.

System Test and Maintenance and Instrument Calibration

A potential major contributor to the failure probability of each system is its unavailability because the system (1) is out of service for test or maintenance when required, (2) is not properly realigned after a test or maintenance activity and therefore unavailable when required, or (3) instruments are miscalibrated during or after a test or maintenance activity. The following information is required:

- Components in each system that are subject to test and maintenance activities while the plant is operating;
- Surveillance period for
  - -- position verification of the system components,
  - -- operability of the system components,
  - -- the functional testing of the system, and
  - -- any other applicable miscellaneous activity;
- Limiting conditions of operation for each system;
- Components in each system that need to be restored after test or maintenance activities so that the system is in its proper configuration; and

- Instrumentation in each system that is subject to calibration activities.

It is assumed that a component is disabled if, when down for maintenance, no isolation valves are available and there is an open pipe.

System Operating History

Fault tree analysis is one of many analytical tools that can be used in Systems Analysis. No single technique identifies all potential contributors to system failure; therefore, examination of the system operating history is performed to identify any potential subtle failures that are not identified in the fault tree analysis (this is discussed in more detail in Step 6.7 in Section 6).

Step 5.5. Develop System Dependency Diagrams

In this step the analyst develops a dependency diagram for each system. The dependencies identified in Step 5.4 are presented in a manner that illustrates their interaction with the system. The dependency diagram is developed for each front-line and support system as follows:

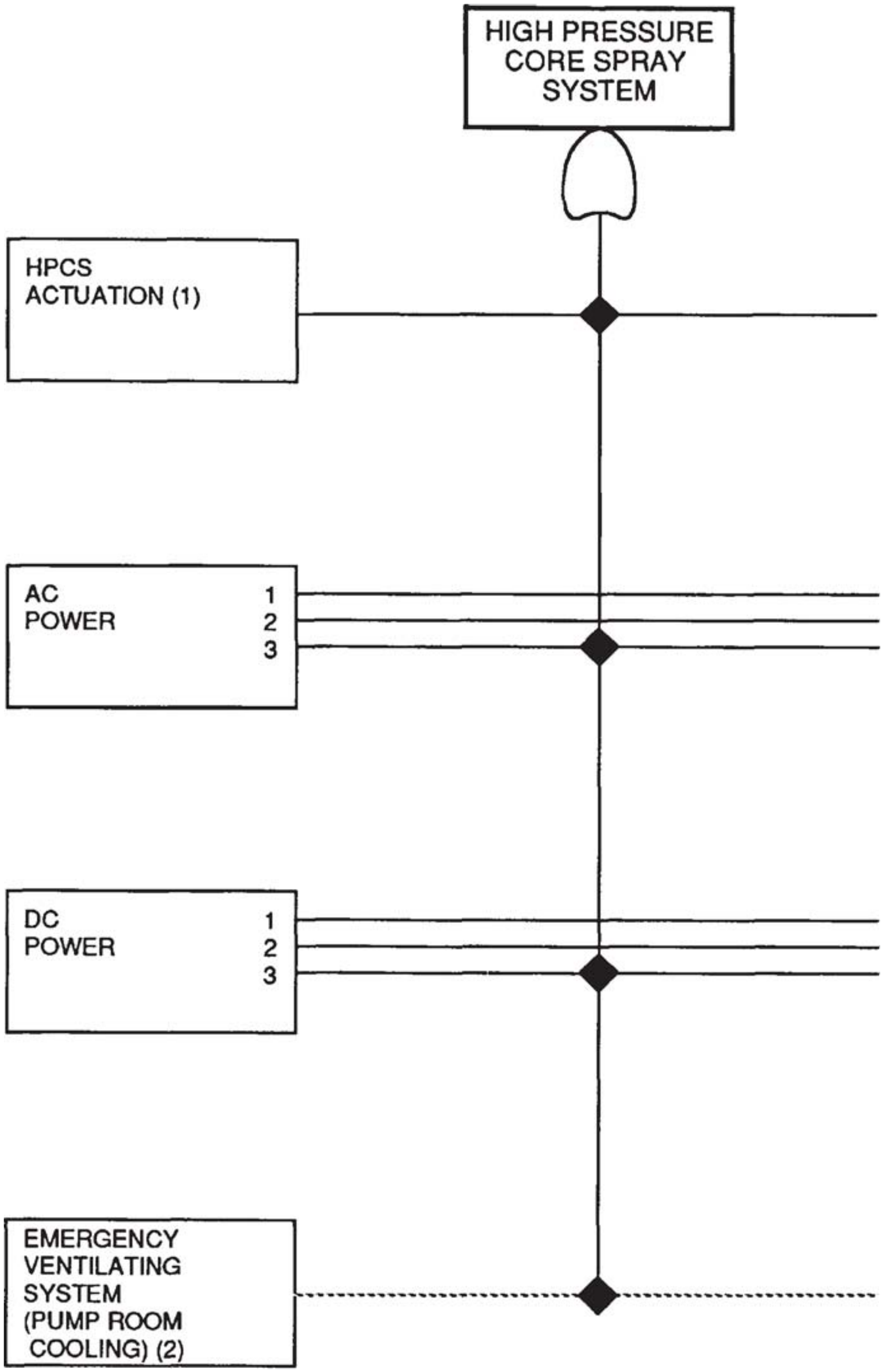
- The dependency diagram is drawn with a modified fault tree approach using failure logic.

- The top event identifies the system under consideration.

- The top gate indicates the success criteria of the system considering its dependencies only; independent failures of system components are not modeled on these diagrams.

- The next levels (events) considered are those trains or components and their success criteria that are required to function for operation of the top system. Trains or components are shown as separate events when their dependencies are different. For example, if a two train system and all its components are dependent on the same support systems, the trains and components do not need to be individually shown on the diagram.

- The last set of levels (events) show the required support systems for operation of each train or component. Each support system is shown on the diagram as a separate event on the left side of the diagram. Vertical lines are drawn from each train or component to the last required support system. Horizontal lines are drawn from each support system across the diagram. If the support system is required only for long-term operation of the train or component, then the horizontal line is drawn as a dashed line. When the vertical and horizontal lines intersect, and the support system is required for the train or component to function, the intersection is highlighted by a blackened diamond. See Figure 5.2-2 for an example.


HIGH PRESSURE CORE SPRAY SYSTEM
HPCS ACTUATION (1)
AC POWER
1
2
3
DC POWER
1
2
3
EMERGENCY VENTILATING SYSTEM (PUMP ROOM COOLING) (2)

Dependency Diagram Is Shown Using Failure Logic.
(1) See Actuation Diagram
(2) Dependency Not Required During Short Term Operation.

Figure 5.2-2. Dependency Diagram Example

Step 5.6. Determine System Failure Modes

The different failure mechanisms (or modes) of each system and its associated components are identified. The different failures considered are as follow:

- The component fails to perform its function because of a hardware fault. These faults include the following:
  - component plugs,
  - component fails to open or close,
  - component fails to start or run, or
  - component fails to function.
- The component (or system) fails to perform its function because it is out of service for test or maintenance.
- The component (or system) fails to perform its function because it wasn't restored after test and maintenance.
- The component fails to perform its function because required instrumentation was miscalibrated.
- The component fails to perform its function because a required support system has failed (see Step 5.5).
- The component fails to perform its function because of a common cause fault. The reader should refer to Section 6 to determine whether this failure should be included for the component.
- The component (or system) fails to perform its function because of some unexpected or subtle failure in the design of the system or component. The reader should refer to Section 6 to determine whether this type of failure exists.

The information obtained in Step 5.4 is reviewed to determine which failures modes apply to the system and to each component.

Step 5.7. Select System Model

In this step the analyst selects the appropriate type of model for each system. As mentioned in the introduction to this section, models of differing levels of detail are used for different systems.

The objectives of the PRA and the available resources (time, manpower) have dictated the level of detail of the system models in the past. It is desirable to achieve as much detail as possible because this ensures more confidence in the final results. In this methodology, knowledge gained over the years in the field of PRA is applied to system model development. Where experience indicates that little is gained from a detailed model, one is not constructed, but instead a simplified model based on the more important system events, data, or components is used. Four different model types are defined below.

1. Detailed Fault Tree. A fault tree that models all the system components shown on the schematic plus all possible failure modes (e.g., hardware, maintenance).

2. Simplified Fault Tree. A fault tree that does not necessarily model all the system components and support systems nor all failure modes. It models only the "major" failures. If the analyst determines that one or more specific failures dominate the system, only those failures are modeled. All significant support system dependencies are modeled.

3. Simplified Boolean Expression. This model is the same as the Simplified Fault Tree model; however, the analyst chooses to directly construct the logic model by writing the Boolean expression instead of constructing the simplified fault tree.

4. Black Box. The system is not represented by an explicit logic model, but by a "black box." A black box is a single event where the system unavailability is represented by a value determined from an established data base.

Guidelines are established to help the analyst in selecting the appropriate model to represent the various systems:

1. The major front-line safety systems are the primary means for accident mitigation and as such their loss has a great impact on the core damage frequency. Subtle failures, dependencies, and interfaces in and among these systems are found by detailed fault tree models. The systems represented by a detailed fault tree model include:

BWR

HPCS
HPCI
RCIC
LPCS
LPCI
RHR (all modes)
Alternate Injection

PWR

HPI
HPR
LPI
LPR
AFW
CSI
CSR
Alternate Injection

2. The unavailability of the remaining front-line safety and nonsafety systems has been found in the past to be dominated by a few specific failures such as operator failing to align the system; therefore, detailed fault trees are not necessary for these systems and they are represented by a simplified model. These systems are represented by either a simplified fault tree or a Boolean equation and include:

BWR	PWR
Primary Pressure Relief	Primary Pressure Relief
-- ADS	-- PORVs
-- SRVs	-- SRVs
CRD	-- Block Valve
SLC	Accumulators

3. Because cooling water support systems have the potential to fail several systems simultaneously and have been shown in the past to be dominant contributors to core damage frequency, it is important to identify any subtle failures, dependencies, and interfaces connected with these systems. Detailed fault tree models are therefore drawn to represent these systems.

4. Although the loss of HVAC, electric power, actuation/ control and instrument air systems, can eventually fail several systems at the same time, they generally have unavailabilities dominated by a few specific failures; therefore, a simplified fault tree or Boolean equation is used to represent the systems.

5. PCS is a normally operating system with much redundancy. There is an established data base for its unavailability from historical data; therefore, PCS is represented by a black box model if no single major failures are identified. Otherwise, it is represented by a simplified model, either fault tree or Boolean expression.

6. The RPS is complex, generally independent of all other systems, and has been analyzed in past PRAs in detail with an established, although very uncertain, value for its unavailability. Therefore, RPS is represented by a black box model.

The above guidelines represent the level of detail that is suggested for the systems identified. However, it is sometimes necessary that the analysis be able to account for the fact that portions of systems may be operable while other portions have failed. If such distinctions are accounted for, the above guidelines are modified. For example, if loss of DC Bus A fails the feedwater pumps, but not the condensate pumps, PCS is modeled in a simplistic manner (either fault tree or Boolean equation form) instead of as a single event. In any case, the judgment of an experienced team leader may lead to changes in the level of detail for specific systems. The external event analysts should also be consulted when making level of detail decisions, as they may desire more detailed models than required for the internal event analysis.

Step 5.8. Define System Failure Criteria

In this step the analyst defines the failure criteria for each system. For the front-line systems, in order to obtain the failure criteria, the analyst converts the success criteria specified for the system into a statement of system failure. This conversion is done for each initiating event; in some cases, the statement differs because the success criteria differ among the initiating events. For the support systems, the failure criteria are also obtained by converting the success criteria into a system failure statement. The support system success criteria (and therefore the support system failure criteria) are specified by the front-line system requirements.

Step 5.9. Construct System Model

In this step the analyst builds the system model for each front-line and support system using the information from the above steps. Once the model type has been selected (Step 5.7), the failure logic is developed for each system. This involves three major steps:

1. The top-level failure logic is developed. The top event indicates the system under consideration with its subsequent failure criteria (see Step 5.8) modeled using the appropriate gates.

2. The failure logic of the system with respect to its associated components generally is modeled using a collection of component failures under OR and AND gates.

3. The failure modes (see Step 5.6) of each component are then usually modeled using a collection of OR and AND gates. It is imperative that the system analyst interface with the data analyst to determine the level of detail to which the failure mode can be developed. In defining a failure mode, the data may not exist to the level of resolution that the system analyst has defined. For example, the component under consideration is a valve and the failure mode identified is a hardware failure. The analyst has the option of defining the event as "valve fails from hardware fault"; or the analyst can further develop the event and define the failure as "valve fails from packing failure, stem failure, etc." The data may not differentiate the manner in which the valve failed; therefore, the former development would be the correct level to which the event should be modeled.

Step 5.10. Identify Basic Events

In this step the analyst identifies the basic events of each system model. Data are required for each basic event. These data will be in one of the following forms:

- Failure rate (see Section 8);
- Test and maintenance unavailability (see Section 8);
- Human error probability (see Section 7); or
- Common cause factor (see Section 6).

5.3 Systems Analysis Nomenclature

Nomenclature was developed for (1) labeling the basic events in the construction of the system models (e.g., fault trees), and (2) constructing the system schematics. The basic event labeling scheme is designed to reflect the flexibility of the systems modeling approach. A basic event label identifies the level to which each event is modeled (e.g., train, pipe segment, individual component, human error). The failure mode of the basic event is also identified in the event name. A variety of failure modes are defined to permit flexibility in system modeling. The nature of a failure mode can either be specific, general, or detailed as is appropriate for each system and each basic event.

The basic event label is made up of a maximum of sixteen characters which are discussed below:

```
XXX - YYY - ZZ - AAAAA
 |     |     |    |__________Event and Component Descriptor
 |     |     |_______________Failure Mode
 |     |_____________________Event Component Type Identifier
 |___________________________System Identifier
```

XXX This is a three-letter code denoting the system to which the basic event either belongs or is related to. See Table 5.3-1 for a list of all the systems and their codes. Many of the systems on the list are standard systems common to many power plants. Wherever possible, the systems of each plant are given the appropriate system name from the list, even though the actual plant name for the system is somewhat different from the name on the list. Some of the system names reflect systems unique to specific plants.

YYY This is a three-letter code denoting the level of modeling corresponding to the event (i.e., basic event type). See Table 5.3-2 for a list of basic event types and their codes. The list includes virtually all the individual components that are needed to model the basic events. Other levels of event modeling such as pipe segments and common cause faults are included as well.

ZZ This is a two-letter code denoting the failure mode associated with the event. See Table 5.3-3 for a list of failure modes for the basic events. The failure modes are grouped by types of components or events for the purpose of illustrating the various failure modes. The grouping does not imply that certain failure modes are applicable only to those events by which they are grouped. Any of the defined failure modes are used for any event type for which the failure mode is relevant and possible.

AAAAA This is a five-letter code for an alphanumeric event descriptor. This field is used to specifically identify the individual components according to their numbering on the system schematics (e.g., 01, 1243, 0A, 1B). Other types of basic events (pipe segment failures, train failures) are also identified according to their designations in the system models. When such specific identification is not applicable, a descriptive abbreviation of the event's nature is appropriate.

Certain symbols were used to construct the system schematics. These are illustrated in Figure 5.3-1.

5.4 Systems Analysis Recommended Reporting

In this task the analysts have spent considerable time and effort in creating the system models for the accident sequences and the plant damage states. These models form the bases in which the quantification of the core damage frequency is estimated and the contributors to core damage are identified. It is important that the reader of the report is given sufficient information to understand how the team analyzed and modeled each system. This information generally includes the following:

- Assumptions. The assumptions that are made in the course of the analysis for each system are discussed.

- System Information. The information used to develop each system model is discussed. This generally includes a brief discussion of: (1) the system description, (2) the system schematic, (3) the system interfaces and dependencies including the dependency diagram, (4) the test and maintenance requirements, (5) the technical specifications, (6) the operating history, and (7) the logic model.

- Fault Trees. Each complete fault tree is included in an appendix in the report.

Table 5.3-1
System Identifiers

System Identifier (XXX)	System Name
ACP	AC Power System
ADS	Automatic Depressurization System
AFW	Auxiliary Feedwater System or Emergency Feedwater System
ARF	Air Return Fan System
CCU	Containment Atmosphere Cleanup
CCW	Component Cooling Water System
CDS	Condensate System
CFC	Containment Emergency Fan Cooler System
CGC	Containment Combustible Gas Control
CHP	Charging Pump System
CHW	Chilled Water System
CIS	Containment Isolation System
CLS	Consequence Limiting Safeguards System
CPC	Charging Pump Cooling System
CSC	Closed Cycle Cooling System
CSR	Containment Spray Recirculation System
CSS	Containment Spray System
CRD	Control Rod Drive System
CVC	Chemical and Volume Control System
DCP	DC Power System
DWS	Drywell (Wetwell) Spray Mode of RHR system
EHV	Emergency Heating, Ventilation, and Air Conditioning System
ESW	Essential Service Water System
FHS	Fuel Handling System
HCI	High Pressure Coolant Injection System (BWR)
HCS	High Pressure Core Spray System
HPI	High Pressure Safety Injection System (PWR)
HPR	High Pressure Recirculation System
HWS	High Pressure Service Water System
IAS	Instrument Air System
ICS	Ice Condenser System
ISR	Inside Containment Spray Recirculation System
ISO	Isolation Condenser System

Table 5.3-1
System Identifiers (Concluded)

System Identifier (XXX)	System Name
LCI	Low Pressure Coolant Injection System (BWR)
LCS	Low Pressure Core Spray System
LPR	Low Pressure Recirculation System
LPI	Low Pressure Safety Injection System (PWR)
MCW	Main Circulating Water System (Main Condenser Cooling System
MFW	Main Feedwater System
MSS	Main Stream System
NHV	Normal Heating, Ventilation, and Air Conditioning System
OEP	Onsite Electric Power System
OSR	Outside Containment Spray Recirculation System
PCS	Power Conversion System
PPS	Primary Pressure Relief System (PORV/SRV)
RBC	Reactor Building Cooling Water system
RCI	Reactor Core Isolation Cooling System
RCS	Reactor Coolant System
RGW	Radioactive Gaseous Waste System
RHR	Residual Heat Removal System
RLW	Radioactive Liquid Waste System
RMT	Recirculation Mode Transfer System
RPS	Reactor Protection System
SDC	Shutdown Cooling Mode of RHR
SGT	Standby Gas Treatment System
SIS	Safety Injection Actuation System
SLC	Standby Liquid Control System
SPC	Suppression Pool Cooling System (or Suppression Pool Cooling Mode of the RHR system
SPM	Suppression Pool Makeup System
SWS	Service Water System
TBC	Turbine Building Cooling Water System

Table 5.3-2
Event and Component Type Identifiers

Component	Identifier (YYY)
Air Cooling Heat Exchanger	ACX
Sensor/Transmitter Units:	
Flow	ASF
Level	ASL
Physical Protection	ASD
Pressure	ASP
Radiation	ASR
Temperature	AST
Flux	ASX
Circuit Breaker	CRB
Calculational Unit	CAL
Electrical Cable	CBL
Signal Conditioner	CND
Control Rods:	
Hydraulically-Driven	CRH
Motor-Driven	CRM
Ducting	DCT
Motor-Driven Compressor	MDC
Motor-Driven Fan	FAN
Fuse	FUS
Diesel Generator	DGN
Hydrogen Recombiner Unit	HRU
Heat Exchanger	HTX
Inverter	INV
Electrical Isolation Device	ISO
Air Cleaning Unit	ACU
Load/Relay Unit	LOD

Table 5.3-2
Event and Component Type Identifiers (Continued)

Component	Identifier (YYY)
Logic Unit	LOG
Local Power Supply	LPS
Motor-Generator Unit	MGN
Motor-Operated Damper	MOD
Pumps:	
Engine-Driven	EDP
Motor-Driven	MDP
Turbine-Driven	TDP
Manual Control Switch	XSW
Rectifier	REC
Transfer Switch	TSW
Transformer	TFM
Tank	TNK
Bistable Trip Unit	TXX
Air Heating Unit	AHU
Electrical Bus - DC	BDC
Electrical Bus - AC	BAC
Manual Damper	XDM
Pneumatic/Hydraulic Damper	PND
Battery	BAT
Valves:	
Check Valve	CKV
Hydraulic Valve	HDV
Safety Relief Valve	SRV
Solenoid-Operated Valve	SOV
Motor-Operated Valve	MOV
Manual Valve	XVM
Air-Operated Valve	AOV
Testable Check Valve	TCV
Explosive Valve	EPV

Table 5.3-2
Event and Component Type Identifiers (Concluded)

Component	Identifier (YYY)
Filter	FLT
Instrument and Control Circuit	ICC
Strainer	STR
Heater Element	HTR
Pipe Segment	PSF
Pipe Train	PTF
Actuation Segment	ACS
Actuation Train	ACT
AC Electrical Train	TAC
DC Electrical Train	TDC
Operator Action	XHE
Common Cause Event	CCF
Miscellaneous Aggregation of Events	VFC
Phenomenological Events	PHN

Table 5.3-3
Failure Mode Codes

Failure Mode	Code (ZZ)
Valves, Contacts, Dampers	
Fail to Transfer	FT
Normally Open, Fail Open (Fails to close)	OO
Normally Open, Fail Closed	OC
Normally Closed, Fail Open	CO
Normally Closed, Fail Closed (Fails to open)	CC
Valves, Filters, Orifices, Nozzles	
Plugged	PG
Pumps, Motors, Diesels, Turbines, Fans Compressors	
Fail to Start	FS
Fail to Continue Running	FR
Sensors, Signal Conditioners, Bistable	
Fail High	HI
Fail Low	LO
No Output	NO
Segments, Trains, and Miscellaneous Agglomerations	
Loss of Flow, No Flow	LF
Loss of Function	FC
Actuation Fails	FA
No Power, Loss of Power	LP
Failure (for miscellaneous fault agglomerations not based on segments or trains)	VF
Hardware	HW
Battery, Bus, Transformer	
No Power, Loss of Power	LP
Short	ST
Open	OP
Tank, Pipes, Seals, Tubes	
Leak	LK
Rupture	RP

Table 5.3-3
Failure Mode Codes

Failure Mode	Code (ZZ)
Human Errors	
Fail to Operate	FO
Miscalibrate	MC
Fail to Restore from Test or Maintenance	RE
Normal Operations (unavailable because of planned activity)	
Maintenance	MA
Test	TE
Test and Maintenance	TM

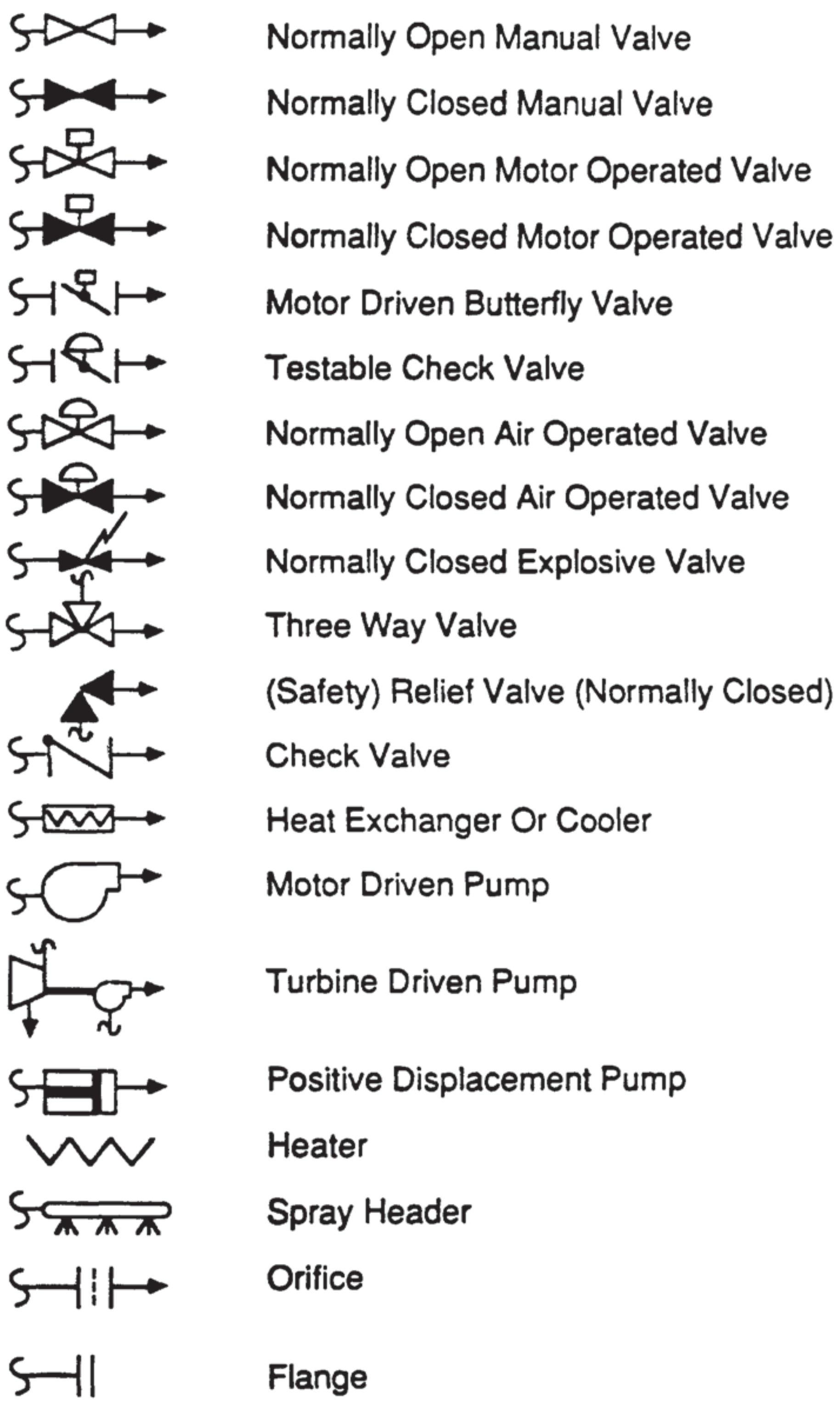

Normally Open Manual Valve
Normally Closed Manual Valve
Normally Open Motor Operated Valve
Normally Closed Motor Operated Valve
Motor Driven Butterfly Valve
Testable Check Valve
Normally Open Air Operated Valve
Normally Closed Air Operated Valve
Normally Closed Explosive Valve
Three Way Valve
(Safety) Relief Valve (Normally Closed)
Check Valve
Heat Exchanger Or Cooler
Motor Driven Pump
Turbine Driven Pump
Positive Displacement Pump
Heater
Spray Header
Orifice
Flange

Figure 5.3-1. Symbols Used in Drawing System Schematics (Page 1 of 3).

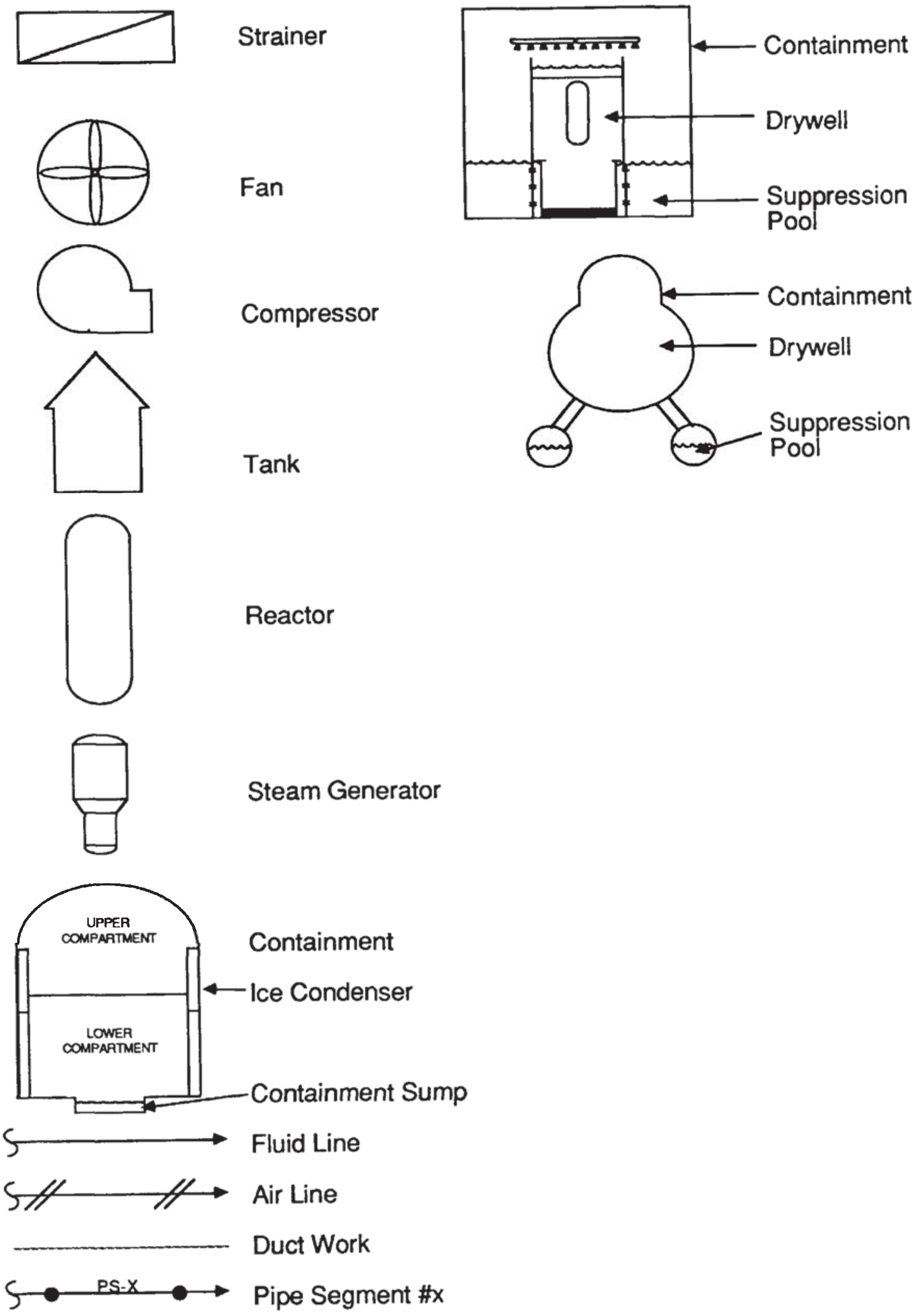


Figure 5.3-1. Symbols Used in Drawing System Schematics (Page 2 of 3).

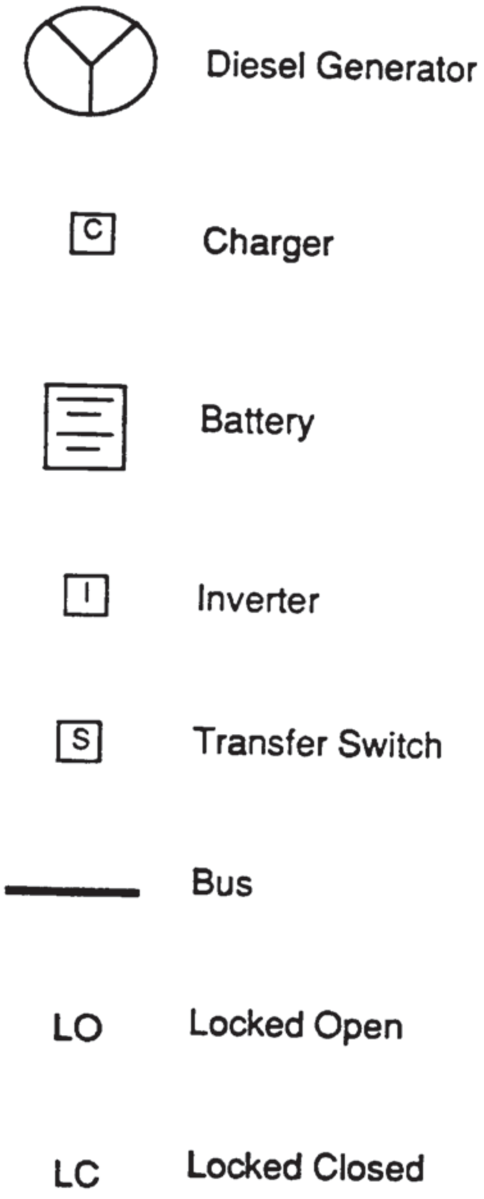


Figure 5.3-1. Symbols Used in Drawing Schematics (Page 3 of 3)

5.5 Example of Systems Analysis

The systems analysis task example is presented using the step-by-step technique previously described. Each step contains an example from the Peach Bottom study. Any pertinent information is also included.

Step 5.1 Select Systems

The Peach Bottom study selected 22 systems requiring models (see Table 5.5-1). The front-line systems were identified by the success criteria in the Accident Sequence Initiating Event analysis task. The support systems are those required to operate in order for the front-line systems to function properly.

One front-line system, Low Pressure Core Spray (LPCS), was chosen to illustrate the systems analysis task. The other 21 systems are approached in a similar manner, depending on the detail in the fault tree justified by the importance of the system to the overall analysis.

Step 5.2 Obtain System Information

Any information necessary to develop the system model is gathered. The following paragraphs describe the information gathered for the development of the LPCS model.

LPCS Description

The function of the LPCS system is to provide coolant makeup to the reactor vessel during accidents in which system pressure is low (event tree nomenclature--V2). The Automatic Depressurization System (ADS) can be used to reduce system pressure sufficiently for injection to occur.

The LPCS system is a two-loop system consisting of motor-operated valves and motor driven pumps. There are two fifty percent capacity pumps per loop, with each pump rated at 3125 gpm with a discharge head of 105 psig. The normal LPCS system suction source is the suppression pool. Pump suction can be manually realigned to the CST.

The LPCS system is automatically initiated and controlled. Operator action is required to manually start the system given an auto-start failure and to stop the system or manually control flow during an Anticipated Transient Without Scram (ATWS) if required.

The success criterion for the LPCS system is injection of flow from any two pumps to the reactor vessel.

Most of the LPCS system is located in the reactor building so that its operation could be affected by either containment venting or containment failure. Room cooling failure is assumed to fail the LPCS pumps in ten hours.

Table 5.5-1.
Systems Included in the Peach Bottom Study

SYSTEM	TYPE OF MODEL
Actuation and Control (ESF)	Fault Tree
Automatic and Manual Depressurization (ADS)	Fault Tree
Condensate (CDS)	Fault Tree
Containment Spray (CSS)	Fault Tree
Control Rod Drive (CRD)	Fault Tree
Electric Power (ACP,DCP)	Fault Tree
Emergency Service Water (ESW)	Fault Tree
Emergency Ventilation (EHV)	Fault Tree
High Pressure Coolant Injection (HCI)	Fault Tree
High Pressure Service Water (HSW)	Fault Tree
Instrument Air (IAS)	Fault Tree
Low Pressure Coolant Injection (LCI)	Fault Tree
Low Pressure Core Spray (LCS)	Fault Tree
Primary Containment Venting (PCV)	Fault Tree
Reactor Building Cooling Water (RBC)	Fault Tree
Reactor Core Isolation Cooling (RCI)	Fault Tree
Shutdown Cooling (SDC)	Fault Tree
Standby Liquid Control (SLC)	Fault Tree
Suppression Pool Cooling (RHR/SPC)	Fault Tree
Turbine Building Cooling (TBC)	Fault Tree
Reactor Protection (RPS)	Data Value
Power Conversion (PCS)	Data Value

LPCS Interfaces and Dependencies

Each LPCS pump is powered from a separate 4160 VAC bus with control and actuation power being supplied by a separate 125 VDC bus. All pumps require cooling.

Each normally closed injection valve is powered from a separate 480 VAC bus (480 VAC/C for Loop A, 480 VAC/D for Loop B).

Upon the receipt of a LPCS injection signal, start signals are sent to all LPCS pumps, open signals are sent to both injection valves, and close signals are sent to the test return valves. The LPCS system is automatically initiated on the receipt of either a low-low reactor water level (378 inches above vessel zero) or high drywell pressure (2 psig) and low reactor pressure (450 psig). All actuation sensors are shared with the LPCI system.

LPCS actuation and control circuitry is divided into two divisions. Division A is associated with the actuation and control of the components in Loop A, and Division B is associated with the actuation and control of the components in Loop B.

Each LPCS pump has a minimum flow line valve (normally open) which is sent an open signal given a pump start.

Both injection valves are prohibited from opening unless a low reactor pressure permissive (450 psig) is met.

LPCS Test and Maintenance

The LPCS system surveillance requirements are the following: (1) pump operability--once/month, (2) MOV operability--once/month, (3) pump capacity test--once/three months, (4) simulated automatic actuation test--once/operating cycle, and (5) logic system functional test--once/six months.

LPCS Technical Specifications

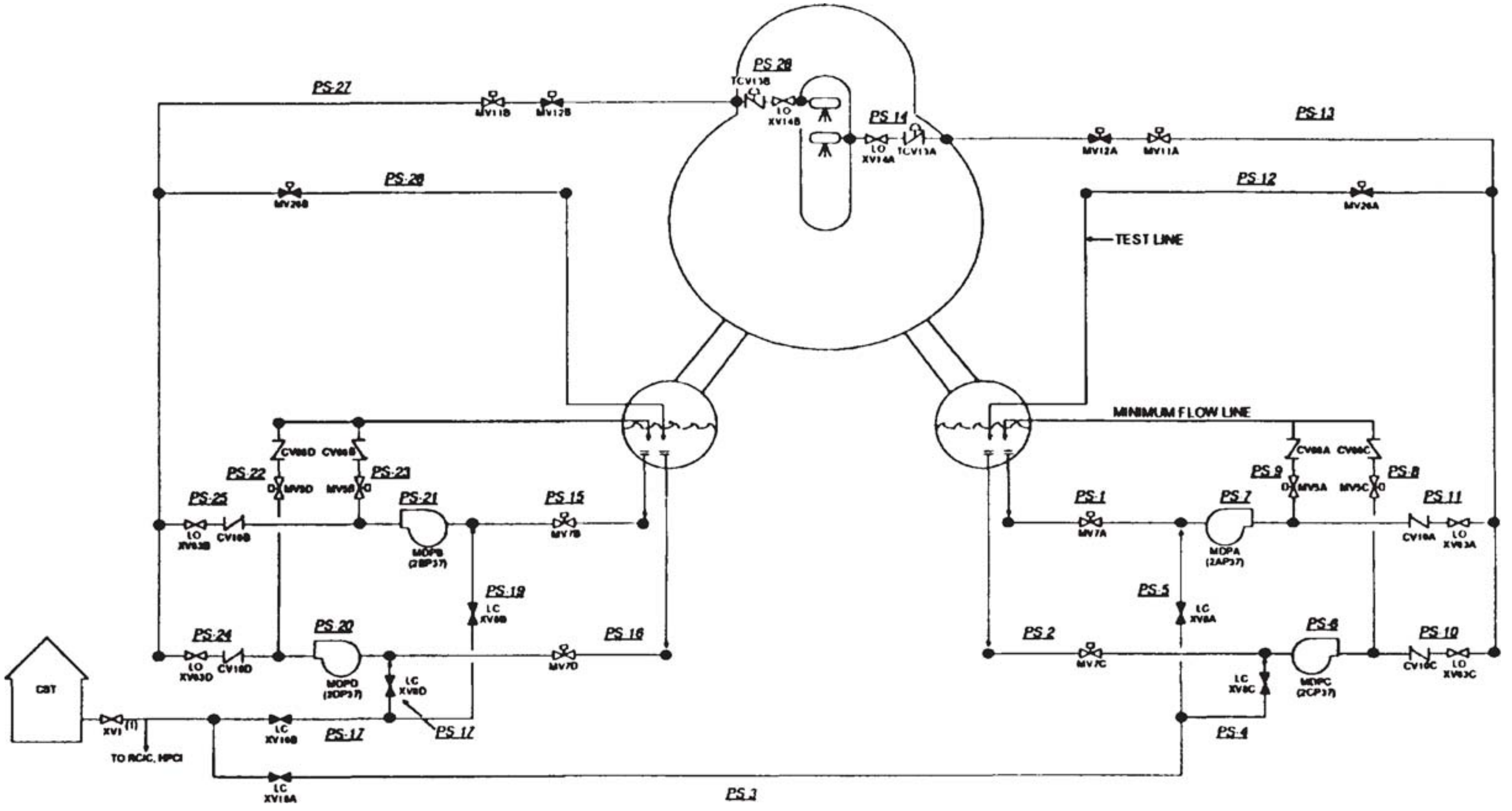
If any one LPCS loop is made or found to be inoperable for any reason, continued reactor operation is permissible for seven days provided that the remaining LPCS loop and the LPCI system are operable. If this requirement cannot be met, the reactor is to be shut down.

LPCS Operation Experience

Nothing was peculiar in the operational history of the LPCS system which would affect either system modeling or failure data.

Step 5.3 Develop System Schematic

A simplified schematic of the LPCS system is developed that represents the system as defined in the analysis (see Figure 5.5-1). This schematic was developed using the criteria outlined in Section 5.2, Step 5.3. Major



VALVE POSITIONS ARE SHOWN IN THEIR STANDBY POSITION
(1) VALVE ALSO LOCATED ON HPCI SCHEMATIC, SEE HPCI SCHEMATIC FOR DEFINITION OF PIPE SEGMENT

Figure 5.5-1. Low Pressure Core Spray System Schematic

components are shown as is the pipe segment definition (e.g., PS-27) used in the system fault tree.

Step 5.4 Review System Information

The information gathered in Step 5.2 is reviewed to identify the potential failure modes of the LPCS system. For example, in Loop B (Figure 5.5-1) when LPCS is required, i.e., on low, low reactor water level or high drywell pressure and low reactor pressure, the motor driven pumps (MDPB and MDPD) must start, motor operated valve (MV 12B) must open, and motor operated valve (MV 24B) must close). If MV12 fails to open, core spray is prevented. If MV 24B remains open, some flow is diverted and core cooling may be inadequate. Reactor vessel pressure must be less than 450 psig in order for MV 12B to open.

Step 5.5 Develop System Dependency Diagrams

The LPCS system dependency diagram is shown as Figure 5.5-2. The top gate of the dependency diagram has been simplified since there are numerous combinations of valve and pump failures which result in the failure of LPCS (see Step 5.6).

The significance of the LPCS dependency diagram lies in indicating which support systems are required for operation of each train and component necessary for the operation of LPCS.

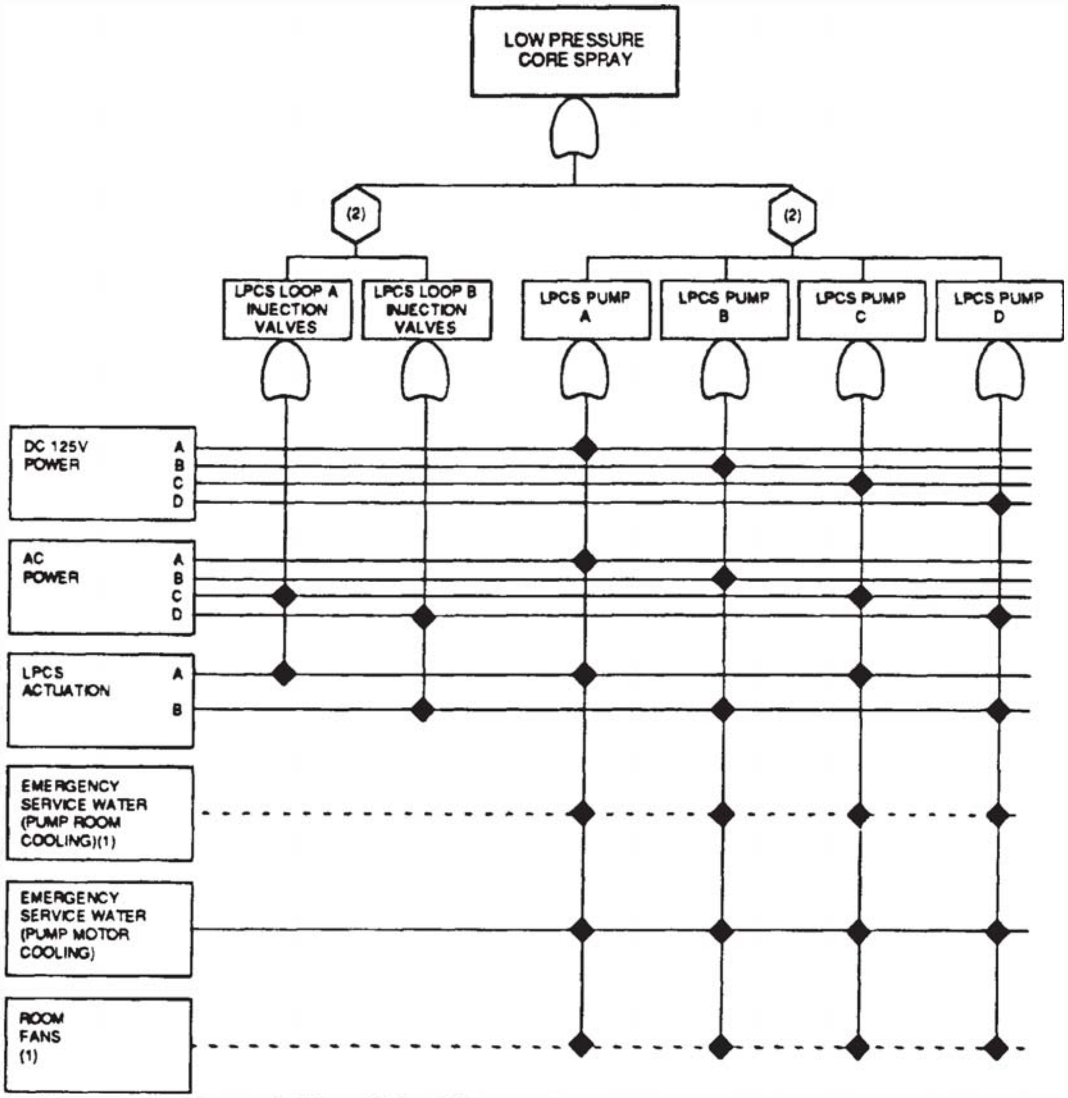
The blackened diamonds are the areas of dependency, e.g., the LPCS Loop A Injection Valves fail if either AC Power Bus C or LPCS Actuation Train A fails. The dashed lines indicate that the support system is required only for long-term operation (e.g., room fans for all LPCS pumps).

Step 5.6 Determine System Failure Modes

A preliminary examination of the LPCS system was undertaken, comparing LPCS against the failure mechanisms discussed in Section 5.2, Step 5.6. Common mode failure of the LPCS pumps, the output injection valves in each train, and other system level failure modes, in addition to various component failures were identified as potential failures to be modeled. Component failures included: pump failure to start, failure to run, failure to restore after maintenance and out due to maintenance, motor-operated valve failure to close, failure to open, plugged, failure to restore after maintenance and out due to maintenance. The support systems to be incorporated into the LPCS system model are those indicated in Step 5.5 (see Figure 5.5-2).

Step 5.7 Select System Model

A detailed fault tree, one which models all the system components shown on the schematic (Figure 5.5-1) plus all possible failure modes was chosen as the appropriate model for the LPCS system analysis.


LOW PRESSURE CORE SPRAY
(2)
(2)
LPCS LOOP A INJECTION VALVES
LPCS LOOP B INJECTION VALVES
LPCS PUMP A
LPCS PUMP B
LPCS PUMP C
LPCS PUMP D
DC 125V POWER
A
B
C
D
AC POWER
A
B
C
D
LPCS ACTUATION
A
B
EMERGENCY SERVICE WATER (PUMP ROOM COOLING)(1)
EMERGENCY SERVICE WATER (PUMP MOTOR COOLING)
ROOM FANS (1)

Dependency Diagram Is Shown Using Failure Logic.

(1) Dependency Not Required During Short Term Operation.

(2) See LPCS Fault Tree For Success Criteria.

Figure 5.5-2. Low Pressure Core Spray System Dependency Diagram

Step 5.8 Define System Failure Criteria

The LPCS system success criterion is flow from any two pumps to the reactor vessel. The success criterion is converted into a system failure statement. System failure occurs if injection flow to the reactor vessel is limited to one pump (see Figure 5.5-1); that is, the Loop A injection line (PS-14) fails and Pump B or D in Loop B fails, the Loop B injection line (PS-28) fails and Pump A or C in Loop A fails, or the Loop A and Loop B injection lines both fail).

Step 5.9 Construct System Model

The fault tree analysis specifies an undesired state of the system. The undesired event serves as the top event of the fault tree and is the starting point of the analysis. The top event for the LPCS system is no flow to the reactor vessel from 2 of the 4 LPCS pump trains.

Once the top event is established, credible events and combinations of events which might produce that system state are identified. The analysis provides a means of answering the question, "In what ways can this system fail?" The answer to this question is developed relative to the top event of the fault tree.

There were five combinations of failures identified that can fail the LPCS system; no flow from Loop A (PS-14) and Loop B (PS-28) injection lines, no flow from Loop A and Pump B (PS-25) or Pump D (PS-24), no flow from Loop B and Pump C (PS-10) or Pump A (PS-11), common mode failure of all LPCS pumps and common mode failure of the LPCS injection valves (see Section 6.5 for discussion of these latter two combinations). An OR gate is used with these failure modes since the output event (no flow to reactor vessel from 2 of 4 LPCS pump trains) occurs if one or more of the inputs (the 5 failure modes) occur. An AND gate is used if and only if all of the input events occur. The LPCS fault tree is presented as Figure 5.5-3.

Based upon analysis discussed in Section 6.5, the common mode failure of the pumps and injection valves are modeled as basic events. The three failure combinations not modeled as basic events are modeled with several levels, each level providing more detail. The event, no flow from Loop A and Loop B injection lines [LCS-2], can occur when there is a combination of no flow from the Loop A [LCS-5] and no flow from the Loop B [LPC-6] injection lines. The next level separately details both of these events. The LCS-5 event can occur when either no flow from PS-13 [LCS-7] or a hardware failure of the LPCS Loop A injection line [LCS-5A] occurs. The LCS-5A event occurs when either testable check valve 13A fails to open or manual valve 14A plugs. This is the level of resolution chosen for these components; therefore, at this point they are modeled as basic events. The level of resolution chosen typically requires assumptions to be made. The LPCS system has 11 assumptions which are listed in the following paragraphs. The remainder of the paths through the LPCS fault tree are developed in a similar manner.

LPCS Assumptions

(1) Incorrect positioning of all manual and motor-operated valves after testing and maintenance is considered to be negligible because positions of these valves are indicated in the control room. Test diverting flow causing LPCS system failure is also felt to be negligible since valves receive signals to close from both Divisions A and B actuation circuitry. The injection valves receive open signals on a real demand. Thus, unavailability due to testing and failure to restore after testing is not important.

(2) During construction of the fault tree, it was necessary to determine which components could be taken out of service (OOS) for maintenance. Maintenance would require components to be effectively removed from the system. Standard safety precautions of component isolation were used to decide which components could be taken OOS for maintenance while the plant was at power or normal operating pressure. The general guidelines used for the component isolation were double blockage for high pressure piping or components and single blockage for low pressure piping or components.

(3) Pump isolation because of spurious signals is assumed to be negligible compared to other system faults.

(4) The LPCS actuation circuitry was not modeled at a great level of detail. Only those elements considered potentially important were included in the fault tree model. Hardware failures of relays and permissives were grouped into one term. The initiating signal sensors and associated support systems were explicitly modeled because they are shared between various ESF systems.

(5) Based on a Philadelphia Electric Company response, the LPCS pumps will fail because of insufficient net positive suction head (NPSH) once the suppression pool has reached saturated conditions.

(6) The Condensate Storage Tank (CST) is an alternate suction source which must be manually valved in and therefore is not explicitly included in the model, but it can be handled as a recovery action.

(7) The LPCS pumps do not trip on low pump suction pressure.

(8) The uravailability of the LPCS pumps from testing does not defeat a real demand from operating the system. Therefore, it was not considered. Failure to restore the LPCS pumps after testing does not apply.

(9) Failure of the suppression pool because of random failure or the plugging of all its strainers is assumed to be negligible compared to other system failures.

(10) It is assumed that calibration of the low and low-low reactor water level sensors is performed at the same time. Miscalibration of these sensors is considered to be the same event.

(11) Failure of room cooling (if not recovered) is assumed to fail LPCS in ten hours. This is based on utility calculations which demonstrate that for approximately 50 hours or more without room cooling, operability is expected even with continuous pump operation. The ten hour LPCS failure value was chosen to be consistent with the general assumptions made for HPCI and RCIC. It is a conservative value.

Step 5.10 Identify Basic Events

Every path through the fault tree ultimately leads to a basic event. Each basic event requires a data value before further analysis can occur. The values are determined by utilizing the techniques in Sections 6, 7, and 8.

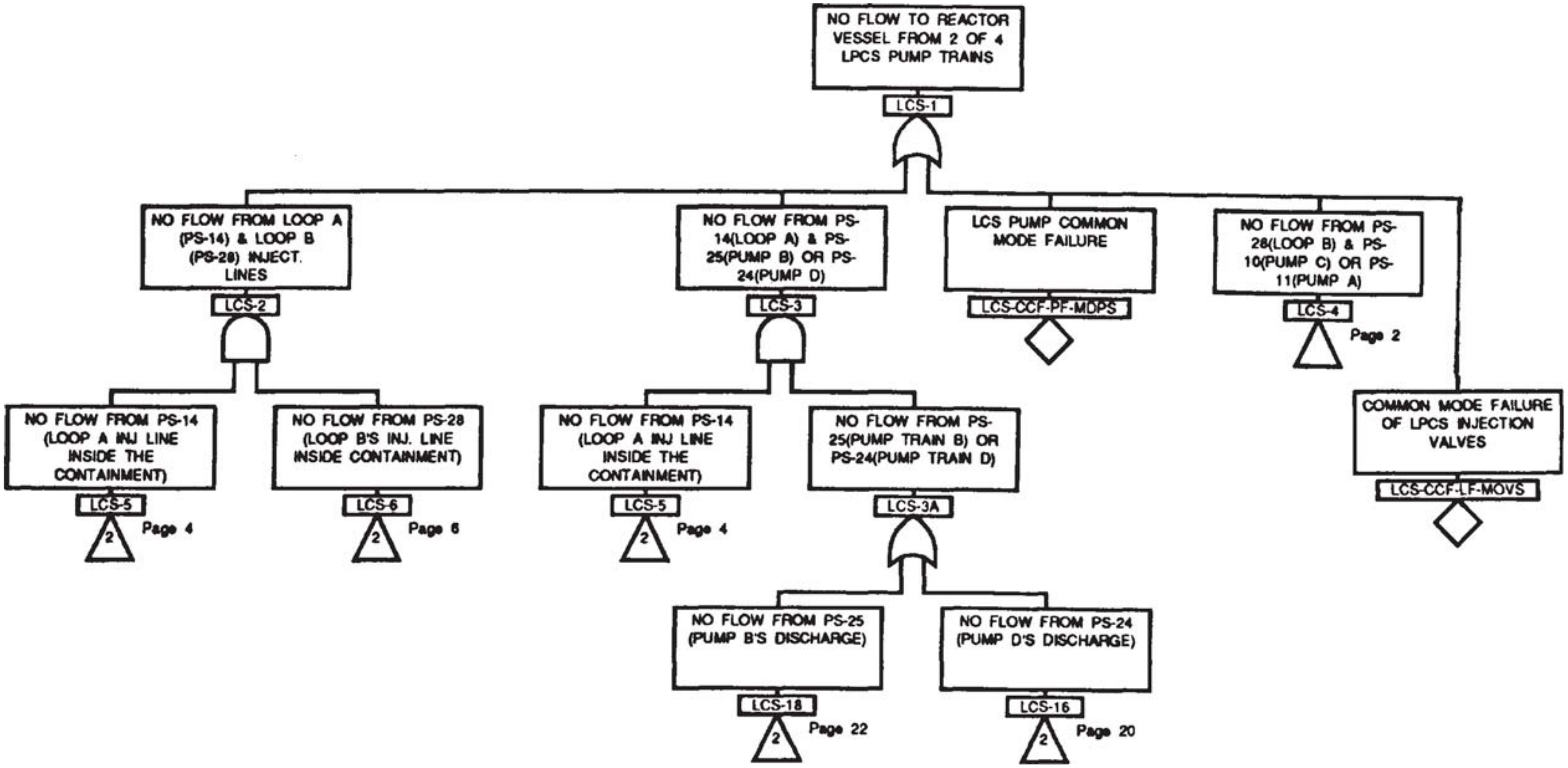

NO FLOW TO REACTOR VESSEL FROM 2 OF 4 LPCS PUMP TRAINS
LCS-1
NO FLOW FROM LOOP A (PS-14) & LOOP B (PS-28) INJECT. LINES
LCS-2
NO FLOW FROM PS-14(LOOP A) & PS-25(PUMP B) OR PS-24(PUMP D)
LCS-3
LCS PUMP COMMON MODE FAILURE
LCS-CCF-PF-MDPS
NO FLOW FROM PS-28(LOOP B) & PS-10(PUMP C) OR PS-11(PUMP A)
LCS-4
Page 2
COMMON MODE FAILURE OF LPCS INJECTION VALVES
LCS-CCF-LF-MOVS
NO FLOW FROM PS-14 (LOOP A INJ LINE INSIDE THE CONTAINMENT)
LCS-5
2
Page 4
NO FLOW FROM PS-28 (LOOP B'S INJ. LINE INSIDE CONTAINMENT)
LCS-6
2
Page 6
NO FLOW FROM PS-14 (LOOP A INJ LINE INSIDE THE CONTAINMENT)
LCS-5
2
Page 4
NO FLOW FROM PS-25(PUMP TRAIN B) OR PS-24(PUMP TRAIN D)
LCS-3A
NO FLOW FROM PS-25 (PUMP B'S DISCHARGE)
LCS-18
2
Page 22
NO FLOW FROM PS-24 (PUMP D'S DISCHARGE)
LCS-16
2
Page 20

Figure 5.5-3. LPCS Fault Tree (Page 1 of 35)

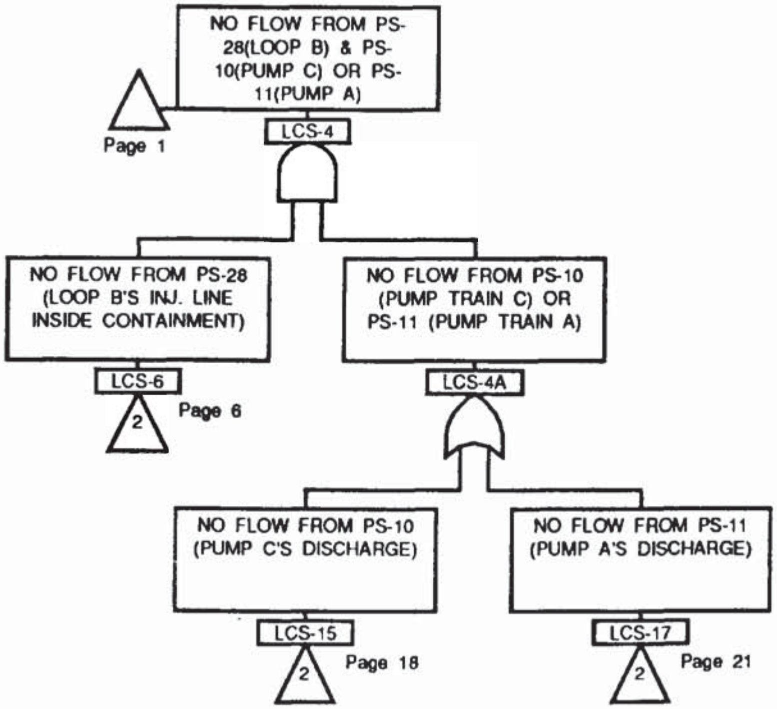

NO FLOW FROM PS-28(LOOP B) & PS-10(PUMP C) OR PS-11(PUMP A)
Page 1
LCS-4
NO FLOW FROM PS-28 (LOOP B'S INJ. LINE INSIDE CONTAINMENT)
LCS-6
2
Page 6
NO FLOW FROM PS-10 (PUMP TRAIN C) OR PS-11 (PUMP TRAIN A)
LCS-4A
NO FLOW FROM PS-10 (PUMP C'S DISCHARGE)
LCS-15
2
Page 18
NO FLOW FROM PS-11 (PUMP A'S DISCHARGE)
LCS-17
2
Page 21

Figure 5.5-3. LPCS Fault Tree (Page 2 of 35)

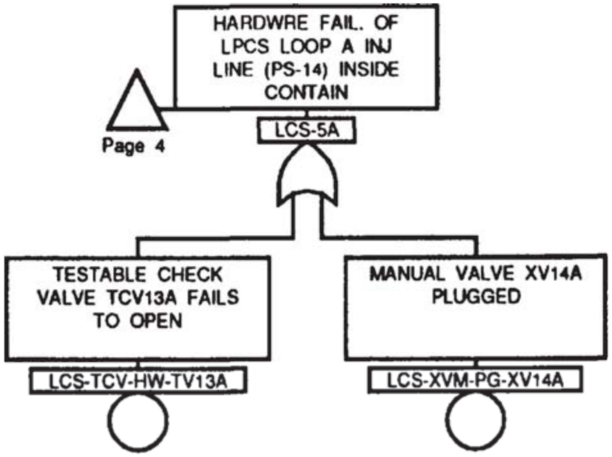

HARDWRE FAIL. OF LPCS LOOP A INJ LINE (PS-14) INSIDE CONTAIN
LCS-5A
Page 4
TESTABLE CHECK VALVE TCV13A FAILS TO OPEN
LCS-TCV-HW-TV13A
MANUAL VALVE XV14A PLUGGED
LCS-XVM-PG-XV14A

Figure 5.5-3. LPCS Fault Tree (Page 3 of 35)

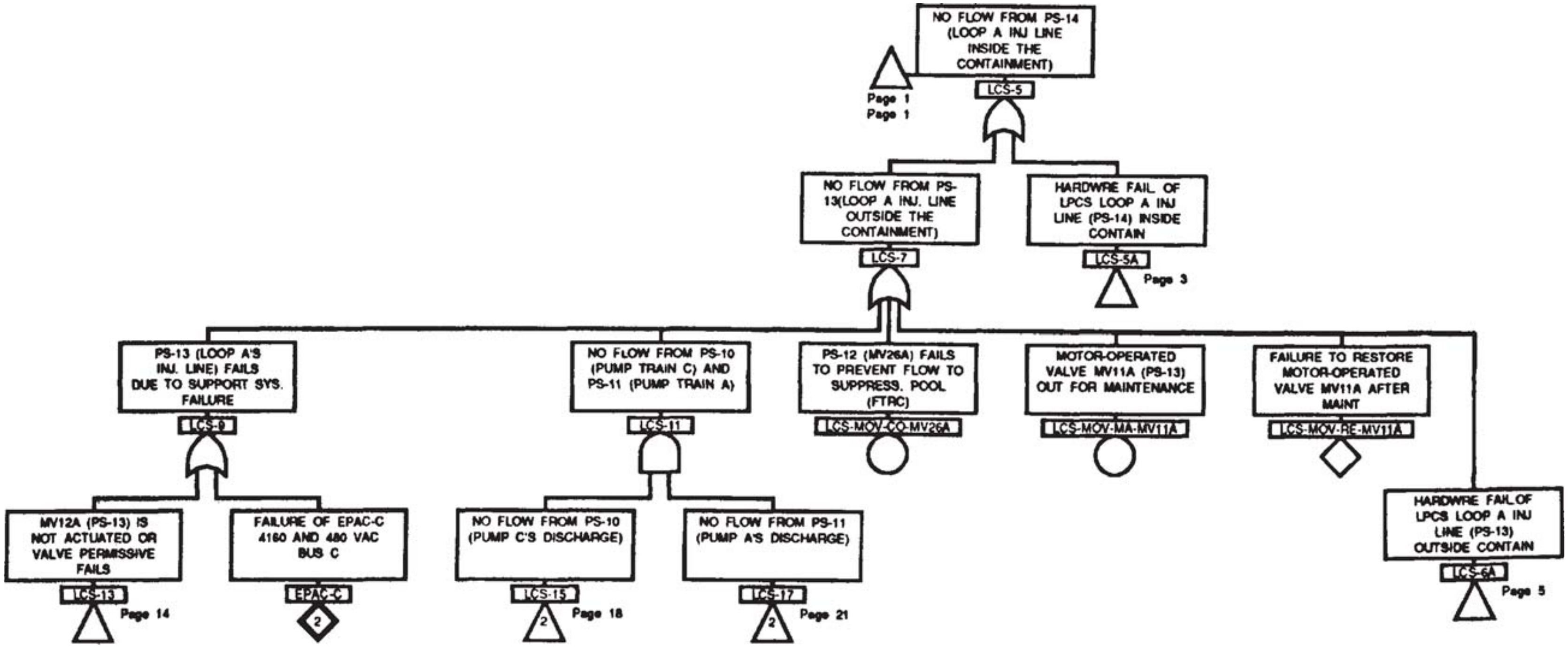

NO FLOW FROM PS-14 (LOOP A INJ LINE INSIDE THE CONTAINMENT)
LCS-5
Page 1
Page 1
NO FLOW FROM PS-13(LOOP A INJ. LINE OUTSIDE THE CONTAINMENT)
LCS-7
HARDWRE FAIL OF LPCS LOOP A INJ LINE (PS-14) INSIDE CONTAIN
LCS-5A
Page 3
PS-13 (LOOP A'S INJ. LINE) FAILS DUE TO SUPPORT SYS. FAILURE
LCS-9
NO FLOW FROM PS-10 (PUMP TRAIN C) AND PS-11 (PUMP TRAIN A)
LCS-11
PS-12 (MV26A) FAILS TO PREVENT FLOW TO SUPPRESS. POOL (FTRC)
LCS-MOV-CO-MV26A
MOTOR-OPERATED VALVE MV11A (PS-13) OUT FOR MAINTENANCE
LCS-MOV-MA-MV11A
FAILURE TO RESTORE MOTOR-OPERATED VALVE MV11A AFTER MAINT
LCS-MOV-RE-MV11A
HARDWRE FAIL OF LPCS LOOP A INJ LINE (PS-13) OUTSIDE CONTAIN
LCS-6A
Page 5
MV12A (PS-13) IS NOT ACTUATED OR VALVE PERMISSIVE FAILS
LCS-13
Page 14
FAILURE OF EPAC-C 4160 AND 480 VAC BUS C
EPAC-C
2
NO FLOW FROM PS-10 (PUMP C'S DISCHARGE)
LCS-15
2
Page 18
NO FLOW FROM PS-11 (PUMP A'S DISCHARGE)
LCS-17
2
Page 21

Figure 5.5-3. LPCS Fault Tree (Page 4 of 35)

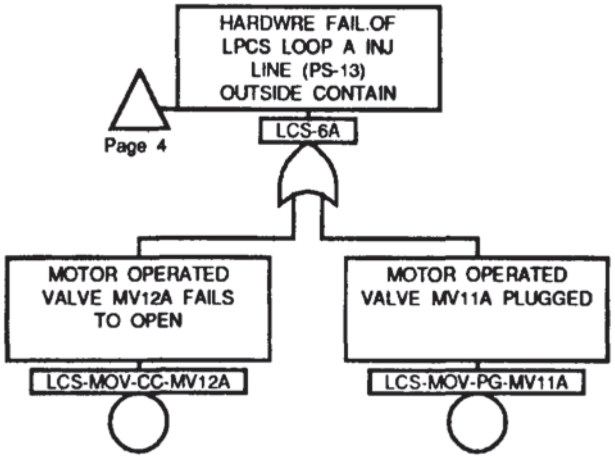

HARDWRE FAIL.OF LPCS LOOP A INJ LINE (PS-13) OUTSIDE CONTAIN
LCS-6A
Page 4
MOTOR OPERATED VALVE MV12A FAILS TO OPEN
LCS-MOV-CC-MV12A
MOTOR OPERATED VALVE MV11A PLUGGED
LCS-MOV-PG-MV11A

Figure 5.5-3. LPCS Fault Tree (Page 5 of 35)

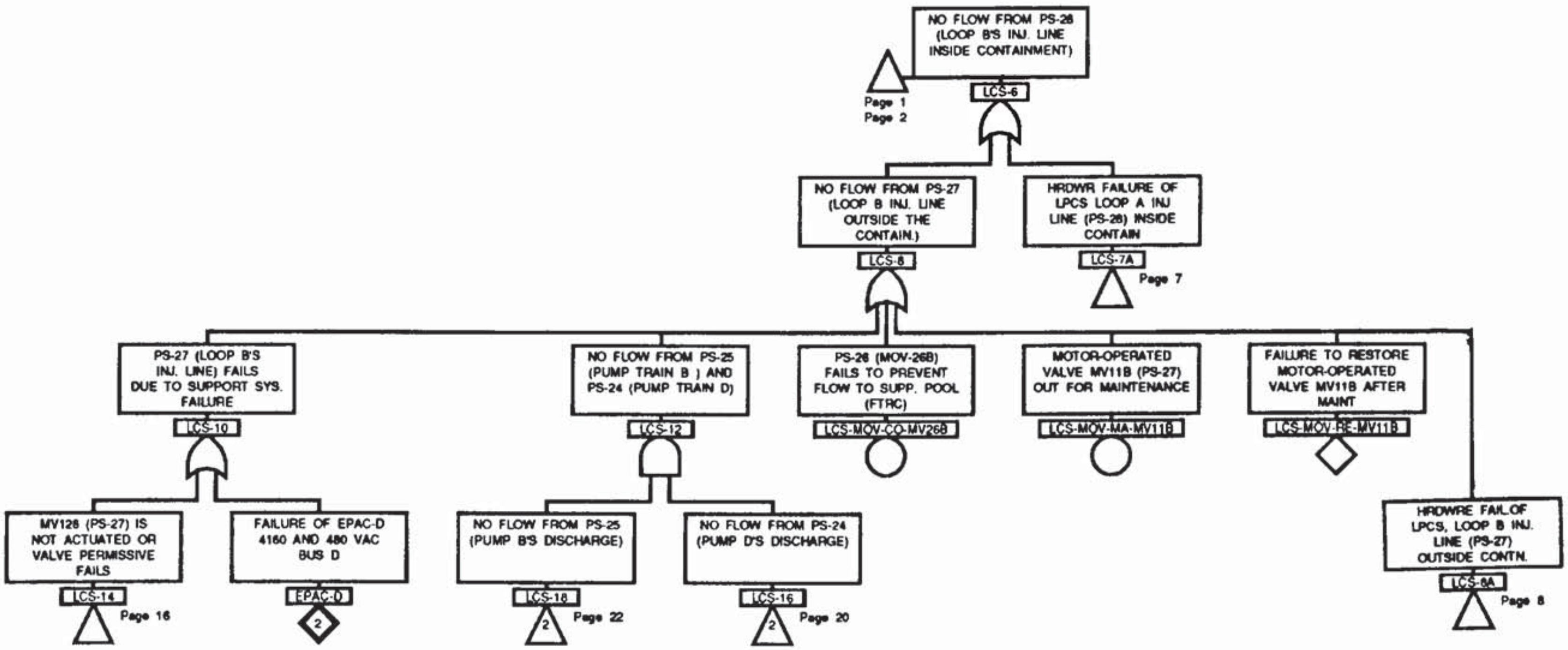

NO FLOW FROM PS-28 (LOOP B'S INJ. LINE INSIDE CONTAINMENT)
Page 1
Page 2
LCS-6
NO FLOW FROM PS-27 (LOOP B INJ. LINE OUTSIDE THE CONTAIN.)
LCS-8
HRDWR FAILURE OF LPCS LOOP A INJ LINE (PS-28) INSIDE CONTAIN
LCS-7A
Page 7
PS-27 (LOOP B'S INJ. LINE) FAILS DUE TO SUPPORT SYS. FAILURE
LCS-10
NO FLOW FROM PS-25 (PUMP TRAIN B) AND PS-24 (PUMP TRAIN D)
LCS-12
PS-28 (MOV-26B) FAILS TO PREVENT FLOW TO SUPP. POOL (FTRC)
LCS-MOV-CO-MV26B
MOTOR-OPERATED VALVE MV11B (PS-27) OUT FOR MAINTENANCE
LCS-MOV-MA-MV11B
FAILURE TO RESTORE MOTOR-OPERATED VALVE MV11B AFTER MAINT
LCS-MOV-RE-MV11B
MV128 (PS-27) IS NOT ACTUATED OR VALVE PERMISSIVE FAILS
LCS-14
Page 16
FAILURE OF EPAC-D 4160 AND 480 VAC BUS D
EPAC-D
2
NO FLOW FROM PS-25 (PUMP B'S DISCHARGE)
LCS-18
2
Page 22
NO FLOW FROM PS-24 (PUMP D'S DISCHARGE)
LCS-16
2
Page 20
HRDWRE FAIL.OF LPCS, LOOP B INJ. LINE (PS-27) OUTSIDE CONTN.
LCS-8A
Page 8

Figure 5.5-3. LPCS Fault Tree (Page 6 of 35)

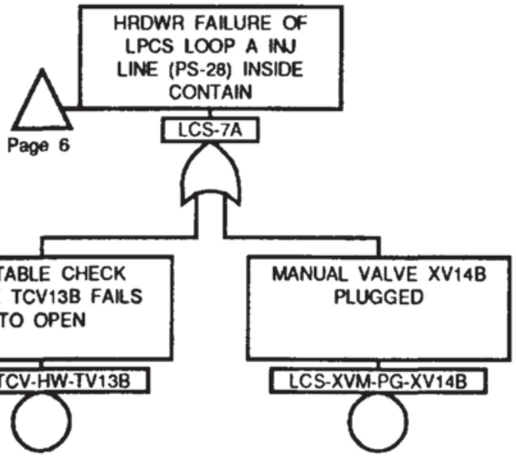

HRDWR FAILURE OF LPCS LOOP A INJ LINE (PS-28) INSIDE CONTAIN
LCS-7A
Page 6
TESTABLE CHECK VALVE TCV13B FAILS TO OPEN
LCS-TCV-HW-TV13B
MANUAL VALVE XV14B PLUGGED
LCS-XVM-PG-XV14B

Figure 5.5-3. LPCS Fault Tree (Page 7 of 35)

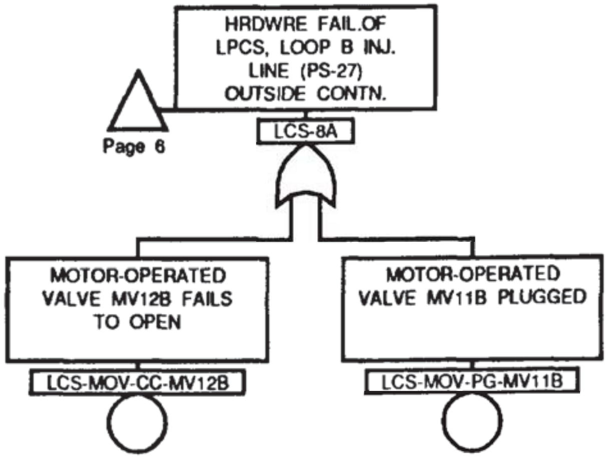

HRDWRE FAIL.OF LPCS, LOOP B INJ. LINE (PS-27) OUTSIDE CONTN.
LCS-8A
Page 6
MOTOR-OPERATED VALVE MV12B FAILS TO OPEN
LCS-MOV-CC-MV12B
MOTOR-OPERATED VALVE MV11B PLUGGED
LCS-MOV-PG-MV11B

Figure 5.5-3. LPCS Fault Tree (Page 8 of 35)

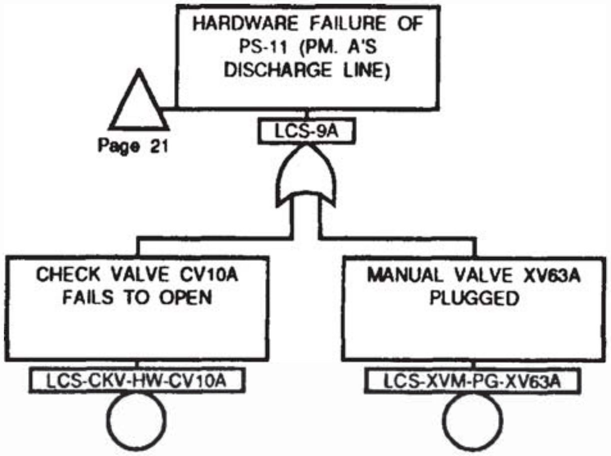

HARDWARE FAILURE OF PS-11 (PM. A'S DISCHARGE LINE)
LCS-9A
Page 21
CHECK VALVE CV10A FAILS TO OPEN
LCS-CKV-HW-CV10A
MANUAL VALVE XV63A PLUGGED
LCS-XVM-PG-XV63A

Figure 5.5-3. LPCS Fault Tree (Page 9 of 35)

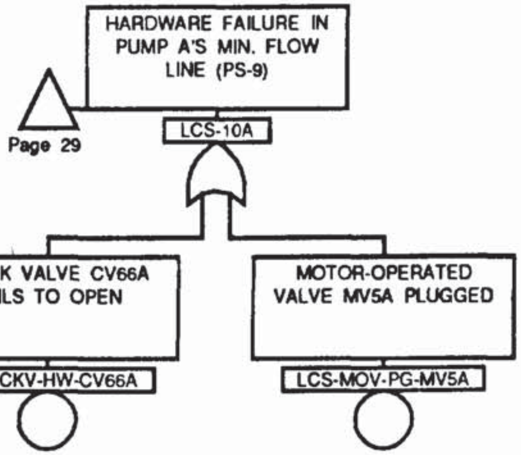

HARDWARE FAILURE IN PUMP A'S MIN. FLOW LINE (PS-9)
Page 29
LCS-10A
CHECK VALVE CV66A FAILS TO OPEN
LCS-CKV-HW-CV66A
MOTOR-OPERATED VALVE MV5A PLUGGED
LCS-MOV-PG-MV5A

Figure 5.5-3. LPCS Fault Tree (Page 10 of 35)

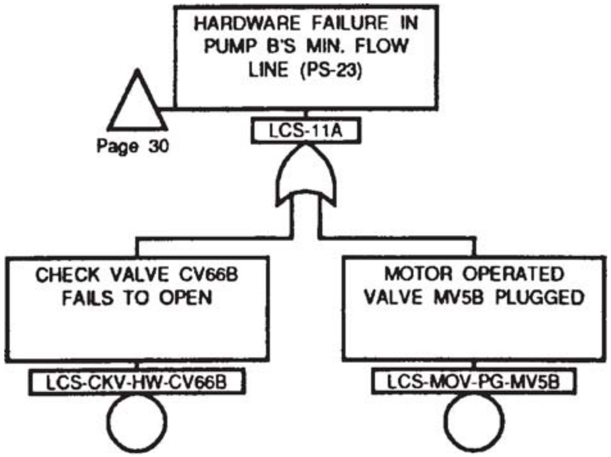

HARDWARE FAILURE IN PUMP B'S MIN. FLOW LINE (PS-23)
LCS-11A
Page 30
CHECK VALVE CV66B FAILS TO OPEN
LCS-CKV-HW-CV66B
MOTOR OPERATED VALVE MV5B PLUGGED
LCS-MOV-PG-MV5B

Figure 5.5-3. LPCS Fault Tree (Page 11 of 35)

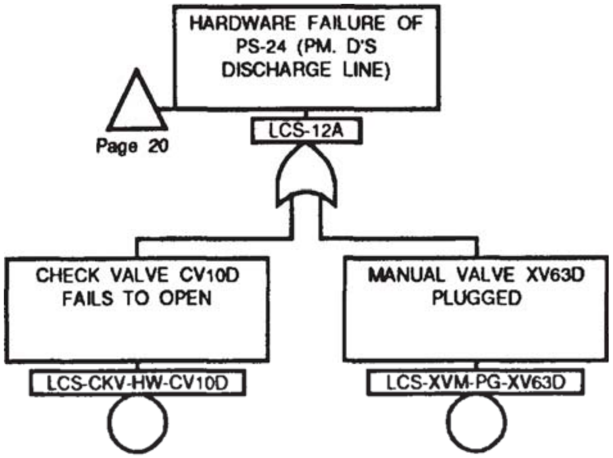

HARDWARE FAILURE OF PS-24 (PM. D'S DISCHARGE LINE)
Page 20
LCS-12A
CHECK VALVE CV10D FAILS TO OPEN
MANUAL VALVE XV63D PLUGGED
LCS-CKV-HW-CV10D
LCS-XVM-PG-XV63D

Figure 5.5-3. LPCS Fault Tree (Page 12 of 35)

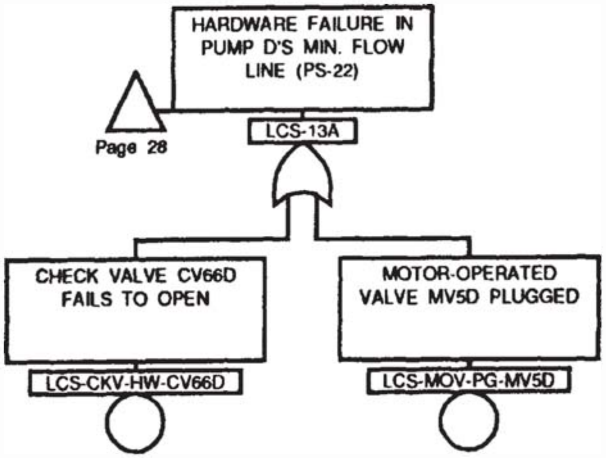

HARDWARE FAILURE IN PUMP D'S MIN. FLOW LINE (PS-22)
Page 28
LCS-13A
CHECK VALVE CV66D FAILS TO OPEN
LCS-CKV-HW-CV66D
MOTOR-OPERATED VALVE MV5D PLUGGED
LCS-MOV-PG-MV5D

Figure 5.5-3. LPCS Fault Tree (Page 13 of 35)

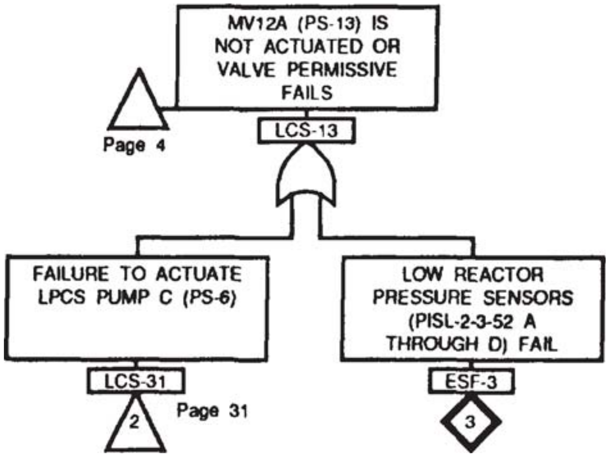

MV12A (PS-13) IS NOT ACTUATED OR VALVE PERMISSIVE FAILS
Page 4
LCS-13
FAILURE TO ACTUATE LPCS PUMP C (PS-6)
LOW REACTOR PRESSURE SENSORS (PISL-2-3-52 A THROUGH D) FAIL
LCS-31
ESF-3
2
Page 31
3

Figure 5.5-3. LPCS Fault Tree (Page 14 of 35)

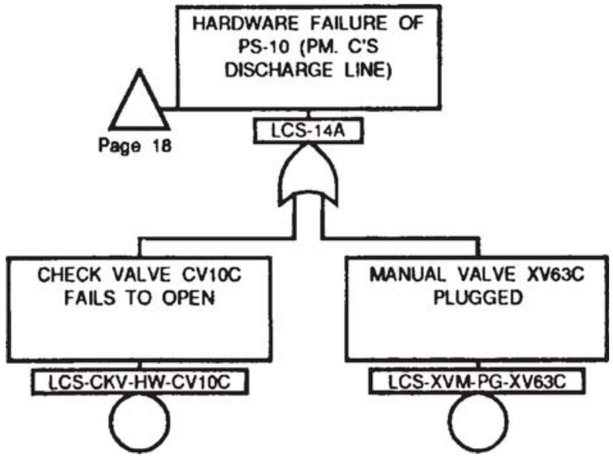

HARDWARE FAILURE OF PS-10 (PM. C'S DISCHARGE LINE)
Page 18
LCS-14A
CHECK VALVE CV10C FAILS TO OPEN
LCS-CKV-HW-CV10C
MANUAL VALVE XV63C PLUGGED
LCS-XVM-PG-XV63C

Figure 5.5-3. LPCS Fault Tree (Page 15 of 35)

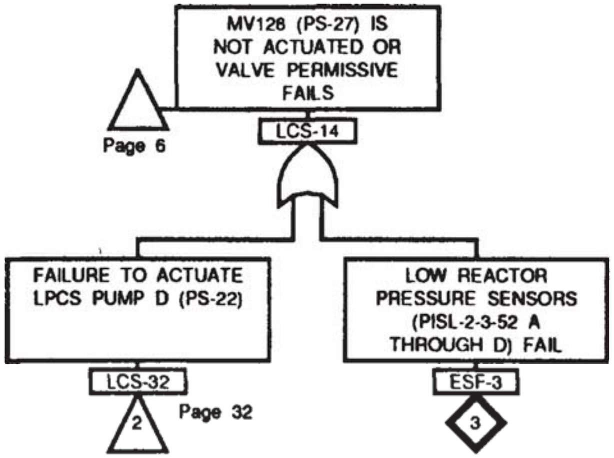

MV128 (PS-27) IS NOT ACTUATED OR VALVE PERMISSIVE FAILS
LCS-14
Page 6
FAILURE TO ACTUATE LPCS PUMP D (PS-22)
LCS-32
2
Page 32
LOW REACTOR PRESSURE SENSORS (PISL-2-3-52 A THROUGH D) FAIL
ESF-3
3

Figure 5.5-3. LPCS Fault Tree (Page 16 of 35)

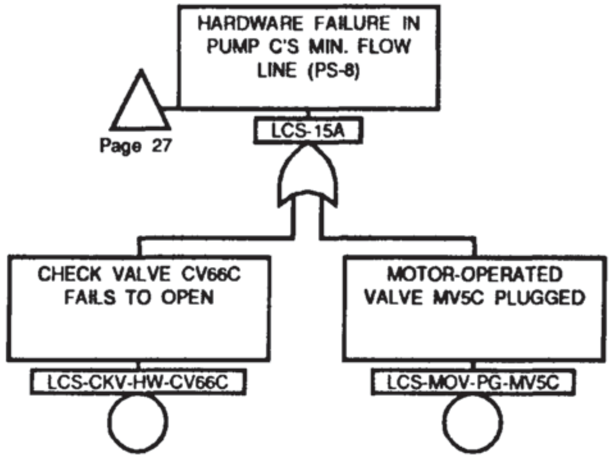

HARDWARE FAILURE IN PUMP C'S MIN. FLOW LINE (PS-8)
LCS-15A
Page 27
CHECK VALVE CV66C FAILS TO OPEN
LCS-CKV-HW-CV66C
MOTOR-OPERATED VALVE MV5C PLUGGED
LCS-MOV-PG-MV5C

Figure 5.5-3. LPCS Fault Tree (Page 17 of 35)

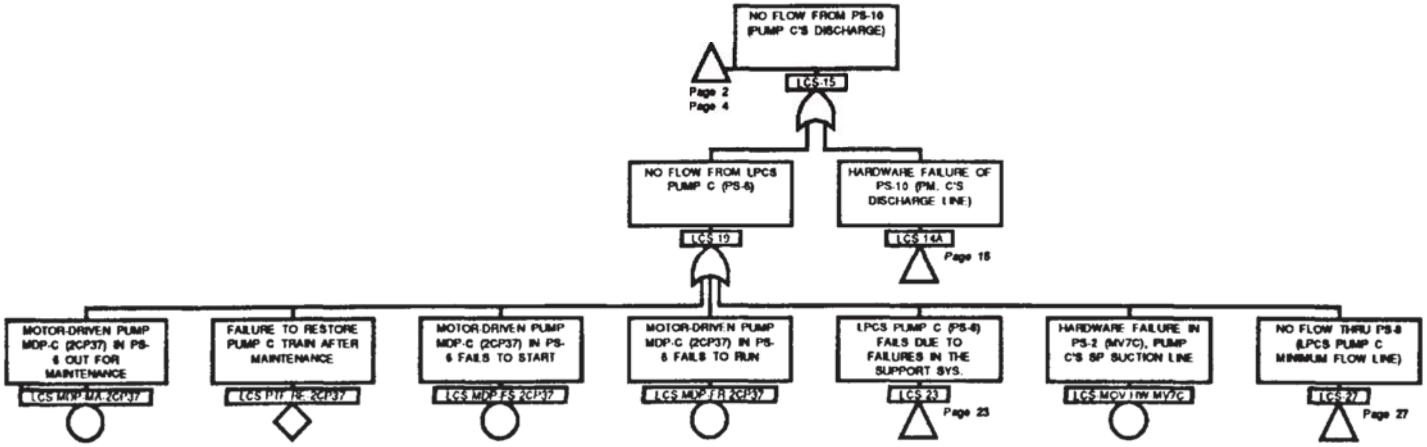

NO FLOW FROM PS-10 (PUMP C'S DISCHARGE)
Page 2
Page 4
LCS-15
NO FLOW FROM LPCS PUMP C (PS-6)
LCS 19
HARDWARE FAILURE OF PS-10 (PM. C'S DISCHARGE LINE)
LCS 14A
Page 16
MOTOR-DRIVEN PUMP MDP-C (2CP37) IN PS-6 OUT FOR MAINTENANCE
LCS MDP-MA-2CP37
FAILURE TO RESTORE PUMP C TRAIN AFTER MAINTENANCE
LCS PTF-RE-2CP37
MOTOR-DRIVEN PUMP MDP-C (2CP37) IN PS-6 FAILS TO START
LCS MDP-FS-2CP37
MOTOR-DRIVEN PUMP MDP-C (2CP37) IN PS-6 FAILS TO RUN
LCS MDP-FR-2CP37
LPCS PUMP C (PS-6) FAILS DUE TO FAILURES IN THE SUPPORT SYS.
LCS 23
Page 23
HARDWARE FAILURE IN PS-2 (MV7C), PUMP C'S SP SUCTION LINE
LCS-MOV-HW-MV7C
NO FLOW THRU PS-8 (LPCS PUMP C MINIMUM FLOW LINE)
LCS-27
Page 27

Figure 5.5-3. LPCS Fault Tree (Page 18 of 35)

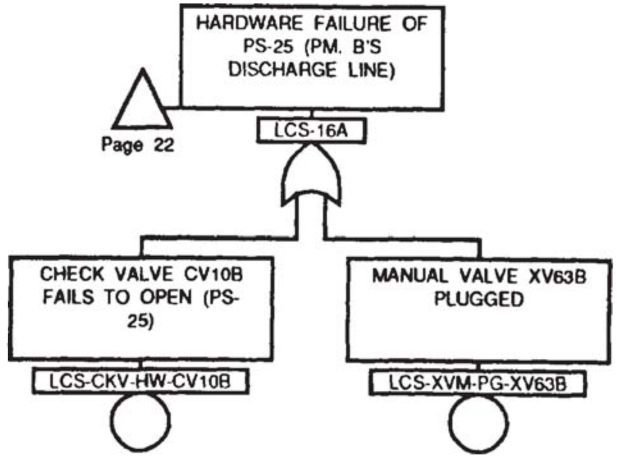

HARDWARE FAILURE OF PS-25 (PM. B'S DISCHARGE LINE)
Page 22
LCS-16A
CHECK VALVE CV10B FAILS TO OPEN (PS-25)
MANUAL VALVE XV63B PLUGGED
LCS-CKV-HW-CV10B
LCS-XVM-PG-XV63B

Figure 5.5-3. LPCS Fault Tree (Page 19 of 35)

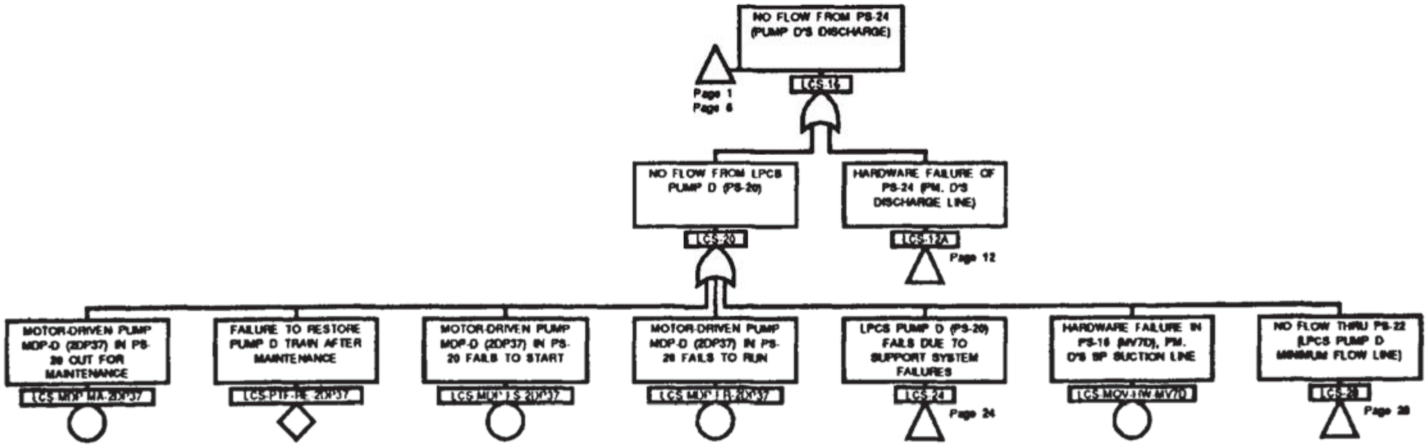

NO FLOW FROM PS-24 (PUMP D'S DISCHARGE)
Page 1
Page 6
LCS-16
NO FLOW FROM LPCS PUMP D (PS-20)
LCS-20
HARDWARE FAILURE OF PS-24 (PM. D'S DISCHARGE LINE)
LCS-12A
Page 12
MOTOR-DRIVEN PUMP MDP-D (2DP37) IN PS-20 OUT FOR MAINTENANCE
LCS-MDP-MA-2DP37
FAILURE TO RESTORE PUMP D TRAIN AFTER MAINTENANCE
LCS-PTF-RE-2DP37
MOTOR-DRIVEN PUMP MDP-D (2DP37) IN PS-20 FAILS TO START
LCS-MDP-FS-2DP37
MOTOR-DRIVEN PUMP MDP-D (2DP37) IN PS-20 FAILS TO RUN
LCS-MDP-FR-2DP37
LPCS PUMP D (PS-20) FAILS DUE TO SUPPORT SYSTEM FAILURES
LCS-24
Page 24
HARDWARE FAILURE IN PS-16 (MV7D), PM. D'S SP SUCTION LINE
LCS-MOV-HW-MV7D
NO FLOW THRU PS-22 (LPCS PUMP D MINIMUM FLOW LINE)
LCS-28
Page 28

Figure 5.5-3. LPCS Fault Tree (Page 20 of 35)

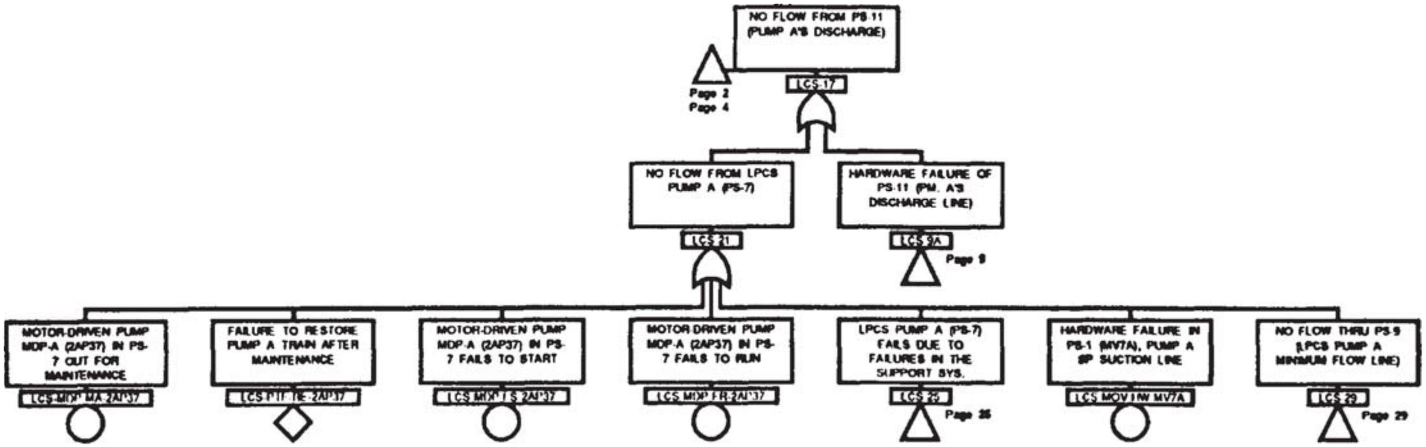

NO FLOW FROM PS-11 (PUMP A'S DISCHARGE)
Page 2
Page 4
LCS-17
NO FLOW FROM LPCS PUMP A (PS-7)
LCS-21
HARDWARE FAILURE OF PS-11 (PM. A'S DISCHARGE LINE)
LCS-9A
Page 9
MOTOR-DRIVEN PUMP MDP-A (2AP37) IN PS-7 OUT FOR MAINTENANCE
LCS-MDP-MA-2AP37
FAILURE TO RESTORE PUMP A TRAIN AFTER MAINTENANCE
LCS-PTF-TE-2AP37
MOTOR-DRIVEN PUMP MDP-A (2AP37) IN PS-7 FAILS TO START
LCS-MDP-TS-2AP37
MOTOR-DRIVEN PUMP MDP-A (2AP37) IN PS-7 FAILS TO RUN
LCS-MDP-FR-2AP37
LPCS PUMP A (PS-7) FAILS DUE TO FAILURES IN THE SUPPORT SYS.
LCS-25
Page 25
HARDWARE FAILURE IN PS-1 (MV7A), PUMP A SP SUCTION LINE
LCS-MOV-NW-MV7A
NO FLOW THRU PS-9 (LPCS PUMP A MINIMUM FLOW LINE)
LCS-29
Page 29

Figure 5.5-3. LPCS Fault Tree (Page 21 of 35)

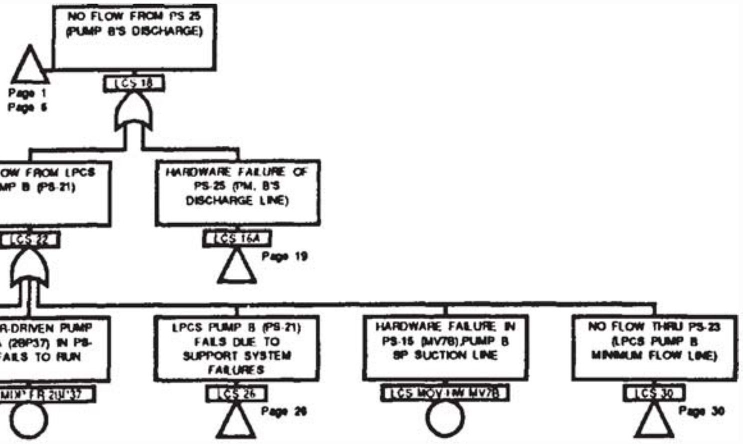

NO FLOW FROM PS 25 (PUMP B'S DISCHARGE)
Page 1
Page 6
LCS 18
NO FLOW FROM LPCS PUMP B (PS-21)
LCS 22
HARDWARE FAILURE OF PS-25 (PM. B'S DISCHARGE LINE)
LCS 16A
Page 19
MOTOR-DRIVEN PUMP MDP-B (2BP37) IN PS-21 OUT FOR MAINTENANCE
LCS MDP MA 2BP37
FAILURE TO RESTORE PUMP B TRAIN AFTER MAINTENANCE
LCS PTT NE 2BP37
MOTOR-DRIVEN PUMP MDP-B (2BP37) IN PS-21 FAILS TO START
LCS MDP FS 2BP37
MOTOR-DRIVEN PUMP MDP-A (2BP37) IN PS-21 FAILS TO RUN
LCS MDP FR 2BP37
LPCS PUMP B (PS-21) FAILS DUE TO SUPPORT SYSTEM FAILURES
LCS 26
Page 26
HARDWARE FAILURE IN PS-15 (MV7B),PUMP B SP SUCTION LINE
LCS MOV HW MV7B
NO FLOW THRU PS-23 (LPCS PUMP B MINIMUM FLOW LINE)
LCS 30
Page 30

Figure 5.5-3. LPCS Fault Tree (Page 22 of 35)

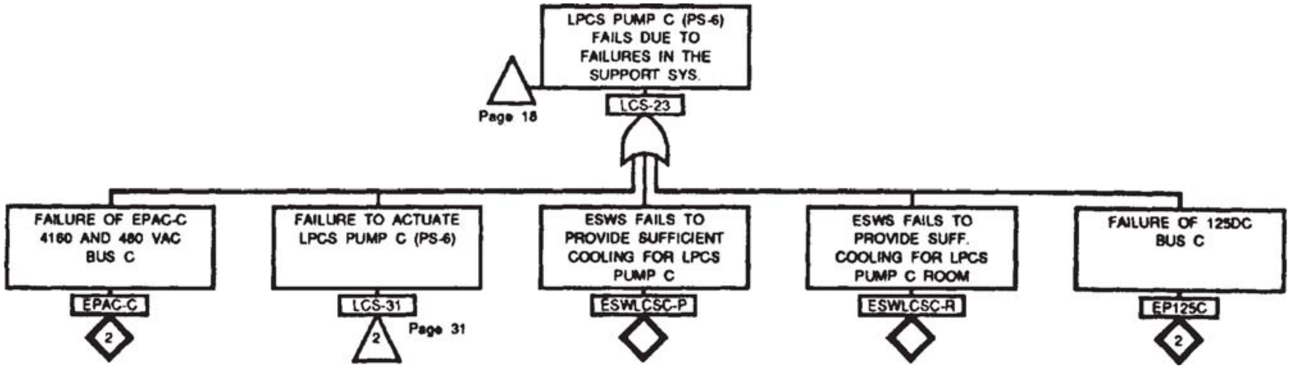

LPCS PUMP C (PS-6) FAILS DUE TO FAILURES IN THE SUPPORT SYS.
Page 18
LCS-23
FAILURE OF EPAC-C 4160 AND 480 VAC BUS C
EPAC-C
2
FAILURE TO ACTUATE LPCS PUMP C (PS-6)
LCS-31
2
Page 31
ESWS FAILS TO PROVIDE SUFFICIENT COOLING FOR LPCS PUMP C
ESWLCSC-P
ESWS FAILS TO PROVIDE SUFF. COOLING FOR LPCS PUMP C ROOM
ESWLCSC-R
FAILURE OF 125DC BUS C
EP125C
2

Figure 5.5-3. LPCS Fault Tree (Page 23 of 35)

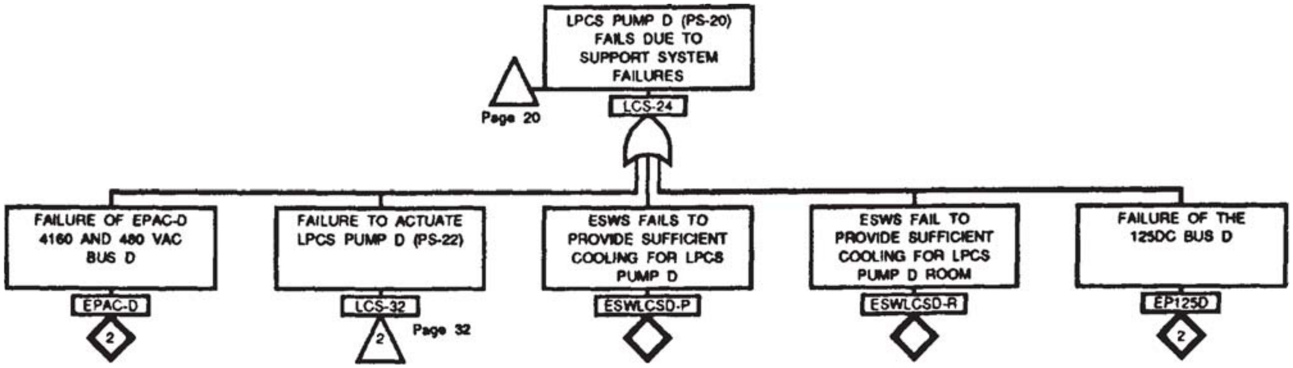

LPCS PUMP D (PS-20) FAILS DUE TO SUPPORT SYSTEM FAILURES
LCS-24
Page 20
FAILURE OF EPAC-D 4160 AND 480 VAC BUS D
EPAC-D
2
FAILURE TO ACTUATE LPCS PUMP D (PS-22)
LCS-32
2
Page 32
ESWS FAILS TO PROVIDE SUFFICIENT COOLING FOR LPCS PUMP D
ESWLCSD-P
ESWS FAIL TO PROVIDE SUFFICIENT COOLING FOR LPCS PUMP D ROOM
ESWLCSD-R
FAILURE OF THE 125DC BUS D
EP125D
2

Figure 5.5-3. LPCS Fault Tree (Page 24 of 35)

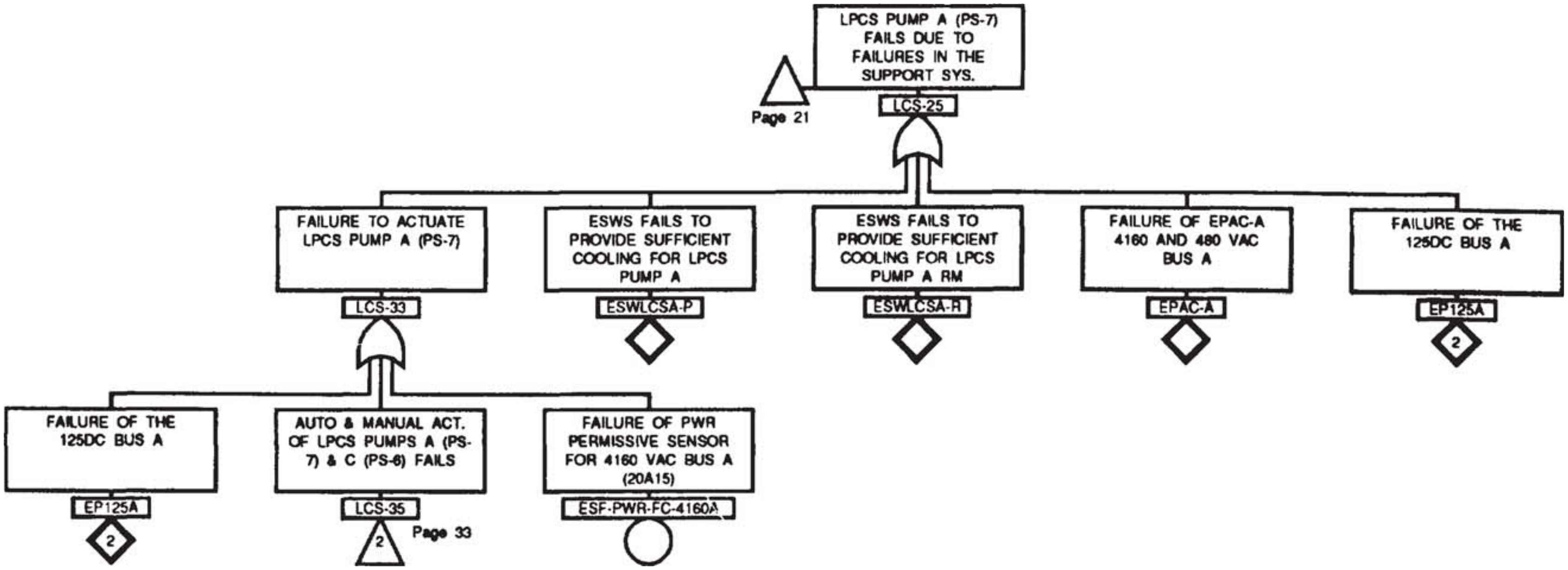

LPCS PUMP A (PS-7) FAILS DUE TO FAILURES IN THE SUPPORT SYS.
LCS-25
Page 21
FAILURE TO ACTUATE LPCS PUMP A (PS-7)
LCS-33
ESWS FAILS TO PROVIDE SUFFICIENT COOLING FOR LPCS PUMP A
ESWLCSA-P
ESWS FAILS TO PROVIDE SUFFICIENT COOLING FOR LPCS PUMP A RM
ESWLCSA-R
FAILURE OF EPAC-A 4160 AND 480 VAC BUS A
EPAC-A
FAILURE OF THE 125DC BUS A
EP125A
2
FAILURE OF THE 125DC BUS A
EP125A
2
AUTO & MANUAL ACT. OF LPCS PUMPS A (PS-7) & C (PS-6) FAILS
LCS-35
2
Page 33
FAILURE OF PWR PERMISSIVE SENSOR FOR 4160 VAC BUS A (20A15)
ESF-PWR-FC-4160A

Figure 5.5-3. LPCS Fault Tree (Page 25 of 35)

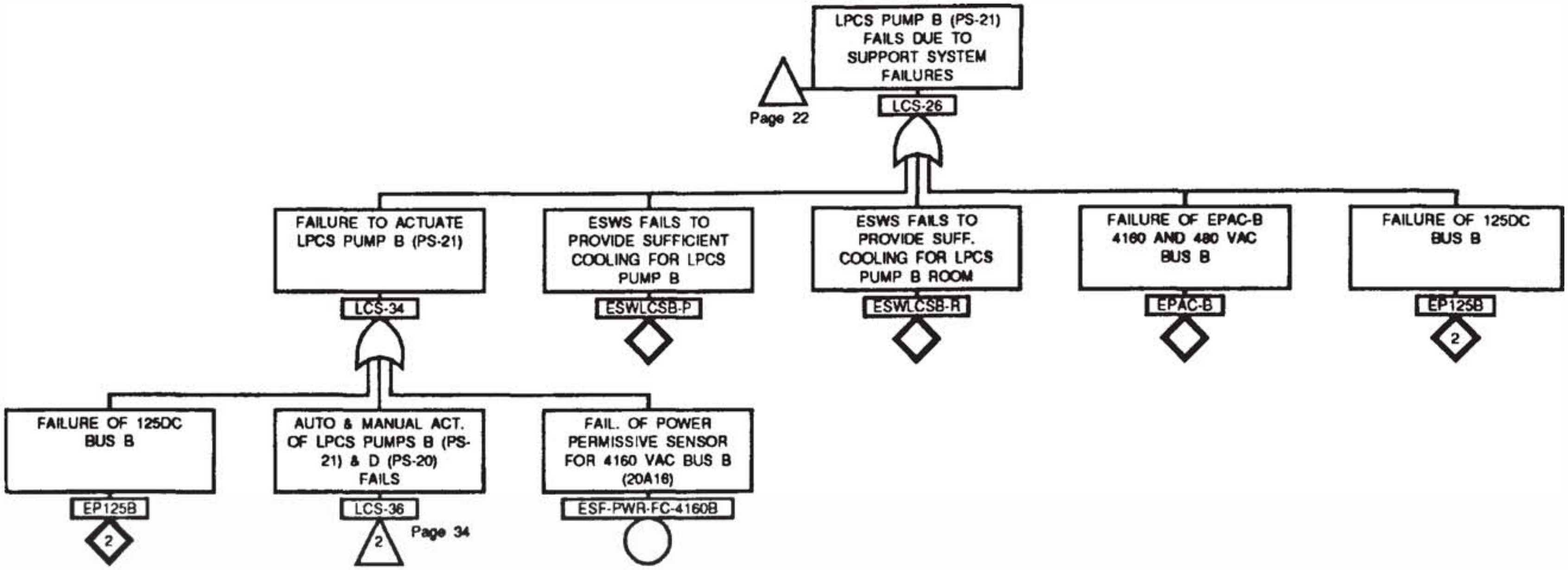

LPCS PUMP B (PS-21) FAILS DUE TO SUPPORT SYSTEM FAILURES
LCS-26
Page 22
FAILURE TO ACTUATE LPCS PUMP B (PS-21)
LCS-34
ESWS FAILS TO PROVIDE SUFFICIENT COOLING FOR LPCS PUMP B
ESWLCSB-P
ESWS FAILS TO PROVIDE SUFF. COOLING FOR LPCS PUMP B ROOM
ESWLCSB-R
FAILURE OF EPAC-B 4160 AND 480 VAC BUS B
EPAC-B
FAILURE OF 125DC BUS B
EP125B
2
FAILURE OF 125DC BUS B
EP125B
2
AUTO & MANUAL ACT. OF LPCS PUMPS B (PS-21) & D (PS-20) FAILS
LCS-36
2
Page 34
FAIL. OF POWER PERMISSIVE SENSOR FOR 4160 VAC BUS B (20A16)
ESF-PWR-FC-4160B

Figure 5.5-3. LPCS Fault Tree (Page 26 of 35)

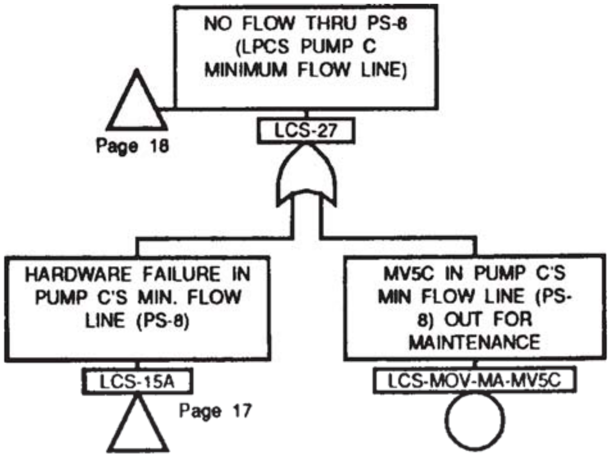

NO FLOW THRU PS-8 (LPCS PUMP C MINIMUM FLOW LINE)
LCS-27
Page 18
HARDWARE FAILURE IN PUMP C'S MIN. FLOW LINE (PS-8)
LCS-15A
Page 17
MV5C IN PUMP C'S MIN FLOW LINE (PS-8) OUT FOR MAINTENANCE
LCS-MOV-MA-MV5C

Figure 5.5-3. LPCS Fault Tree (Page 27 of 35)

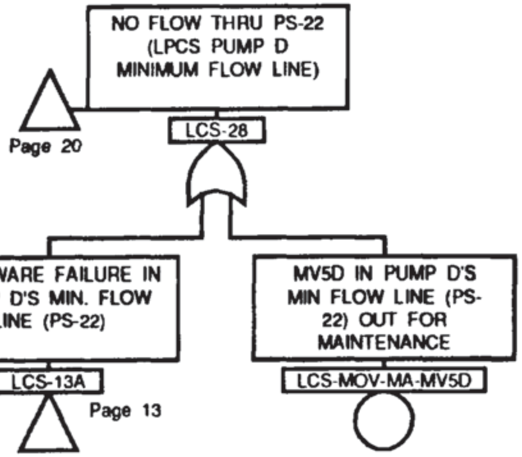

NO FLOW THRU PS-22 (LPCS PUMP D MINIMUM FLOW LINE)
Page 20
LCS-28
HARDWARE FAILURE IN PUMP D'S MIN. FLOW LINE (PS-22)
MV5D IN PUMP D'S MIN FLOW LINE (PS-22) OUT FOR MAINTENANCE
LCS-13A
Page 13
LCS-MOV-MA-MV5D

Figure 5.5-3. LPCS Fault Tree (Page 28 of 35)

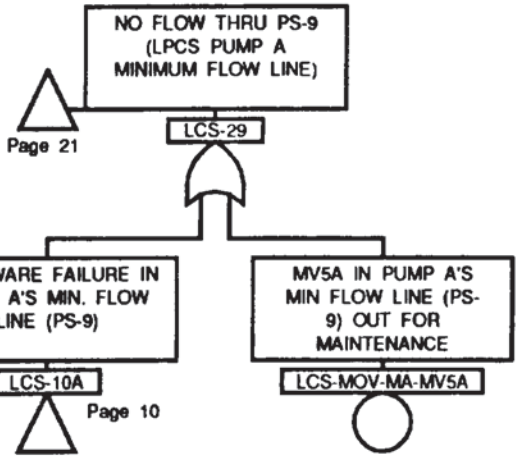

NO FLOW THRU PS-9 (LPCS PUMP A MINIMUM FLOW LINE)
Page 21
LCS-29
HARDWARE FAILURE IN PUMP A'S MIN. FLOW LINE (PS-9)
LCS-10A
Page 10
MV5A IN PUMP A'S MIN FLOW LINE (PS-9) OUT FOR MAINTENANCE
LCS-MOV-MA-MV5A

Figure 5.5-3. LPCS Fault Tree (Page 29 of 35)

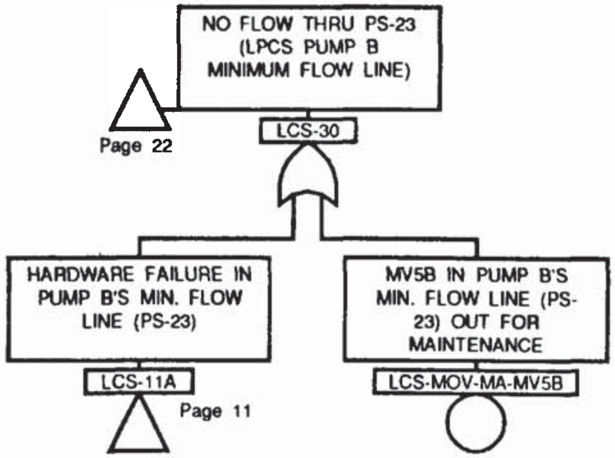

NO FLOW THRU PS-23 (LPCS PUMP B MINIMUM FLOW LINE)
LCS-30
Page 22
HARDWARE FAILURE IN PUMP B'S MIN. FLOW LINE (PS-23)
LCS-11A
Page 11
MV5B IN PUMP B'S MIN. FLOW LINE (PS-23) OUT FOR MAINTENANCE
LCS-MOV-MA-MV5B

Figure 5.5-3. LPCS Fault Tree (Page 30 of 35)

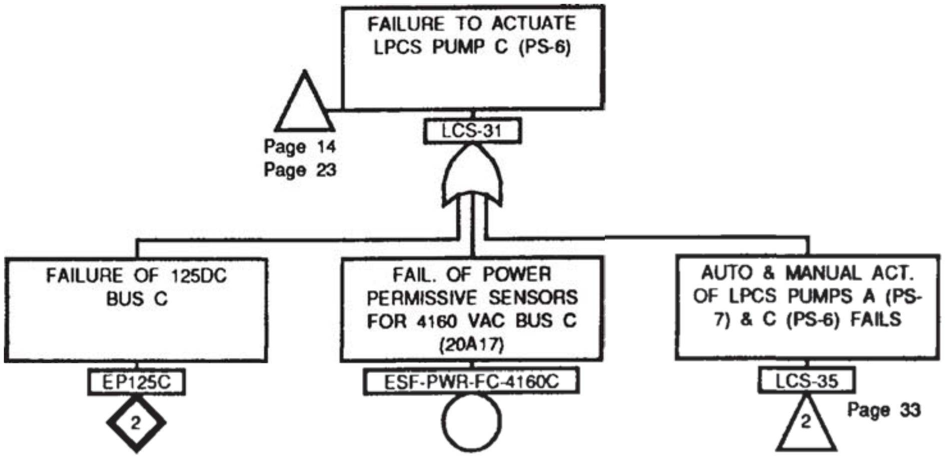

FAILURE TO ACTUATE LPCS PUMP C (PS-6)
LCS-31
Page 14
Page 23
FAILURE OF 125DC BUS C
EP125C
2
FAIL. OF POWER PERMISSIVE SENSORS FOR 4160 VAC BUS C (20A17)
ESF-PWR-FC-4160C
AUTO & MANUAL ACT. OF LPCS PUMPS A (PS-7) & C (PS-6) FAILS
LCS-35
2
Page 33

Figure 5.5-3. LPCS Fault Tree (Page 31 of 35)

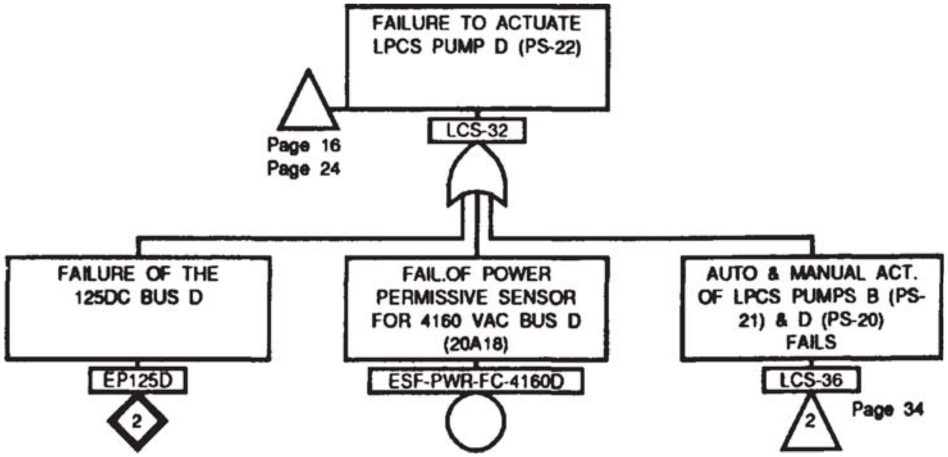

FAILURE TO ACTUATE LPCS PUMP D (PS-22)
Page 16
Page 24
LCS-32
FAILURE OF THE 125DC BUS D
EP125D
2
FAIL.OF POWER PERMISSIVE SENSOR FOR 4160 VAC BUS D (20A18)
ESF-PWR-FC-4160D
AUTO & MANUAL ACT. OF LPCS PUMPS B (PS-21) & D (PS-20) FAILS
LCS-36
2
Page 34

Figure 5.5-3. LPCS Fault Tree (Page 32 of 35)

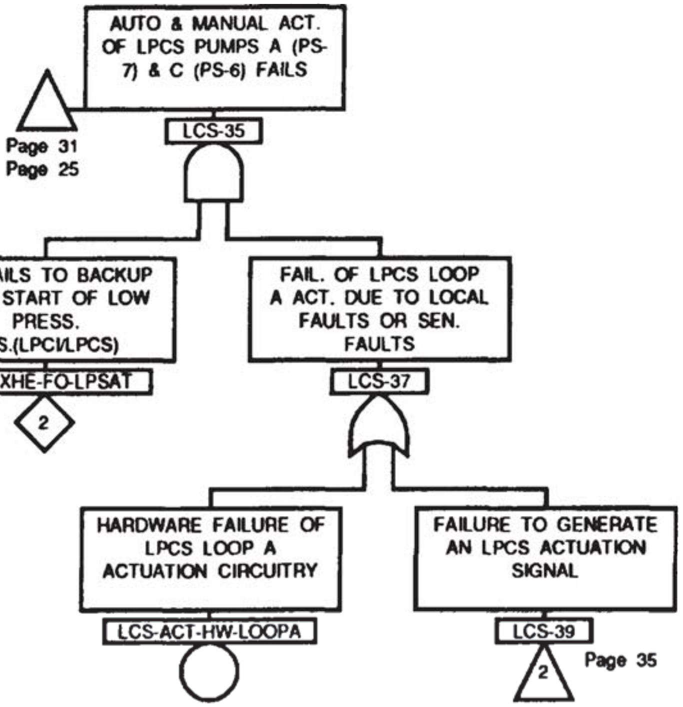

AUTO & MANUAL ACT. OF LPCS PUMPS A (PS-7) & C (PS-6) FAILS
LCS-35
Page 31
Page 25
OP. FAILS TO BACKUP AUTO START OF LOW PRESS. SYS.(LPCI/LPCS)
ESF-XHE-FO-LPSAT
2
FAIL. OF LPCS LOOP A ACT. DUE TO LOCAL FAULTS OR SEN. FAULTS
LCS-37
HARDWARE FAILURE OF LPCS LOOP A ACTUATION CIRCUITRY
LCS-ACT-HW-LOOPA
FAILURE TO GENERATE AN LPCS ACTUATION SIGNAL
LCS-39
2
Page 35

Figure 5.5-3. LPCS Fault Tree (Page 33 of 35)

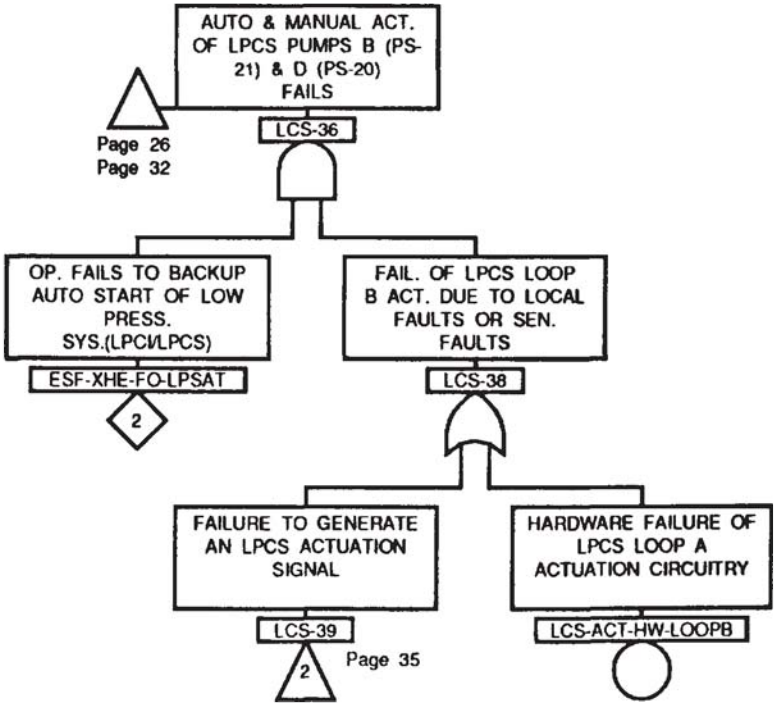

AUTO & MANUAL ACT. OF LPCS PUMPS B (PS-21) & D (PS-20) FAILS
LCS-36
Page 26
Page 32
OP. FAILS TO BACKUP AUTO START OF LOW PRESS. SYS.(LPCI/LPCS)
ESF-XHE-FO-LPSAT
2
FAIL. OF LPCS LOOP B ACT. DUE TO LOCAL FAULTS OR SEN. FAULTS
LCS-38
FAILURE TO GENERATE AN LPCS ACTUATION SIGNAL
LCS-39
2
Page 35
HARDWARE FAILURE OF LPCS LOOP A ACTUATION CIRCUITRY
LCS-ACT-HW-LOOPB

Figure 5.5-3. LPCS Fault Tree (Page 34 of 35)

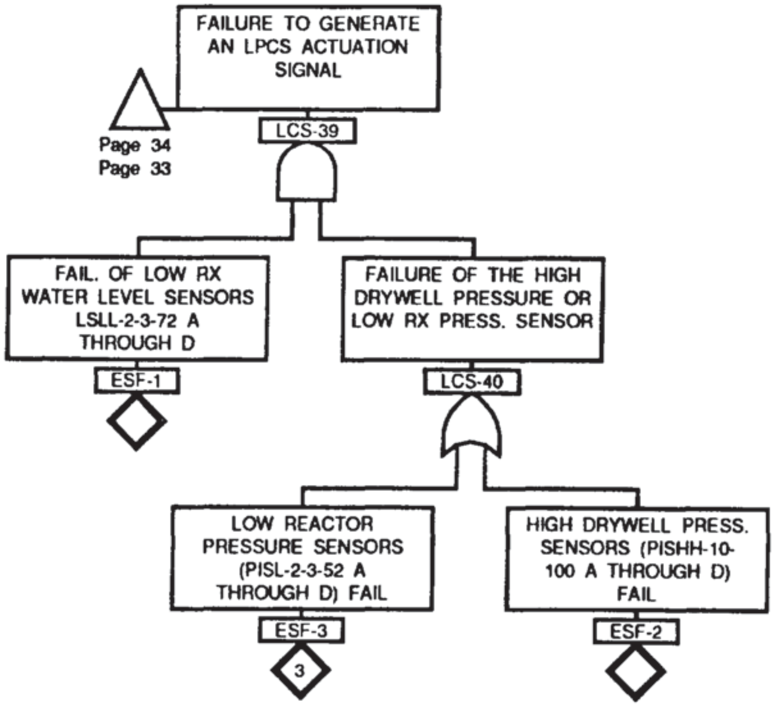

FAILURE TO GENERATE AN LPCS ACTUATION SIGNAL
Page 34
Page 33
LCS-39
FAIL. OF LOW RX WATER LEVEL SENSORS LSLL-2-3-72 A THROUGH D
ESF-1
FAILURE OF THE HIGH DRYWELL PRESSURE OR LOW RX PRESS. SENSOR
LCS-40
LOW REACTOR PRESSURE SENSORS (PISL-2-3-52 A THROUGH D) FAIL
ESF-3
3
HIGH DRYWELL PRESS. SENSORS (PISHH-10-100 A THROUGH D) FAIL
ESF-2

Figure 5.5-3. LPCS Fault Tree (Page 35 of 35)

6. DEPENDENT AND SUBTLE FAILURE ANALYSIS

Dependent failures are those failures that defeat the redundancy or diversity that is employed to improve the availability of some plant function such as coolant injection. Subtle failures are design related failures which are not readily identified in the modeling process. Several such failures have been observed in operating experience or have been identified from the insights of other studies. Therefore, subtle failure analysis has been incorporated in the NUREG/CR-4550 methodology.

Dependent failures involve two types of relationships between components; explicit dependencies between components, and failure mechanisms which effect more than one component but which are not explicitly identified in the systems analysis. The explicit dependencies are included in the logic models of the systems as individual basic events. For example, functional dependencies between front line systems and support systems, such as power and cooling, are included in the system fault trees. Cascading or propagating failures are also modeled explicitly in the fault trees. An example of such an event is failure of a pump to start due to the malfunction of a circuit breaker in the pump control circuit.

The dependencies among components which are not explicitly identified in the systems analysis are accounted for by introducing the concept of common cause failures. These are modeled by common cause basic events applied to the fault trees. A common cause event is defined as the simultaneous failure or unavailability of more than one component due to some shared cause. The methodology for common cause failure analysis presented below evolved from insights from past PRA studies, operating experience, and from efforts within the risk assessment community to model common cause failures. Specifically, EPRI NP-3967[21] was used as both a data source and a methods guide for quantifying common cause failures. The methods presented here are simplified compared to those presented in a more recent report, NUREG/CR-4780,[75] which became available too late for incorporation into the NUREG-1150 studies. However, the simplified methods presented herein are felt to be adequate for most PRAs.

Subtle failures occur as a result of design related inadequacies. That is, under abnormal conditions a system or component does not, in fact, respond in accordance with nominal design specifications. These subtle failures are generally specific to a particular design or installation and are not identified without a detailed analysis. For example, observed subtle failures have involved logic circuits, gas or vapor binding of pumps, check valve performance, and other similar phenomena. The NUREG/CR-4550 methodology draws extensively from the experience of prior studies to define a set of generic subtle failure possibilities which should be considered in any plant study.

6.1 Dependent and Subtle Failure Analysis Assumptions and Limitations

Plant specific data on multiple failures are rare, so data collection and analysis for common cause analysis must be done on an industry wide basis. However, data from other plants must be screened for applicability in a particular analysis due to design, operational, and manufacturing differences between components at different plants. Data collection is further complicated by the fact that the descriptions of events in the data base are often inadequate for proper classification into independent or common cause categories. Therefore, the uncertainty incorporated into the parameter estimation for common cause models must account for the potential misclassification of data.

Common cause failures across system boundaries were not modeled. The detection and prevention of failure mechanisms which can lead to common cause failures are strongly influenced by maintenance practices. Because maintenance and testing of different systems are done separately for each system, and because there are no procedures requiring actions between systems that would lead to common cause failures, common cause failures between systems are not modeled in the ASEP methodology.

In most cases the NUREG/CR-4550 common cause analysis was limited to those failures which defeat the complete redundancy or diversity of a system design. Partial common cause failures were not modeled for most systems. For example, if a system has three similar trains with a success criterion of one out of three trains, only a common cause failure of all three trains would be modeled. Common cause failure of two trains combined with the independent failure of the third train was not generally considered. However, in cases where such failure combinations are probabilistically significant, they were included in the common cause model (see the discussion on page 6-10 for BWR Safety Relief Valves).

6.2 Dependent and Subtle Failure Development

Dependent failures and subtle failures represent two different types of events, therefore they are discussed separately.

6.2.1 Dependent Failure Development

Dependent failure analysis is divided into two categories consistent with the major types of dependent failure events; functional dependencies and propagating failures which are explicitly identified in the systems analysis, and those dependencies which cannot be readily identified and are accounted for by common cause basic events. The two types of failures are analyzed differently as illustrated in Figure 6.2.1, but both procedures start with the gathering of information.

Step 6.1. Obtain Information for Dependent Failures

The information required to identify functional dependencies and components susceptible to common cause events, and to analyze data for common cause failure quantification is gathered as part of plant familiarization (see Section 2). The general information sources are:

- System descriptions,
- Piping and Instrumentation Diagrams,

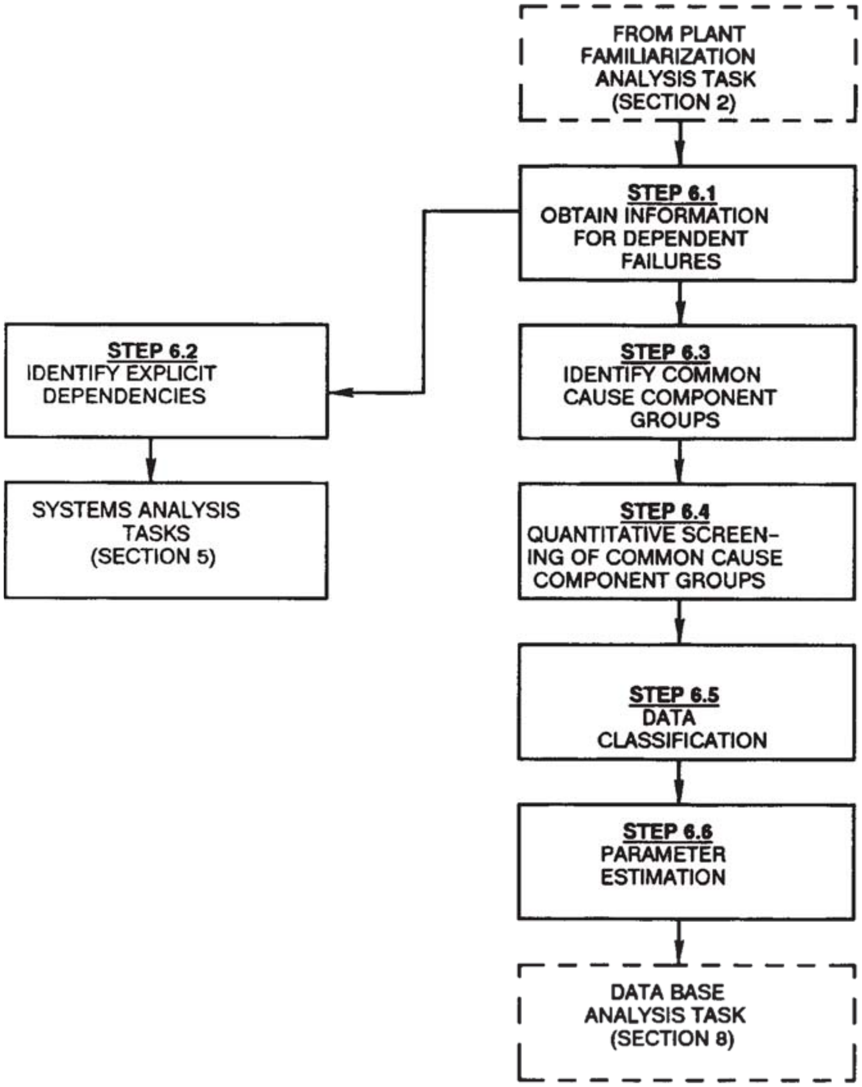

FROM PLANT FAMILIARIZATION ANALYSIS TASK (SECTION 2)
STEP 6.1 OBTAIN INFORMATION FOR DEPENDENT FAILURES
STEP 6.2 IDENTIFY EXPLICIT DEPENDENCIES
SYSTEMS ANALYSIS TASKS (SECTION 5)
STEP 6.3 IDENTIFY COMMON CAUSE COMPONENT GROUPS
STEP 6.4 QUANTITATIVE SCREENING OF COMMON CAUSE COMPONENT GROUPS
STEP 6.5 DATA CLASSIFICATION
STEP 6.6 PARAMETER ESTIMATION
DATA BASE ANALYSIS TASK (SECTION 8)

Figure 6.2-1. Step Relationship for Dependent Failure Analysis

- Instrumentation and control drawings,
- Licensee Event Reports,
- Maintenance request records,and
- Operator log books.

Step 6.2. Identify Explicit Dependencies

The dependencies which can be explicitly modeled are identified in the various tasks relevant to the type of events for each dependency. Explicit dependencies are:

- Initiating events - Accident initiators can affect the unavailability of more than one system. These types of dependencies are identified as part of the Accident Sequence Initiating Event Analysis task (Section 3).

- Support system dependencies - Operation of front-line reactor core and containment safety systems can be directly or indirectly dependent on certain support systems. The functional relationships between support and front line systems include:

    - Electrical power,
    - Heating, ventilation, and cooling
    - Actuation, and
    - Isolation.

  These types of dependencies are identified and explicitly modeled in the systems analysis task (Section 5).

- Shared equipment dependencies - Individual components which are shared by more than one system are identified and explicitly modeled in the systems analysis (Section 5).

- Human errors - Operator failure to respond according to procedures can result in the failure or unavailability of more than one component or system. These types of dependencies are identified in the human reliability analysis (Section 7) and modeled explicitly in the systems analysis.

- Propagating failures - Failure of one component due to the failure of another component directly linked to it is identified and modeled in the systems analysis.

Step 6.3. Identify Common Cause Component Groups

A search is made for common attributes of similar components and for failure mechanisms which can lead to common cause failures. Analysts have traditionally relied on common sense, engineering insights, and obvious signs of dependence to identify component groups for common cause analysis. These analysis techniques can be enhanced by directing the identification of potential common cause component groups and events within the context of the following guidelines (Reference 75):

- Identical nondiverse components which are used to provide redundancy should always be put into a common cause group. The components placed into a group can belong to different systems, but any common cause event relevant to the group will model only a common cause failure of components within a particular system. For example, MOVs used in the discharge lines of redundant trains in the SWS and the CCWS may be identified as identical components, and thus placed in a the same common cause component group, but separate common cause events will be developed for the valve combinations in each system.

- Diverse redundant components generally are assumed to be independent, and this assumption is supported by data. However, if the diverse components have subcomponents which are identical and redundant, the subcomponents should be identified as potential common cause failures. For example, a system may have two pumps in parallel but with different displacement mechanisms (e.g., a centrifugal pump and a positive displacement pump). However, the pumps may have common devices for starting (e.g., electrical circuit breakers). Such common devices should be analyzed for potential common cause failure mechanisms. One method for identifying common subcomponents is to go inside component boundaries.

- Certain passive components are usually omitted from systems analysis. However, care must be exercised not to overlook potential common cause failures, e.g., debris in components such as redundant strainers.

These guidelines can be used to focus attention on important attributes which may lead to common cause failures. A generic list of such attributes is provided below. This list should not be considered to be an exhaustive compilation of all potential common cause indicators, but only a guide. Analysts should identify any reasonable attribute based on experience and judgment. Some of the well recognized common attributes to be looked for when identifying common cause component groups are:

- Component type (e.g., MOV, MDP, AOV),

- Component use (e.g., system isolation, parameter sensing),

- Manufacturer of component,

- Internal environment of component (e.g., temperature, pressure, flow rate), (a low-pressure cool water system pump may not have a common cause linkage with a high-pressure hot water system pump),

- External environment of component (e.g., temperature, humidity, dust),

- Operating mode of component (e.g., normally closed or open, normally running or standby),

- Testing and maintenance procedures and characteristics which may introduce common cause failure mechanisms.

An important type of common cause failure mechanism which must be addressed is human error in maintenance and testing. Common cause errors such as miscalibration of parameter sensing devices or improper maintenance of redundant components are potentially significant contributors to risk. Human induced common cause mechanisms are analyzed in the human reliability analysis (Section 7).

The following is a list of component groups which were identified for the NUREG/CR-4550 analyses:

- MOVs,
- MDPs,
- SRVs,
- AOVs,
- DGs,
- Batteries.

This list is indicative of those component groups which were identified in all of the NUREG/CR-4550 plant analyses. Other component groups may be identified in a particular plant analysis depending on the level of detail and design of plant systems.

Step 6.4 Quantitative Screening of Common Cause Component Events

Step 6.3 produces various groups of components potentially susceptible to common cause failures. From these groups, common cause events for components of the same common cause group and within the same system must be developed and included explicitly in the system fault trees as part of the systems analysis task (Section 5). The number of possible common cause basic events can be quite large and require a significant amount of data analysis and basic event quantification. However, by quantifying the common cause basic events with a simplistic and conservative model, and including them in the preliminary quantification of the fault trees and accident sequence equations (Section 10, steps 10.3 and 10.4), many common cause events can be screened out of the analysis when the system and accident sequence equations are truncated based on the probability of the cut sets.

For screening purposes, common cause events can be quantified using the independent failure probability of the component in question and a conservative beta factor of 0.1. The beta factor model is one of several common cause models, and is the most frequently used model in the NUREG/CR-4550 analyses. It is explained in more detail in Step 6.6. For example, suppose three normally closed MOVs (designated as valves A,B,C) have been placed in a redundant configuration within a system. A common cause event where all three MOVs fail to transfer to open upon system actuation has been identified by the analyst. This event, Pc(ABC), can be conservatively quantified by:

$$Pc(ABC) = \beta * P_T(A), \qquad (6.1)$$

where $P_T(A)$ is the total failure probability of MOV A,

$P_T(A) = P_T(B) = P_T(C)$, and $\beta = 0.1$

The total failure probability, $P_T(A)$, can be calculated using the estimates for the β factor and the independent failure probability, $P_I(A)$, as follows:

$$P_T = \frac{P_I}{(1 - \beta)}$$

$P_I(A)$ is either estimated from plant specific data or the generic data base (Section 8.0).

If any well accepted quantification models exist for specific common cause events, these models can be used directly in the preliminary quantification steps of Section 10.

Step 6.5. Data Classification

As noted at in the introduction to this Section, plant specific data for common cause phenomena are scarce. Industry wide data and compilations of generic data must be used to develop common cause model parameters. EPRI NP-3967,[21] and a series of reports from Idaho National Engineering Laboratories (References 22,23,24) contain compilations and classification of common cause events for the purpose of quantifying common cause models presented in those same reports. As noted earlier, it is important to review the data in such studies for plant specific applications. Design and operating differences between plants may eliminate certain generic data for a particular plant situation.

Plant specific data can be obtained by searching sources such as operator log books and maintenance request records. However, the success of plant specific data collection is highly dependent on factors such as the quality of record keeping at the plant and the age of the plant.

Once the generic and plant specific data have been collected, the data must be reviewed and classified to assure that only true common cause events and potential common cause events are used. NUREG/CR-4780[75] and EPRI NP-3967[21] present a data classification system developed by EPRI for common cause analysis. Applying this method to the data collected requires considerable effort, and the method was not directly employed in the NUREG/CR-4550 analyses. However, the data and its classification presented in EPRI NP-3967 were reviewed for applicability to the NUREG/CR-4550 plants. It was determined that the data in that report was applicable and that most of it was correctly classified. Thus, EPRI NP-3967 was the data source used to quantify most of the common cause basic events in this analysis.

Step 6.6. Parameter Estimation

Most common cause basic event models indirectly quantify the estimate of probability. Parameters of the models are estimated from the data reviewed and classified in Step 6.5, and the basic event probabilities are derived from the models. A direct approach, called basic parameter modeling estimates the common cause failure probability directly from the data. However, failure data for common cause events are rarely adequate to derive reliable estimates directly. Therefore, parametric models which link common cause failure rates to the independent or total failure rates of the individual components are used.

NUREG/CR-4780[75] discusses four parametric models:

Beta Factor,
Multiple Greek Letter,
Alpha Factor, and
Binomial Failure Rate.

The beta factor model is also presented in EPRI NP-3967, and the binomial failure rate (BFR) model is presented in the work done by Atwood, et al. (References 22,23,24). The primary model used in the NUREG/CR-4550 analyses was a combination of the beta factor model from EPRI NP-3967 and the BFR model from Atwood's work. The beta factor model was chosen for common cause events involving the loss of two out of two redundant components. However, this model was not extended to higher order common cause events in NP-3967. For higher order common cause events involving k components (e.g., three of three, four of four) the beta factors derived for two out of two events from EPRI NP-3927 were multiplied by the ratio of two common cause parameters from Atwood's BFR analysis. The models are illustrated below.

A beta factor represents that fraction of component faults that could also result in faults for similar components in the same group. It is also the conditional probability of a component failure given that a similar component has failed. Such failures are concurrent, or approximately so, and are not due to any other component fault. Mathematically, the data from EPRI NP-3967 are manipulated to derive beta factors defined by:

$$\beta = A / (A+B), \quad \text{where} \qquad (6.2)$$
$$A = N_{ac} + W_c N_{pc} + 1$$
$$B = N_{ai} + W_i N_{pi} + 1$$

N_{ac} = number of actual component failures due to common cause.
N_{pc} = number of potential component failures due to common cause.
N_{ai} = number of actual independent failures.
N_{pi} = number of potential independent failures.
W_i, W_c = weighting factors for considering potential failures as actual failures

The common cause event probability ,Pc, for two out of two components (A and B) is estimated as follows:

$$Pc(AB) = P(A) * \beta,$$

where P(A) represents the total failure rate of the component.

Multipliers from Atwood's work (References 22,23,24) are used to adjust the beta factors for higher order events. The multiplier for a particular beta factor is the ratio of the two factors:

r_k - the rate at which a specific set of k components becomes inoperable simultaneously due to a common cause, and

r_2 - the same factor for k = 2.

A higher order common cause event probability,P_c, (say for components E, D, and F) is estimated by:

$$P_c(EDF) = P(E) * \beta * r_k/r_2 \qquad (6.3)$$
$$P_c(EDF) = P(E) * \beta_k.$$

The product of the beta factor and the ratio of r_i's is explicitly incorporated into the Boolean expression for the accident sequences as a higher order beta factor.

Not all common cause beta factors used in the present analyses are based on the EPRI report because either a more component-specific analysis existed elsewhere or the EPRI report did not analyze data for certain components. The beta factors not based on EPRI NP-3967 are those for air operated valves and batteries. BWR safety relief valve failure to reclose was also a special case as described below.

AOV failures were not specifically addressed in the various references on common cause failures. The screening value of 0.1 was chosen as a beta factor for two or even more AOVs failing from a common cause. This was the result of an expert judgment elicitation performed among the project staff, and is documented in part 2 of the NUREG/CR-4550 Expert Judgment report.[70]

The DC Power Study, NUREG-0666,[25] was the source for the beta factor for a common cause failure of two redundant batteries. That study suggests a worst case beta factor of 0.4 for a two battery configuration in the minimum standard DC power system reported. This value should be adjusted according to guidelines in the report to account for any plant specific features which may warrant a lower beta factor. Higher order beta factors are calculated with a formula based on the assumption that the conditional probability of the k_{th} (k>2) battery failing, given that (k-1) have failed is the average of 1.0 and the beta for (k-1) of k batteries failing, i.e.,

$$\text{Cond Prob } k_{th} \text{ battery fails} = (1.0 + \beta_{k-1})/2 \qquad (6.4)$$

The beta factor for k batteries failing may then be obtained by iteratively applying this equation. This results in the relation:

$$\beta_k = \prod_{i=2}^{k} \{[2^{i-2} - 1.0 + \beta_2]/(2^{i-2})\} \qquad (6.5)$$

where β_k = beta factor for the failure of k batteries out of k batteries,

β_2 = beta factor for failure of 2 batteries

In the NUREG/CR-4550 analyses, the BWR SRV failure-to-reclose common cause event was modeled with data from EPRI NP-3967 using a nonparametric model instead of the beta factor model. BWRs have from eight to ten SRVs, so it was necessary to model the failure of various combinations of these valves. This is an exception to the assumption that was used for most other components, where the common cause failure of k redundant components was modeled for only one failure combination, all k components. These SRV failures include all multiple SRV failures-to-reclose. So, the probabilities of these outcomes include the contribution of combinations of independent failures as well as common cause failures.

At Grand Gulf and Peach Bottom, the resulting LOCA size is the same, regardless of whether three SRVs fail or more than three fail. Therefore, the SRV fail-to-close events which were modeled are:

- Failure of any two SRVs to reclose, and

- Failure of any three or more SRVs to reclose.

The available data contain only two events which involve the failure of two SRVs to reclose. This is drawn from approximately 300 reactor years of BWR experience. Further, there was an average of five transients that occur per reactor year. This information was used to estimate the probability of exactly two SRVs failing-to-reclose with the following equation:

$$P_{SRV}(X=2) = 2/(300 * 5)$$
$$P_{SRV}(X=2) = 1.3E\text{-}3$$

No event has been observed where three or more SRVs have failed-to-reclose. For cases where no outcomes have been observed, one-third of an outcome is used in the expression for the event probability:[76]

$$P_{SRV}(X>2) = (1/3)(300 * 5)$$
$$P_{SRV}(X>2) = 2.2E\text{-}4$$

The data for the SRV multiple failure analysis is derived from industry experience with Target Rock SRVs. Therefore, for SRV designs which are not similar to the Target Rock valves, the data may not be relevant. For these cases, one must either use a similar approach with relevant data if it is available (e.g., test data or plant specific operational experience), or use some other model suitable for problems involving many potential combinations of component failures such as is the case with the SRVs. The MGL method is discussed in NUREG/CR-4780.[75] Although the parameters of the MGL model can be estimated from data, the model is also usable in cases where no data are available. In the model, the total failure probability for one component, Q_t, is estimated from data, or if no failure events have been observed, from Bayesian methods.[76] The equation for Q_k is:

$$Q_k = \frac{1}{\binom{M-1}{k-1}} \left(\prod_{i=1}^{k} \rho_i \right) \left(1-\rho_{k+1} \right) Q_t \tag{6.6}$$

where $\rho_1 = 1.0$ and $\rho_{M+1} = 0$.

The ρ_is are the conditional probabilities that a common cause failure shared by (i-1) or more components will be shared by i or more components. In lieu of data for these parameters, values for ρ_is, starting with ρ_2, must be estimated using some method, such as the relationship used for higher order beta factors for batteries (Equation 6.4). ρ_2 can be estimated by use of a screening value appropriate for mechanical type common cause failures. Although values of 0.1 or 0.05 are recommended as appropriate, engineering judgment of the susceptibility of the SRVs to common cause failures should be used to select the actual value for ρ_2. Using Equation 6.4 for MGL parameters to estimate the remaining yields:

$$\rho_k = (1.0 + \rho_{k-1})/2 \quad ; \quad k > 2 \tag{6.7}$$

The common cause failure probabilities for k out of M components are then used to calculate the probability for each outcome of interest, e.g., one SRV fails-to-reclose, two SRVs fail-to-reclose. It is important to consider the combinations of independent failures and common cause failures which would result in the outcome of interest. For example, as noted above, the failure-to-reclose of one, two, and three or more SRVs were the outcomes considered in the NUREG/CR-4550 analyses. The equations for P(X=1), P(X=2), and P(X>2) become:

$$P(X=1) = \binom{M}{1} Q_1 \tag{6.8}$$

$$P(X=2) = \binom{M}{2} \left[Q_2 + Q_1^2 \right] \tag{6.9}$$

$$\begin{aligned} P(X>2) = \binom{M}{3} \left[Q_3 + \binom{3}{2} Q_2 Q_1 + Q_1^3 \right] \\ + \binom{M}{4} \Big[Q_4 + \binom{4}{3} Q_3 Q_1 + 1/2 \binom{4}{2} Q_2^2 \\ + \binom{4}{2} Q_2 Q_1^2 + Q_1^4 \Big] \\ + \binom{M}{5} \Big[Q_5 + \binom{5}{4} Q_4 Q_1 + \binom{5}{3} Q_3 Q_2 \\ + \binom{5}{3} Q_3 Q_1^2 + 3/2 \binom{5}{2} Q_2^2 Q_1 \\ + \binom{5}{2} Q_2 Q_1^3 + Q_1^5 \Big] + \ldots \end{aligned} \tag{6.10}$$

where M is the total number of SRVs in the set being evaluated and the Qs are calculated using Equation 6.6.

It was originally intended that the NUREG/CR-4550 analyses would use diesel generator common cause information directly from an NRC in-house data base. However, the analysis teams did, in fact, use the techniques discussed above to develop the appropriate beta factors for diesel generators. The availability of the NRC data base should be explored in any future studies.

The uncertainty associated with most beta factors was modeled as lognormally distributed with an error factor of 3. A sensitivity analysis on the data classification in EPRI NP-3967 was conducted as part of the project staff expert judgment elicitations (Reference 70). It was decided that an error factor of 3 for a lognormal distribution was sufficient to encompass the true beta factors, even if large errors in data classification existed in the EPRI work. In fact, it was the judgment of the analysts that the data in the EPRI report was well classified in general, and that any error sufficient to surpass the uncertainty range covered by an error factor of 3 was improbable.

The beta factor parameter estimates and their uncertainty are summarized in Table 6.2-1.

Table 6.2-1
Common Cause Beta Factors

Component	Number of Components	Lognormal Parameters	
		Mean	Error Factor
DC Battery - Fail to Deliver Power	See Note 1		
Diesel Generators - Fail to Start	Two	0.038	3
	Three	0.018	3
	Four	0.013	3
Service Water Motor Driven Pumps (SWS, CCWS) Fail to Start	Two	0.026	3
	Three	0.014	3
	Four	0.0096	3
Low Pressure Coolant Injection Motor Driven Pumps (RHR, LPCI, LPCS, LPIS) Fail to Start	Two	0.15	3
	Three	0.11	3
	Four	0.10	3
High Pressure Injection Motor Driven Pumps - Fail to Start	Two	0.21	3
	Three	0.10	3
Containment Spray Motor Driven Pumps - Fail to Start	Two	0.11	3
Auxiliary Feedwater Motor Driven Pumps - Fail to Start	Two	0.056	3
	Three	0.030	3
Motor Operated Valves - Fail to Operate	Two	0.088	3
	Two	0.054	3
	Three	0.057	3
Air Operated Valves - Fail to Operate	Two or more	0.10	3
PWR Safety Relief Valves - Fail to Open	Two	0.07	3

Table 6.2-1
Common Cause Beta Factors (Cont.)

Component	Number of Components	Lognormal Parameters Mean	Error Factor
BWR Safety Relief Valves - Fail to Open	Two	0.22	3
	Three	0.15	3
	Four	0.12	3
BWR Safety Relief Valves - Fail to Reclose	See Note 2		

1) Beta factors for two redundant batteries are estimated from Table 6 in NUREG-0666.[24] Plant specific information on the configuration of the DC power system is used to determine the actual value used for the beta factor. For three or more redundant batteries, Equation 6.5 is used in conjunction with the beta factor for two.

2) See Step 6.6 of Dependent Failure Development.

6.2.2 Subtle Failure Development

In this portion of the analysis subtle interactions or subtle design peculiarities are identified. These types of interactions are sometimes buried in the depths of the design and operation of the system and can be difficult to uncover. The process to identify these failures involves several steps illustrated in Figure 6.2-2.

Step 6.7. Obtain Information for Subtle Interactions

In this step the analyst obtains the necessary information required for identifying the subtle failures. This process is performed as part of the Plant Familiarization Analysis task (see Section 2), and involves:

- Gathering essential information, e.g., procedures, system descriptions, P&IDs, instrumentation and control drawings,
- Examining plant data, e.g., LERs, maintenance logs, etc.
- Reviewing previous safety analyses

Step 6.8. Review Plant Design

The analyst reviews system designs to determine whether any peculiarities exist which might result in reduced system availabilities. These are identified by determining the response of the system, its components, and supporting systems to (1) each initiating event and (2) the various phenomena caused by each initiating event. Interactions not already included in the model from the systems analysis (Section 5.0) must be incorporated into the event trees or fault trees.

Step 6.9. Review Plant Operational History

The analyst reviews LERs and plant data to identify any peculiar interfaces between systems and components. Failures that have not been included in the system models or event trees must be incorporated in the models.

Step 6.10. Identify Subtle Interactions

In this step the analyst identifies any additional subtle interactions. In the NUREG/CR-4550 analysis to ensure that subtleties are not overlooked, several experienced PRA practitioners from government and industry were asked to provide a list of these types of interactions that (1) have been found in past assessments and PRA-related studies or (2) they have knowledge of based on their expertise.

Such a potential subtle interaction list is compiled before the first plant visit. During the plant visit(s), the team reviews the list with plant personnel and identifies those subtle interactions applicable to that plant. These interactions are then analyzed and added to the system models. The subtle interactions assessed during the NUREG/CR-4550 study are described below.

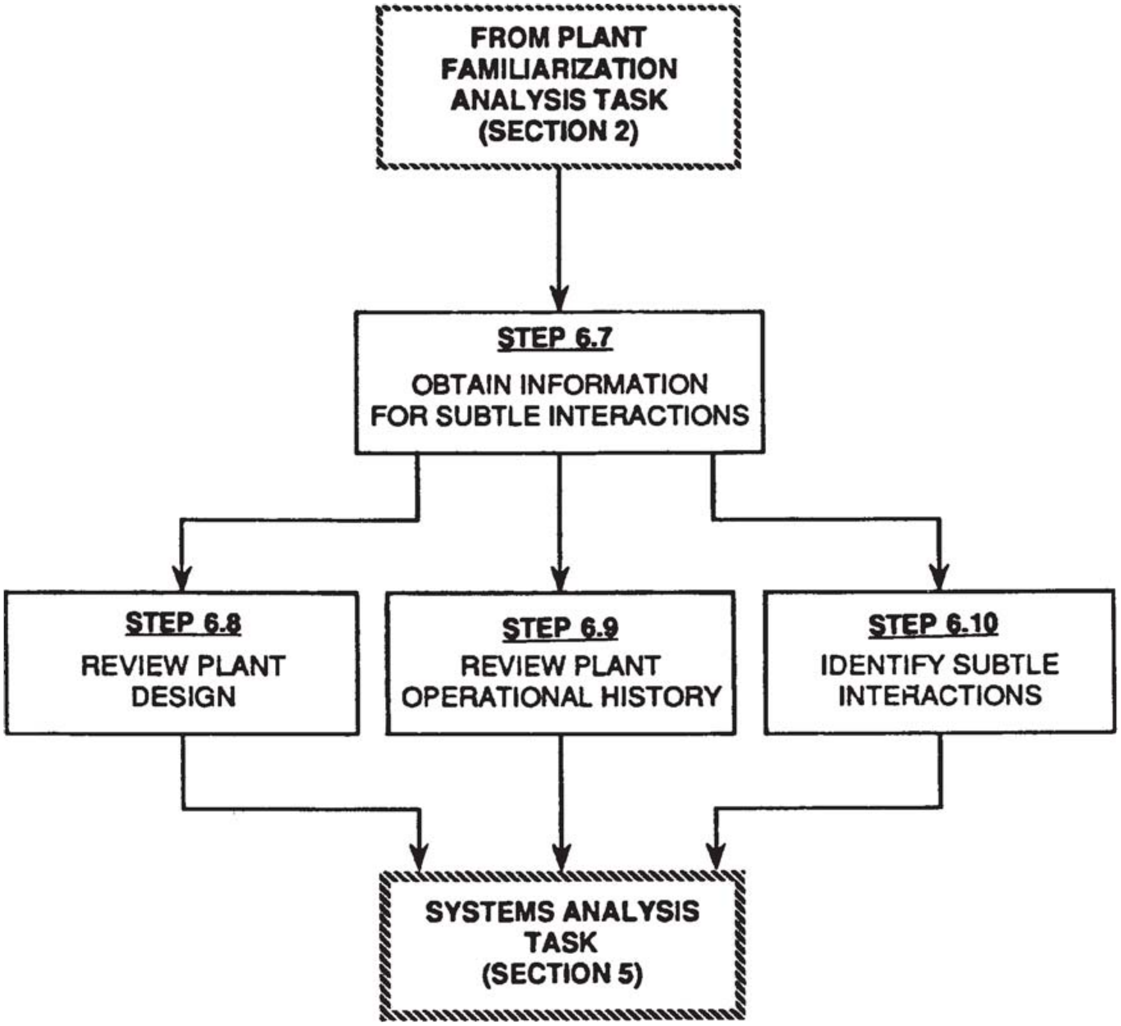

FROM PLANT FAMILIARIZATION ANALYSIS TASK (SECTION 2)
STEP 6.7
OBTAIN INFORMATION FOR SUBTLE INTERACTIONS
STEP 6.8
REVIEW PLANT DESIGN
STEP 6.9
REVIEW PLANT OPERATIONAL HISTORY
STEP 6.10
IDENTIFY SUBTLE INTERACTIONS
SYSTEMS ANALYSIS TASK (SECTION 5)

Figure 6.2-2. Step Relationship for Subtle Failure Analysis.

1. DG Load Sequence Failures

Description

The Interim Reliability Evaluation Program studies[7,29,30,31] identify several single failures in a diesel generator load sequencer system of a BWR. The circuit is designed to strip off loads on the DGs following LOSP. The circuit uses redundant trip relays to ensure that this function is accomplished.

The circuit (Figure 6.2-3) is designed to work in the following manner: (1) a LOSP deenergizes the coils associated with Contacts 1 through 4; (2) upon deenergization, these normally-open contacts close; (3) given closure of Contacts 1 or 2, Trip Coil A energizes; (4) given closure of Contacts 3 or 4, Trip Coil B energizes; and (5) if either of the trip coils are energized, all loads are stripped off the DGs and can not be reloaded. As can be seen, redundancy is employed in this load stripping circuit. The problem with this circuit design is that redundancy is not employed during the subsequent reload.

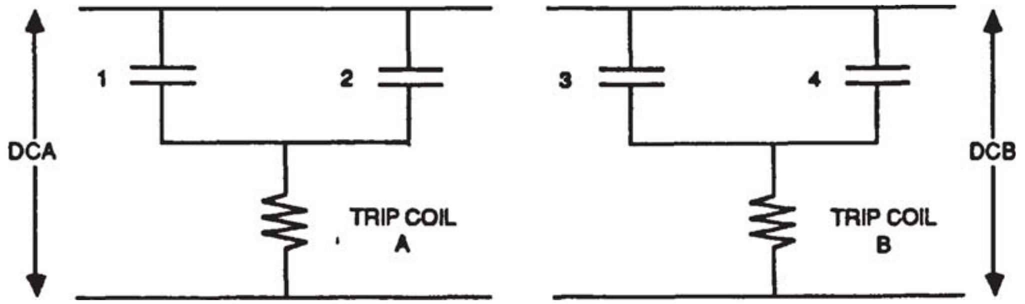


Figure 6.2-3. BWR Load Sequencer.

Applicability to Particular Plants

The PRA analyst should review the load stripping and reloading portion of the diesel load sequencer circuit to ensure that redundancy is employed during both load stripping and reloading.

2. Sneak Circuits Following Power Restoration

Description

Sandia National Laboratories (SNL) recently discovered a potential problem in the Reactor Core Isolation Cooling (RCIC) system circuitry at a particular BWR. The problem occurs following power restoration to the RCIC circuits. This could occur during a LOSP and subsequent energization of the circuits by the diesel. Because of the design of the RCIC steam leak detection circuit, it is possible for a sneak circuit to occur and cause an unintended isolation of the RCIC pump.

Fault tree analysis is not a very good tool for identifying such a failure mode because it is caused by a sequencing problem in the relays. Since fault trees are generally time-independent, they are normally incapable of identifying sequencing failure modes.

It appears there are at least three subtle design aspects which lead to the occurrence of this failure mode: (1) the RCIC system contains an isolation circuit, (2) the isolation circuitry is deenergized given a LOSP (i.e., the circuitry is not fed by a noninterruptible, battery-backed vital AC power supply), and (3) the isolation circuit contains a seal-in circuit.

The sneak circuit interaction can be followed in the circuit diagrams illustrated in Figure 6.2-4. Within this particular RCIC control system, there exists the potential for a nonrecoverable RCIC isolation preceding a station blackout. This isolation can result from the restoration of power to Bus 242 or 236X-3 (242Y feeds 236X-3, thus the same result for loss of power to either bus). The postulated scenario occurs in a situation where a total LOSP is followed by a subsequent failure of Bus 242 after it has been reengerized with the diesel or an alternate feed from Unit 1.

The normal circuit condition preceding a loss of Bus 242 is shown in circuit diagrams 1, 2, and 3. The steam leak detection relay, K4B (circuit diagram 3) is normally energized. This holds the K4B contact pair in circuit diagram 2 open. This prevents K33 from energizing, preventing the K33 contact pair in circuit diagram 1 from closing. When a high temperature is detected, one of the four high temperature switches (circuit diagram 3) opens, deenergizing K4B; this closes the K4B contact pair (circuit diagram 2), energizing K33. When K33 energizes, its contact pair in circuit diagram 1 closes, energizing the closing coil for F063. When the F063 contactors close, contact Ca in the F063 closing circuit seals in ensuring the valve travels to the full closed position. This is the way the circuit is designed to function isolating the RCIC system when a steam leak is indicated.

The condition of these same three circuits following a loss of power to the steam leak detection circuit is shown in circuit diagrams 4, 5, and 6. The loss of power can result from a loss of 242, 236X-3, or a failure of the circuit breaker or fuses supplying the Steam Leak Detection (SLD) circuit.

When the circuit deenergizes, K4B (circuit diagram 6) deenergizes, closing the K4B contact pair in circuit diagram 5. This would cause the F063 valve to close because it would appear as if one of the temperature switches had opened, indicating a steam leak. However, the K10B and K11B relays in circuit diagram 6 also deenergize, opening their contact pairs in circuit diagram 5, preventing K33 from energizing. The potential for an isolation of the RCIC system occurs when power is restored to the SLD circuit. This condition is shown in circuit diagrams 7 through 9. This would occur following a LOSP when the DG reenergizes Bus 242. When the SLD circuit is reenergized, both K10B and K11B contacts in circuit diagram 8 close. At the same time, the K10B contact in circuit diagram 9 closes to energize K4B, which will open the K4B contact pair in circuit diagram 8. This should keep K33 from energizing, preventing the K33 contacts in circuit diagram 7 from closing, causing F063 to close. However, the K10B contacts in circuit diagram 9 must close before the K4B relay can energize. Since the K10B contact pair in circuit diagram 8 closes at the same time as the contact pair in circuit diagram 9, there exists a momentary delay in the K4B contacts opening in circuit diagram 5 while the K4B relay energizes. This short duration completion of the K33 control circuit allows K33 to momentarily energize, closing the K33 contacts in circuit diagram 1. This energizes the F063 closing coil. This closes the F063 contactors, causing the Ca seal-in contacts to close, driving the F063 valve to the full closed position, isolating the RCIC system. This condition is shown in circuit diagrams 10 through 12. This does not normally create a problem, since it follows power restoration and the operator can manually reopen F063 from the control room after resetting the isolation signal. The situation is worse should a station blackout occur, followed by restoration of power to the steam leak detection circuit before the operator notices the RCIC isolation and manually reopens F063.

Applicability to Particular Plants

The PRA analyst identifies those systems that are potentially affected by isolation control systems. PWRs typically have a steam generator isolation system that may also isolate the Auxiliary Feedwater (AFW) system. BWRs typically have a steam leak detection isolation system on RCIC and (HPCI).

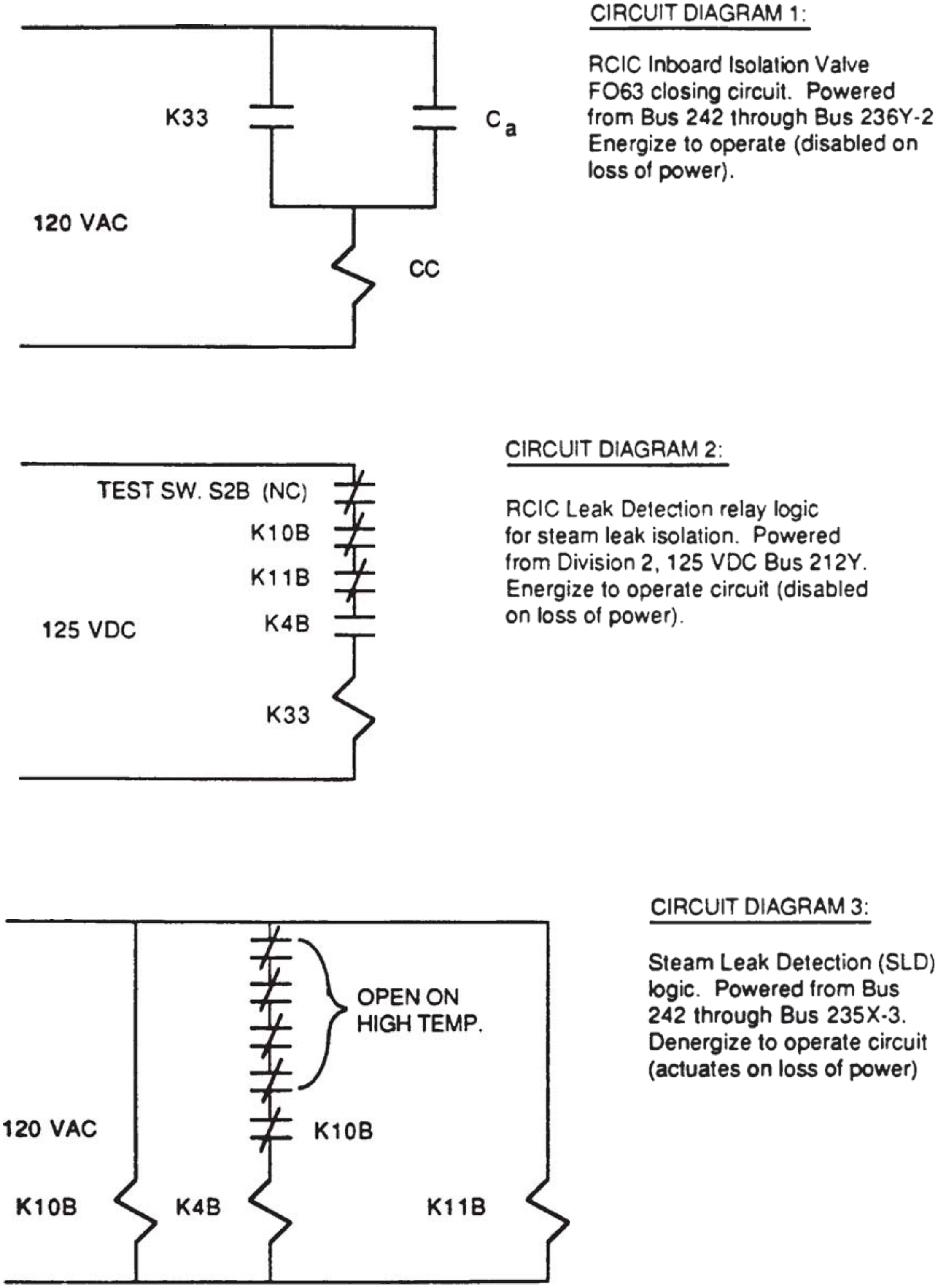
The analyst determines whether these isolation systems have a noninterruptible power supply feeding them. If the circuit receives power from a DC bus or from a vital AC bus, the power can be considered uninterruptible. (Vital AC power is obtained from a DC bus via an inverter.)

Finally, the isolation circuits are examined to determine if they contain a seal-in feature.

3. Bus Switching Logic Problems

Description

Brookhaven National Laboratory recently discovered a problem in the bus switching logic at a PWR. There are at least two subtle aspects to this interaction: (1) a safety-related DC power supply is also being used to perform a bus switching operation in the switchyard and safety-related loads are normally powered from the unit transformer rather than from



CIRCUIT DIAGRAM 1:

RCIC Inboard Isolation Valve FO63 closing circuit. Powered from Bus 242 through Bus 236Y-2 Energize to operate (disabled on loss of power).

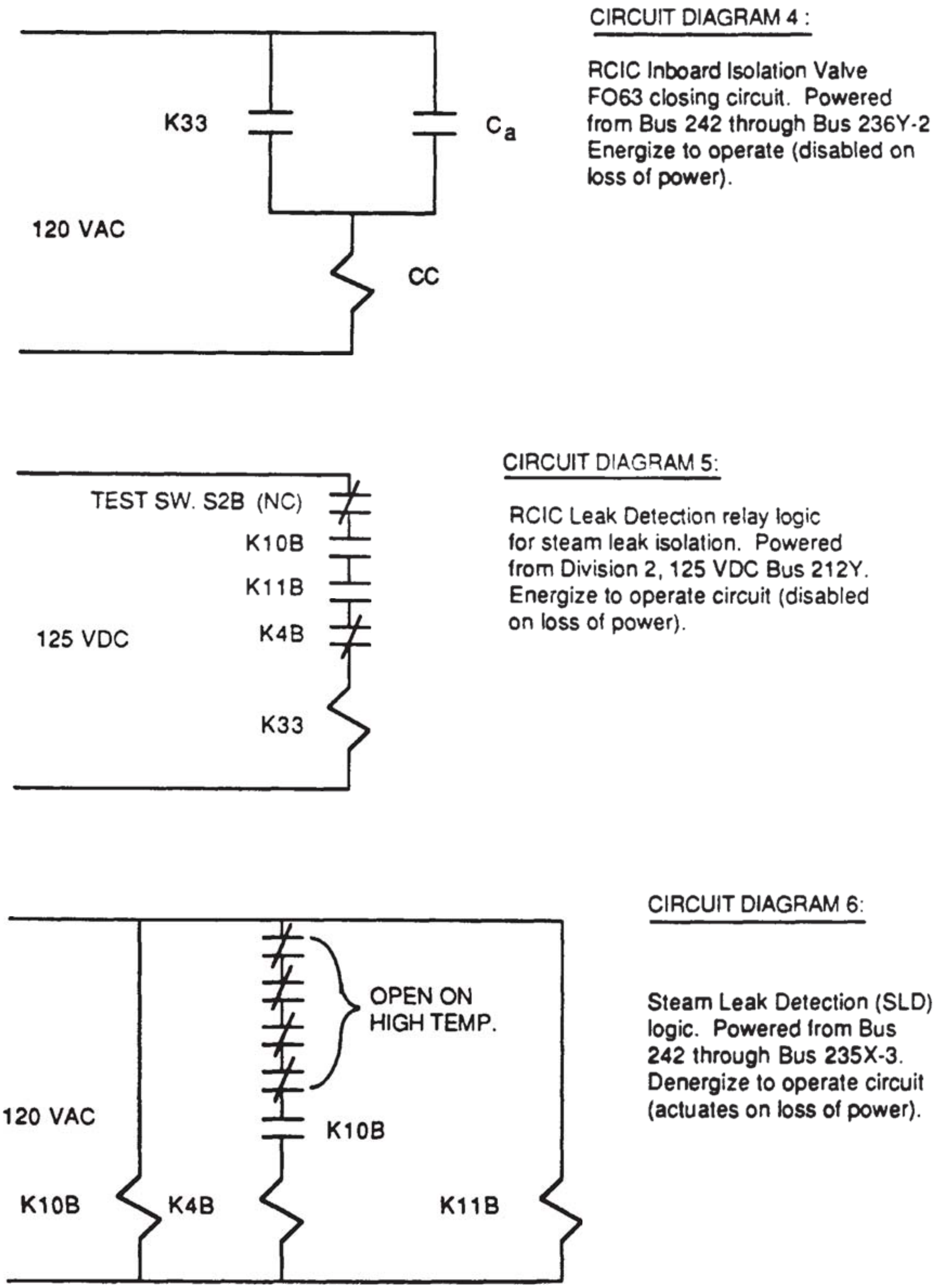
CIRCUIT DIAGRAM 2:

RCIC Leak Detection relay logic for steam leak isolation. Powered from Division 2, 125 VDC Bus 212Y. Energize to operate circuit (disabled on loss of power).

CIRCUIT DIAGRAM 3:

Steam Leak Detection (SLD) logic. Powered from Bus 242 through Bus 235X-3. Denergize to operate circuit (actuates on loss of power)

Figure 6.2-4. RCIC Steam Leak Isolation Circuitry (Page 1 of 4).



CIRCUIT DIAGRAM 4 :

RCIC Inboard Isolation Valve FO63 closing circuit. Powered from Bus 242 through Bus 236Y-2 Energize to operate (disabled on loss of power).

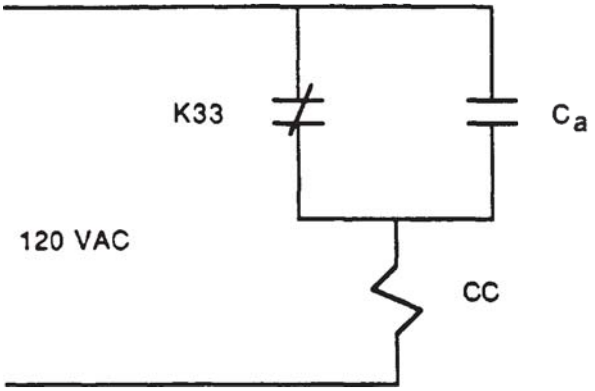
CIRCUIT DIAGRAM 5:

RCIC Leak Detection relay logic for steam leak isolation. Powered from Division 2, 125 VDC Bus 212Y. Energize to operate circuit (disabled on loss of power).

CIRCUIT DIAGRAM 6:

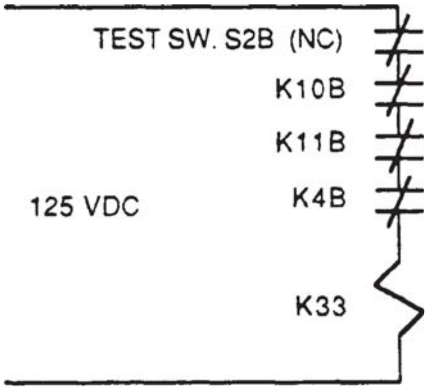
Steam Leak Detection (SLD) logic. Powered from Bus 242 through Bus 235X-3. Denergize to operate circuit (actuates on loss of power).

Figure 6.2-4. RCIC Steam Leak Isolation Circuitry (Page 2 of 4).



CIRCUIT DIAGRAM 7:

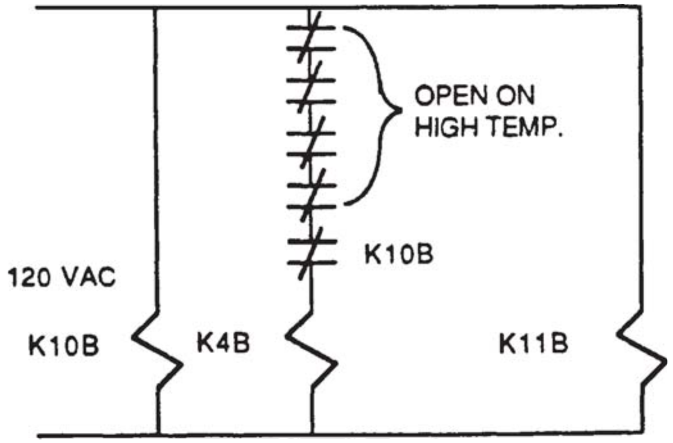
RCIC Inboard Isolation Valve FO63 closing circuit. Powered from Bus 242 through Bus 236Y-2 Energize to operate (disabled on loss of power).



CIRCUIT DIAGRAM 8:

RCIC Leak Detection relay logic for steam leak isolation. Powered from Division 2, 125 VDC Bus 212Y. Energize to operate circuit (disabled on loss of power).

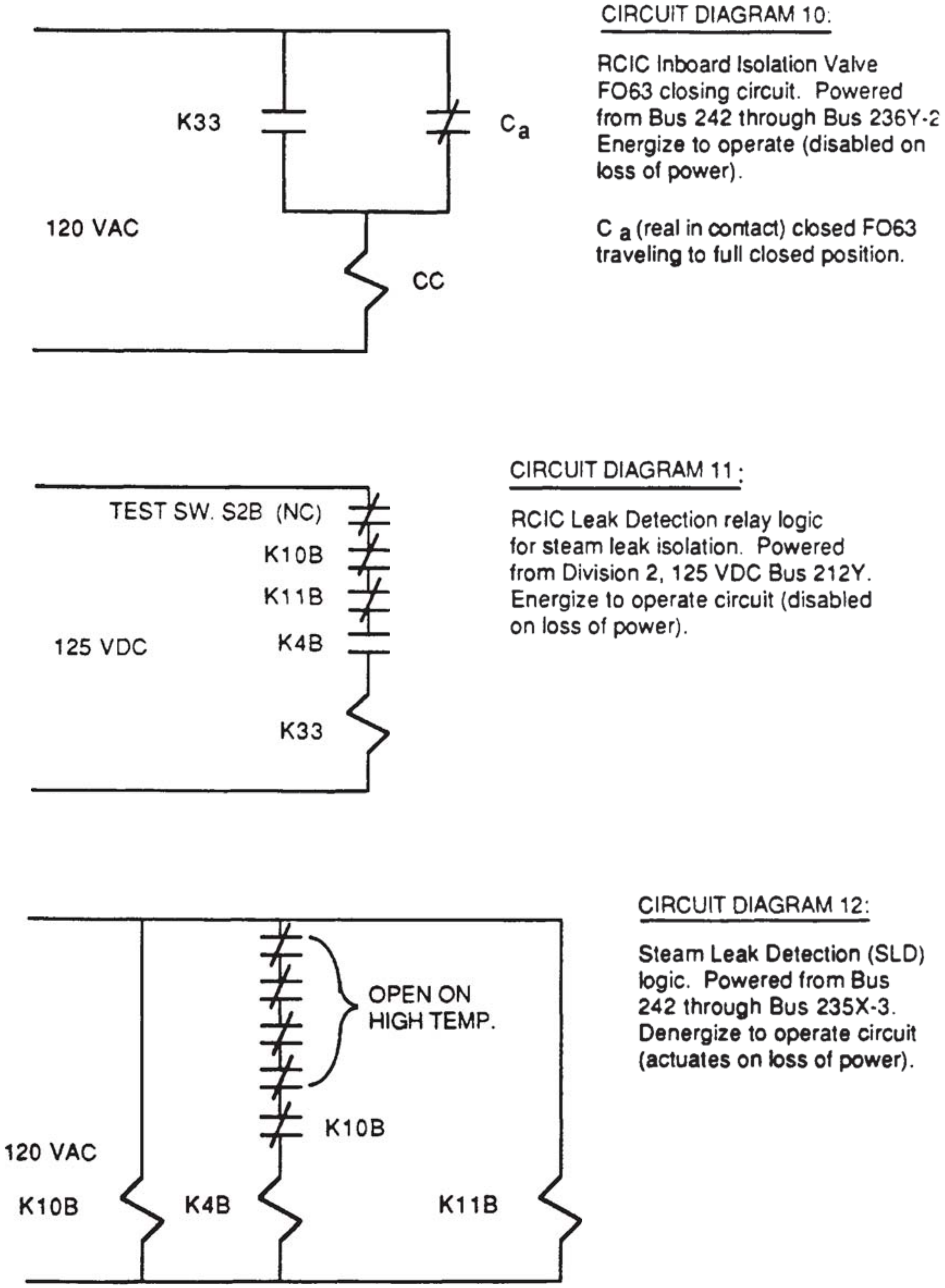
Contact state K4B begins to energize after K10B has closed.



CIRCUIT DIAGRAM 9:

Steam Leak Detection (SLD) logic. Powered from Bus 242 through Bus 235X-3. Denergize to operate circuit (actuates on loss of power).

Figure 6.2-4. RCIC Steam Leak Isolation Circuitry (Page 3 of 4).



CIRCUIT DIAGRAM 10:

RCIC Inboard Isolation Valve FO63 closing circuit. Powered from Bus 242 through Bus 236Y-2 Energize to operate (disabled on loss of power).

C_a (real in contact) closed FO63 traveling to full closed position.

CIRCUIT DIAGRAM 11:

RCIC Leak Detection relay logic for steam leak isolation. Powered from Division 2, 125 VDC Bus 212Y. Energize to operate circuit (disabled on loss of power).

CIRCUIT DIAGRAM 12:

Steam Leak Detection (SLD) logic. Powered from Bus 242 through Bus 235X-3. Denergize to operate circuit (actuates on loss of power).

Figure 6.2-4. RCIC Steam Leak Isolation Circuitry (Page 4 of 4).

offsite power; and (2) a safety-related AC bus does not have a diesel directly powering it; it must rely on diesel power from another bus via a breaker which only closes given a LOSP.

Applicability to Particular Plants

The PRA analyst examines the systems modeled and determines if they are powered from the plant generator through an auxiliary transformer or from offsite power lines. For those systems that are powered from the turbine, the analyst identifies the switchyard circuit breakers that must transfer to allow these systems to be powered from offsite power following a turbine trip and identifies the power supplies required by these circuit breakers.

The analyst also determines which safety-related circuit breakers at the plant require a LOSP signal before changing state. Obvious ones are the circuit breakers that are used to connect the diesel to the Emergency Safeguard Features (ESF) bus. The power supplies required by these circuit breakers should also be identified.

4. Pump Room Cooling

Description

A particular plant design may be such that, given loss of room cooling, the maximum room temperature remains below the temperature for which a pump and its control circuits are qualified. An analyst may, therefore, conclude that room cooling for this pump is not required. However, upon further investigation, it is found that a room cooler isolation control circuit exists which trips the pump at 200°F; this temperature is reached within twenty minutes following loss of room cooling. Therefore, room cooling is actually required for this pump.

SNL has found room cooler test procedures to be inadequate at two different plants. In both cases it was found that a portion of the actuation circuit was never verified to be functioning properly. These cases are briefly described below:

1. At one plant, it was determined that cooling of the ESF switchgear room was required. The cooling system was safety-grade and was tested monthly. The cooling system was actuated by a wall-mounted thermostat. However, the monthly test required the cooler to be started via a switch which bypassed the thermostat portion of the actuation circuit. The plant has since changed the test procedure so that the availability of the thermostat is verified monthly. The plant now uses a hot air blower to actuate the thermostat.

2. At another plant it was determined that cooling of the Residual Heat Removal (RHR) pump room is required. The room cooler at this plant is actuated from a slave relay following pump start. The RHR pumps are tested monthly.

> However, the pump test procedure does not require test personnel to verify that the room cooler is functioning properly.

It is becoming a standard practice in PRAs to assign very low non-recovery probabilities to failure of room cooling. The rationale for this is that all the operators have to do is open the door to the room to allow natural circulation cooling to occur. This may not be a plausible recovery method for certain rooms that have doors whose open and close status is under administrative control or governed by technical specifications. For example, certain Emergency Core Cooling System (ECCS) pumps are enclosed behind water-tight flood doors that are only allowed to be in the open position for a short time. This severely hampers recovery efforts following loss of room cooling.

Applicability to Particular Plants

The PRA analyst identifies those systems that have room coolers. Documentation and engineering judgment supporting whether room cooling is actually required for system success is obtained. For those systems that are believed not to require room cooling, it is determined if there is a pump isolation control circuit present that actuates on high room temperature and how long it will take to reach the isolation temperature given loss of room cooling. These isolation circuits are typically located in steam-powered systems such as turbine-driven AFW pump trains, HPCI, and RCIC systems.

For those systems determined to require room cooling, the analyst verifies that test procedures exist and that the entire actuation circuit is being tested.

The PRA analyst also determines whether there are administrative controls or technical specifications that govern the status of the room doors for those systems that require room cooling.

5. Voltage Droop

Description

PRAs typically assume that a LOSP occurs instantaneously. There have been several LOSPs in the industry in which it took several minutes for the grid to degrade to the point at which offsite power was totally lost. During these several minutes, the grid voltage or frequency "drooped" out of tolerance. This degraded condition may cause fuses to blow following subsequent power surges and breakers to open within plant systems that are normally powered from the grid. At one plant, breakers apparently opened in some of the normally operating service water pumps. These pumps are also used to supply cooling to the diesels. As a worst case, this event can result in a station blackout if all the service water pumps trip off before the total LOSP. In this case, the operators recognized the problem and reset the breakers before the total LOSP.

Because of events like this, many plants have upgraded the circuits that cut off the grid supply to the plant. Some plants have raised the cutoff set point so that grid separation occurs before significant degradation of the grid.

Applicability to Particular Plants

The analyst determines if these conditions can occur and if modifications have been performed at the plant being analyzed. If so, this interaction is not applicable. Otherwise, the chance of blown fuses or inadvertent breaker openings should be considered.

6. Terminal Block Inside Containment

Description

Recent equipment qualification studies indicate that many types of terminal blocks do not perform adequately in a steam environment. (A terminal block is located in an electrical junction box and is used to connect wire ends within a circuit.) Studies indicate that instrument errors can occur in circuits that contain terminal blocks when exposed to a high temperature (> 100°C) saturated steam environment. There is a concern that ECCS actuation systems which contain terminal blocks in containment will malfunction following a Loss of Coolant Accident (LOCA) and not actuate core cooling in time to prevent core damage.

Applicability to Particular Plants

The PRA analyst determines if modeled systems have terminal blocks located within the containment or other areas that may be subjected to steam and where in the circuits they are located. If terminal blocks are only found in the actuation system, it may not be necessary to perform a detailed analysis if manual actuation of these systems has a high probability of success (e.g., > 0.99). Many newer plants do not have terminal blocks in containment.

7. Isolation of all Feedwater Flow

Description

Many PWRs have steam generator isolation control systems that are designed to shut off all feedwater to the generator given low secondary pressure. These systems have caused problems at PWRs in the past. For example, at one plant a power bus failure caused the secondary atmospheric dump valves to open. This resulted in the blowdown of all steam generators. The isolation system actuated and cut off all main and auxiliary feedwater flow to the generators. Following this event, some plants made modifications to the steam generator isolation logic so that simultaneous isolation of all steam generators is prohibited. The fix allows isolation of a subset of the steam generators that are below the low-pressure actuation setpoint, but prohibits isolation of all of them if they are all at low pressure. This ensures that some feedwater can be delivered to at least one of the generators given a common cause event occurs that causes all generators to go below the low-pressure isolation setpoint.

Applicability to Particular Plants

The PRA analyst determines if the plant has a steam generator isolation control system that isolates both main and auxiliary feedwater from a depressurized steam generator. If this condition is found, a failure mode and effects analysis is performed to determine if there are credible single events that can cause simultaneous depressurization of all steam generators.

8. Alternate Core Cooling Systems

Description

Many published PRAs have only given credit for safety grade core cooling systems. This may be unduly conservative. Many plants have several alternate core cooling modes that are not preferred or safety grade but can be used in an emergency as a "last ditch effort." The following list gives examples of these core cooling modes:

- Using service water to supply makeup to the PWR steam generator or the BWR reactor;
- Aligning a diesel fire pump to supply makeup to the PWR steam generator or the BWR reactor;
- Increasing control rod drive injection system flow in BWRs;
- Blowing down the reactor vessel (BWR) or steam generators (PWR) and allowing the condensate pumps to inject, or
- Aligning the boron injection pumps from a large water source.

These types of alternate core cooling systems should be considered in a PRA analysis if the following conditions are met:

- Use of these systems are described in the emergency procedures;
- A flow rate of at least 200 gpm can be delivered to the PWR steam generators or the BWR reactor; and
- The time required to establish flow from these systems is consistent with cooling requirements.

Applicability to Particular Plants

The PRA analyst answers the following questions when considering the issue:

- What alternate core cooling systems are called out in the procedures?

- Have the operators received training regarding the operation of these systems?

- What is the maximum flow rate that can be delivered to the PWR steam generators or the BWR reactor from these systems?

- If the plant has more than one alternate core cooling system, in what time order are they implemented?

- How much time will the operators spend attempting to recover preferred/safety grade core cooling systems before giving up on them and attempting to establish core cooling via an alternate/non-preferred systems?

- How long will it realistically take an operator to establish core cooling using an alternate system? (It should be noted that some of these systems may require the use of special tools to install components such as spool pieces.)

9. Steam Binding of the Auxiliary Feedwater Pumps

Description

Steam binding of AFW pumps has been shown to be a problem at PWRs as reported in an AEOD report.[32] Several of the instances reported occurred at the PWRs under investigation in the NUREG/CR-4550 studies.

Applicability to Particular Plants

The analyst reviews the above report to determine its applicability to their specific plant. The status of MOVs (normally open or closed), the presence of common headers, and procedures for testing the system are all important factors.

10. Air Binding of Cooling Water Systems

Description

There have been several incidents involving the failure or partial failure of the cooling water systems because of air binding caused by leaks in a load being cooled. The plant compressed air systems have both compressor cooling and aftercoolers that are supplied with some form of cooling water. If a leak develops in these coolers, the higher pressure air will enter the cooling system and could result in air binding. This is particularly a problem with closed-cooling systems, but could also be a problem with open systems. This can result in failure of multi-train systems, depending on plant design. Depending on the other loads on the cooling system, this potential common cause failure of the air system and the entire cooling system can be important as a failure or an initiating event.

Applicability to Particular Plants

The PRA analyst determines if there are compressed air loads on the important cooling water systems and if air-binding can occur in one cooling water train and propagate to another.

11. Steam Line Break Isolation Circuitry

Description

There have been several cases of problems involving isolation of steam-driven systems in BWRs. These systems usually have isolation circuitry to protect against steam-line breaks. This circuitry uses temperature readings as an indication of a line break. These temperature readings may include all locations where the steam pipe is routed. Therefore, when assessing the need for room cooling, the cooling requirements of equipment in all areas where isolation temperature readings are taken must be considered. This can be overlooked by just assuming a need for cooling of the room where the pump is located. This problem is further complicated because some plants have the cooling to these other areas as nonessential loads. It should also be noted that this type of event is not limited to BWRs.

Applicability to Particular Plants

The PRA analyst determines if there are steam-line break isolation signals in steam-driven systems and where all input measurements for isolation are taken. If the areas containing these input measuring devices require room cooling, the analyst models this dependency. Also, the analyst determines if this room cooling system is subject to power load sheds or cooling water isolations that effectively fail the system.

12. Passive Component Failures

Description

The internal event core-damage frequency in one PWR PRA[33] is dominated by the failure of a manual butterfly valve in the discharge of the nuclear service water system. This valve is in a common line that nearly all of the service water loads discharge to before returning to the lake. Failure of this valve in a manner that blocks flow prevents cooling of most safety loads. In addition, this scenario is difficult to diagnose and even more difficult to recover from. Although passive failures (e.g., stem/disc separation) of valves are rare; these events need to be considered at pinch points, particularly in common support systems. It is also interesting to note that the plant has experienced this failure mode in a service water valve of the same design and size as the common valve. The valve that did fail is further upstream and only blocked flow from one RHR heat exchanger.

Applicability to Particular Plants

The PRA analyst reviews plant systems for common components and considers component failure modes that might not otherwise be modeled (e.g., pipe break, blockage, failure of a valve due to stem/disc separation). These failures are added to the models where the impact of failure affects multiple trains or when they are in important support systems. These events are also considered as potential initiators.

13. Isolation of Nonessential Cooling Water Loads

Description

Sometimes the failure to isolate the nonessential headers of an important cooling water system can result in inadequate cooling of the essential loads because of the potential for pump runout and failure. This means that care should be taken when determining the impact of potential diversion paths from support cooling systems.

Applicability to Particular Plants

The PRA analyst reviews flow and cooling requirements for the important cooling systems to determine if nonessential load isolation is critical to system performance.

14. Discharge Check Valve Failures for Cross-Tied Pumps

Description

There have been many occurrences of system failure caused by failure (stuck open) of the discharge check valve in one train of a two-train, cross-tied system. Thus, when one pump is turned on with the other pump idle, the flow simply recirculates backward through the idle pump and results in functional failure of the system. The same failure mode occurs if one pump operates and the other fails while its discharge valve is stuck open. Thus, even if the backflow itself is not sufficient to constitute failure of the system, a stuck-open check valve can be important if the normally operating pump fails and the idle pump cannot be actuated, or if the attempted actuation of the idle pump results in system rupture. Sometimes, the check valves in both trains have been found stuck open at the same time. This failure mode is not normally included in system fault trees, but this review suggests that perhaps it should be.

The importance of this event is determined by the failure probability of the check valve. This failure probability is partially determined by the procedure involving the pump tests. How often are the check valves functionally tested for their ability to prevent backflow? If the pump discharge valve on the idle pump is closed or the trains are isolated during test, the check valve may receive a plant lifetime of demands with no verification that the valve reseats to a closed position preventing backflow. On the other hand, other indications such as loss of water from a water leg fill system could lead to a continuous status check, depending on system configuration.

Applicability to Particular Plants

The PRA analyst locates all the cases of multiple-pump systems with normally-open cross-ties. For each system, the verification frequency for the pump discharge check valve operability is determined. This involves review of normal operations and system test procedures, as well as any regular maintenance activities during cold shutdown. The analyst also determines approximate demands on the check valve over the period where verification is not ensured.

15. System Failure Following Station Blackout

Description

In a review of eight PRAs relative to the station blackout issue, there is a vast difference in treatment of the failure modes of reactor coolant pump seals following loss of seal cooling (often the result of a total LOSP), and in treatment of battery depletion. These differences introduce a significant degree of uncertainty into the PRA, since they are all based on analyst assumptions and little or no data.

Applicability to Particular Plants

The PRA analyst determines the details of the reactor coolant pump seal design, reviews any plant-specific analyses, and collects any applicable experience. For the battery depletion question, the analyst determines the actual loads on the batteries for a station blackout condition, reviews the design criteria, and collects any data on actual full load battery tests to estimate battery depletion times.

16. Dependent Events based on Operating Experience

Description

There have been a number of recent activities to better scope out the problem of dependent and common cause events. Probably the best current collection of actual events that are in the nuclear data base are compiled in EPRI NP-3967.[20] While there is considerable controversy on how to account for common cause events, the report clearly demonstrates the inaccuracy of models that do not specifically treat common cause events. While it has been a frequent criticism that quantification of these events leads to numbers but no indication of how to improve plants, a review of the events in EPRI NP-3967 will demonstrate that causes are known for a large percentage of these events.

Applicability to Particular Plants

See Steps 6.3 and 6.4 earlier in this section.

17. Main Feedwater Following Plant Trip

Description

Many PRAs have demonstrated that the availability of main feedwater after a plant trip is highly plant-specific and that it is, therefore, not correct to make assumptions about main feedwater availability. For many plants, main feedwater is not available at all following a reactor trip.

Applicability to Particular Plants

The PRA analyst specifically reviews both design and experience to determine an appropriate model for main feedwater for the full range of initiating events. This includes (1) collecting data on main feedwater availability by reviewing all trip reports, (2) establishing the initiating event conditions that affect feedwater and determining its availability for each case, and (3) reviewing the potential for recovering feedwater in critical timeframes.

18. Refill of Dry Steam Generators

Description

Different PWR operators appear to have different concerns relative to refill of a dry steam generator. At some plants it is administratively precluded, but operators say they would use the option; at others, operators say they would not use the option. Another issue is whether the admission of water can lead to damage that makes the sequence more serious (i.e., many broken tubes leading to LOCA and containment bypass).

Applicability to Particular Plants

To help resolve this issue, the PRA analyst determines the order of core cooling options called for by the plant procedures and whether the operators will use these options, particularly when all other alternatives have failed.

19. Main/Auxiliary Feedwater Commonalities

Description

A PWR PRA[34] identifies a number of areas in which failure modes for the main feedwater system can also affect the emergency (or auxiliary) feedwater system. Although newer plants are likely to have virtually total separation between the two systems, other plants may also exhibit similar problems.

In this case, the Emergency Feedwater (EFW) pumps draw suction from the upper surge tank. When this tank becomes depleted, the operators are instructed to switch suction over to the main condenser hotwell. (As a side note, the two motor-driven EFW pumps can draw only a limited amount of water from the hotwell following the switchover, because of the location of their suction pipe; and then, only if the condenser vacuum is broken. For cooling beyond about two hours, the plant must rely on the turbine-driven EFW pump alone.) The primary purpose of the upper surge tank is to accommodate fluctuations in the condensate inventory during power operation. This leads to several potential problems. For example, if there is a large leak or rupture in the main feedwater or condensate lines, the operators must take quick action to isolate the break before the upper surge tank inventory is depleted by draining to the condenser as inventory is lost. This can happen in as little as four to five minutes in the case of a large feedwater line break. A more frequent occurrence is the loss of instrument air, which causes loss of main feedwater. It also causes the makeup valve from the upper surge tank to the condenser hotwell to fail open, rapidly draining the upper surge tank. If the loss of air is a consequence of a LOSP (the air compressors are all load-shed), the situation is somewhat worse, since the valve the operators must open to supply suction to the turbine-driven pump from the hotwell is motor-operated, and its power supply is also load-shed.

Applicability to Particular Plants

The PRA analyst determines if the plant AFW systems have an ensured source of suction supply that will last for the duration of plausible demands on the system. If, following a loss of main feedwater, the AFW system relies on portions of the main feedwater and condensate systems or any other systems that supply them, such as demineralized water, the analyst determines any potential common failures that affect both systems.

20. PORV Block Valve Closure

Description

Many PWRs have trouble with leakage from PORVs and, as a matter of practice, have a large PORV unavailability because of block valve closure (there are some cases where the valves are closed more than 80% of the time). In many PRAs, it has been assumed that the technical specifications prohibit this, but this is often not the case. The PORV unavailability can lead to a different characterization of plant sequences since a transient-induced LOCA is more likely if the safety valves must lift because the PORVs are unavailable. This topic is also critical to the anticipated transient without scram sequences and the success of feed and bleed.

Applicability to Particular Plants

The PRA analyst includes block valve closure in the Systems Analysis and determines, from experienced operators and plant data, the percentage of time that the PORV block valves are closed.

21. Overfill of Steam Generators

Description

PRAs have been somewhat inconsistent in their treatment of steam generator overfill leading to failure of a turbine-driven pump. Water carry-over through the steam lines to the turbine can lead to a sequence involving successful initial response followed by a later loss of the turbine-driven feedwater pump.

Applicability to Particular Plants

The PRA analyst determines what control actions (automatic or manual) are required to prevent steam generator overfill and the impact of each initiating event and failure of each support system on these control actions. The analyst also determines if the operators will have instrumentation in the various situations. This condition could similarly apply to turbine-driven systems for BWRs.

22. Normal Operating Configuration

Description

Various plant-specific PRAs have shown that the normal operating configuration of systems cannot always be inferred from plant P&IDs. For example, the P&ID shows valves as normally closed when, in reality, the plant operates with these valves open. As another example, the P&ID indicates that a room containing three high-pressure injection pumps has two room coolers, each receiving power and cooling water from a different division. Discussions with the plant revealed that, during normal operation, only one of the two room coolers is normally operating. Further discussion also revealed that it is not prohibited to power the cooler fan from Division 1 and supply the cooling water to the cooler heat exchanger from Division 2. By correctly modeling the normal operating configuration of this system, several single failures of the three high-pressure injection pumps were identified.

Applicability to Particular Plants

The PRA analyst verifies with plant personnel the normal operating configuration of systems.

23. Locked Door Dependencies

Description

During a station blackout, the security system at some plants locks the powered security restrictive and key-locked doors, that is, they do not fail open, thereby, potentially restricting accident response actions. The plant configuration is not always obvious during special types of accidents such as a station blackout.

Applicability to Particular Plants

The analyst reviews the effects of loss of power on the key-locked doors and other powered security restrictive doors.

6.3 Dependent and Subtle Failures Analysis Recommended Reporting

In this task the analyst has performed a detailed analysis in identifying dependent and subtle failures. Parts of the analysis are reported in other sections which include the direct functional dependencies. These failures are reported in the Systems Analysis section of the report. However, the remaining information is generally reported in this task. This information includes the following:

- Common Cause Failure Analysis. The components that are identified as 'similar' and therefore subject to common cause failure are discussed. This discussion also includes the common cause factor used in the quantification of this failure.

- Subtle Failures. The subtle failures listed in Steps 6.8 through 6.10 are discussed. The reasons for either including or excluding each event are discussed.

6.4 Example of Dependent and Subtle Failure Analysis

The system failure models and analyses in the Peach Bottom study[4] explicitly account for the various system dependencies such as the need for power, room cooling, etc. These dependencies can be a source of possible system interactions as well as representing a common cause failure potential for the accident mitigating systems. In addition, specific tasks were performed as part of this study to address particular subtle interactions as well as common cause failures among components.

Step 6.1. Obtain Information for Dependent Failures

The dependent failure analysis was based upon information available in:

- Plant documentation, including system descriptions, Final Safety Analysis Report, instrumentation and control drawing, piping and instrumentation diagrams, and plant operations and maintenance procedures;

- Maintenance logs;

- Peach Bottom internal "hi spot" reports; and

- Licensee Event Reports.

Step 6.2. Identify Explicit Dependencies

Operation of the front-line core and containment cooling systems are directly or indirectly dependent on various support systems as noted in Section 6.2. The dependencies for the Low Pressure Core Spray (LPCS) system are shown on Figure 5.5-2, page 5-33. It may be observed that the four LPCS pumps are directly dependent upon AC and DC power, the LPCS actuation signal, and emergency service water. The pumps are less dependent upon pump room cooling (emergency service water and fans) because the lack of room cooling is only an issue for late times in an accident progression. These dependencies are incorporated into the LPCS Fault Tree, Figure 5.5-3, page 5-37. Event (or gate) LCS-3A involving loss of flow includes the Event LCS-18, No Flow from PS-25 (Pump B Discharge). This latter event includes Event LCS-26, LPCS Pump B Fails Due to Support System Failures (Figure 5.5-3, page 5-58). The further development of the support system failures is shown on Figure 5.5-3, page 5-62. In this analysis, the service water (i.e., room cooling) and electric power failures are developed and quantified as separate system trees. The failure to actuate is developed further here, but it also has events which are developed elsewhere. These transfers and relationships with other fault trees are treated appropriately in the quantification process (see Section 10).

Step 6.3. Identify Common Cause Component Groups

Using the guidelines and attributes discussed in Step 6.3 of the dependent methods earlier in this section, both front-line and support systems were analyzed for potential common cause component groups.

There were no cases observed in the Peach Bottom analysis where nonidentical but diverse components placed in redundant configurations contained identical subcomponents. Thus, there was never a need to define common cause groups consisting of subcomponents of major components. All common cause component groups involved identical or nearly identical components.

Certain types of components, such as MDPs, were grouped in different common cause groups depending on attributes such as operating pressure and function (e.g., containment cooling, component cooling, core cooling). Other component types, such as valves, were grouped into more general groups based on the type of operator (e.g., MOV, AOV, Check valve). These groupings were based on information in EPRI NP-3967[21] which shows that common cause phenomena for pumps is sensitive to the type of system in which pumps are employed, whereas for valves, operator type is more significant than the system type.

The resulting common cause component groups are:

- Diesel Generators - fail to start
- ADS valves - fail to open
- ADS accumulators - leakage
- AOVs - fail to open
- MOVs - fail to open
- Batteries - fail to deliver power

- Ventilation dampers - fail to open

- Support cooling systems (Emergency SWS, HPSWS) - fail to start

- MDPs - fail to start

- HPSWS MDPs - fail to start

- Low pressure core cooling systems (LPCI, LPCS, RHR) - fail to start

- SLC pumps - fail to start

Step 6.4. Quantitative Screening of Common Cause Component Events

The set of common cause component groups developed in Step 6.3 was used to define specific common cause events in the system models. These events are shown in Table 6.4-1. For the preliminary quantification of the system fault trees and accident sequence equations (Section 10) the common cause failures were included in the fault trees as specific basic events. Later on, in the final sequence quantification and uncertainty analysis (Section 12) the common cause events were transformed into the product of a beta factor and the relevant component total failure rate. This transformation is shown in Table 6.4-1 in the alternate event name.

For the preliminary quantification of the system and sequence models, the set of common cause events developed for the systems analysis (Table 6.4-1) did not present a significant amount of work in terms of data analysis and event quantification. For that reason, the common cause events were quantified with the final parameter estimates developed for the common cause beta factors in Steps 6.5 and 6.6. No screening quantification was necessary

Step 6.5. Data Classification

There was insufficient data on common cause events at Peach Bottom to do a plant specific analysis. Thus, the data classification process developed in EPRI NP-3967 and NUREG/CR-4780 was not used. However, the results of the data classification in EPRI NP-3967 was reviewed to ascertain whether or not the data was applicable to Peach Bottom. No data was discarded, and the generic beta factors in Table 6.2-1 were used.

Step 6.6. Parameter Estimation

Too few Peach Bottom failure data were available to quantify plant-specific common cause factors. Therefore, EPRI NP-3967[21] and other analyses,[22,23,24] were used to quantify the common cause values. Again, referring to the LPCS pump example cited above, the system success criteria requires flow from at least two pumps. Thus, common cause failure of three pumps fails the system, the common cause factor can be estimated using the equation:

$$\beta_3 = \beta_2[r_3/r_2]$$

$$= 0.15\ [5.0E\text{-}7/7.1E\text{-}7]$$

$$\beta_3 = 0.11$$

where r_2 and r_3 are taken from page 128 of Reference 22.

The event value is:

$$\text{LCS-CCF-PF-MDPS} = \text{LCS-MDP-FS-CCF} * \text{BETA-3RHRMDPS}$$

$$= 3.0E\text{-}3 * 0.11$$

$$= 3.0E\text{-}4/d$$

The other common cause factors were estimated in a comparable manner, except for batteries and AOVs which were handled as described in Section 6.2.

A complete summary of the common cause values used in the Peach Bottom analysis is presented in the Data Section of Reference 4.

Step 6.7. Obtain Information for Subtle Interactions

Subtle interactions occur as a result of design related inadequacies. That is, under abnormal conditions, a system or component does not, in fact, respond in accord with nominal design specifications. Two methods were employed to investigate these interactions. Review of (1) the system design and interfaces and (2) the Licensee Event Reports (LERs) and other plant data were used to identify any peculiar or unexpected interactions. An example of this type of interaction in the Peach Bottom PRA is tripping of the Reactor Core Isolation Cooling (RCIC) turbine by a high turbine exhaust pressure signal following failure of containment heat removal.

Step 6.8. Review Plant Design

The first type of subtle interactions examined were 'peculiar' or 'unexpected' physical interactions or phenomenological dependencies. These are modeled by virtue of the event tree constructions. For example, HPCI success followed by containment cooling failure will ultimately lead to HPCI failure because of high suction water temperature. Other systems must then be used to prevent core damage. Such a dependency is explicitly covered by the event tree construction which requires success of such systems as Condensate, CRD, etc. following success of HPCI but failure of RHR (all modes). Further information on such dependencies is covered in each event tree writeup (See Section 4.4, Reference 4) where appropriate.

Step 6.9. Review Plant Operational History

In the Peach Bottom study, this step was folded together with Step 6.10.

Step 6.10. Identify Subtle Interactions

In addition to reviewing the list of interactions presented in Section 6.2, knowledgeable experts in nuclear power plant safety analysis were asked to identify subtle system interactions which they were aware of and which could cause mitigating system failures. All of the above were reviewed to the extent possible for applicability to the Peach Bottom analysis, given the resource and priority constraints of the program. Several examples of these types of failures and their disposition are discussed below. The full list examined for Peach Bottom is provided in Reference 4.

Air binding of cooling water systems

The failure or partial failure of cooling water systems has occurred because of air binding caused by leaks in a load being cooled. Plant air compressors usually are cooled by some cooling water system. Air in leakage into the cooling water system can cause failure of multiple systems because of air binding and loss of cooling.

The two most critical service water systems (Emergency Service Water, ESW, and High Pressure Service Water, HPSW) do not directly interface with air systems. Review of the Peach Bottom licensee event reports and maintenance records did not reveal problems in this area. Hence, this does not seem to be significant at Peach Bottom and so is not explicitly modeled.

Bus switching problems

Two subtle aspects concerning bus switching have been identified at one power plant: (1) a safety-related DC power supply is also being used to perform a bus switching operation in the switchyard and safety-related loads are normally powered from the unit transformer rather than from offsite power, and (2) a safety-related AC bus does not have a diesel directly powering it; it must rely on diesel power from another bus via a breaker which only closes given a loss of offsite power.

Resources did not permit a detailed review of bus switching at Peach Bottom. The analysis methodology called for "simple" modeling of the onsite bus arrangement. Since there are no similar bus-to-bus cross feeds in normal use at Peach Bottom and since a diesel exists on all four division safety 4160V buses, the problem did not appear important for Peach Bottom.

Table 6.4-1
Peach Bottom Common Cause Events

EVENT NAME	DESCRIPTION
ACP-CCF-LP-DGS (ACP-DGN-LP-CCF*BETA-4DGNS)	Common cause failure of all four diesel generators
ADS-CCF-CC-ADSRV (ADS-AOV-CC-CCF*BETA-3SRVS)	Common cause failure of at least three ADS valves to open
ADS-CCF-CC-NADSV (ADS-AOV-CC-CCF*BETA-4SRVS)	Common cause failure of at least four non-ADS safety relief valves to open
ADS-CCF-LK-ACC (not separated into two events; value based on engineering judgment)	Common cause failure of ADS accumulators (leakage)
CSS-CCF-LF-MOVS (CSS-MOV-CC-CCF*BETA-2MOVS)	Common cause failure of the two containment spray injection valves to open
DCP-CCF-LP-BAT (DCP-BAT-LF-CCF*BETA-5BAT)	Common cause failure of at least five batteries to supply sufficient power to their loads
EHV-CCF-LF-AOVS (EHV-AOV-CC-CCF*BETA-6AOVS)	Common cause failure of at least six ventilation dampers (for diesel room cooling) to open
ESW-CCF-LF-AOVS (ESW-AOV-CC-CCF*BETA-3AOVS)	Common cause failure of at least three emergency service water valves (to supply diesel jacket cooling) to open
ESW-CCF-PF-MDPS (ESW-MDP-FS-CCF*BETA-2SWPS)	Common cause failure of the two primary emergency service water pumps
HSW-CCF-LF-MDPS (HSW-MDP-FS-CCF*BETA-4SWPS)	Common cause failure of all four high pressure service water pumps

Table 6.4-1
Peach Bottom Common Cause Events (Concluded)

EVENT NAME	DESCRIPTION
HSW-CCF-LF-MOVS (HSW-MOV-CC-CCF*BETA-4MOVS)	Common cause failure of all four high pressure service water valves (used for supply to RHR heat exchangers) to open
LCI-CCF-LF-MOVS (LCI-MOV-CC-CCF*BETA-2MOVS)	Common cause failure of the two LPCI injection valves to open
LCS-CCF-LF-MOVS (LCS-MOV-CC-CCF*BETA-2MOVS)	Common cause failure of the two LPCS injection valves to open
LCS-CCF-PF-MDPS (LCS-MDP-FS-CCF*BETA-3RHRMDPS)	Common cause failure of at least three LPCS pumps
RHR-CCF-PF-MDPS (RHR-MDP-FS-CCF*BETA-4RHRMDPS)	Common cause failure of all four RHR (also used for LPCI) pumps
SLC-CCF-PF-MDPS (SLC-MDP-FS-CCF*BETA-2SIPUMPS)	Common cause failure of both standby liquid pumps
SPC-CCF-LF-MOVS (SPC-MOV-CC-CCF*BETA-2MOVS)	Common cause failure of the two suppression pool cooling valves to open

Room cooling

Several aspects concerning pump room cooling must be considered in a PRA systems analysis. First, a given plant's design may be such that, given loss of room cooling, the maximum room temperature remains below the temperature for which a pump and its control circuits are qualified. A system analyst may, therefore, conclude that the room cooling for the pump is not required. However, in some cases, a room temperature signal is used to trip the pump. The potential for reaching this temperature given loss of the room cooler should be examined.

Second, pump room coolers are often standby systems that actuate only upon actuation of the pump through a slave relay or by a thermostat. In either case, test procedures should be such that all of the actuation circuit is verified to function properly.

Finally, credit for opening pump room doors for cooling the room given failure of the room cooler should only be taken after considering administrative controls and technical specifications which may prohibit such action.

Peach Bottom predominantly uses slave relay type circuits and high room temperature trips of HPCI/RCIC because of the use of steam-line break detection thermocouples in the turbine rooms. There are typically numerous ways to detect loss of room cooling: steam line break detection circuitry, cooling trouble alarms, separate fire detection circuitry, etc. Failure of all indications seems small. Isolation and even failure of systems caused by high temperatures in rooms was considered for systems where appropriate (see individual systems analysis sections of this report). While it may be possible for plant staff to recover room cooling failures (such as opening doors to critical areas normally locked) credit was not given for such recovery due to the uncertainty as to whether or not such actions would successfully restore adequate cooling (some rooms represent closed-in, static areas where adequate flow is uncertain).

Alternate core cooling systems

There are methods of core cooling available, which although not preferred and not necessarily safety grade, could possibly be used in emergency situations. Some examples of such methods include:

- use of service water to supply makeup to the reactor,
- aligning a fire water pump to supply makeup to the reactor,
- increasing control rod drive injection system flow,
- aligning the boron injection pumps from a large water source.

In order to qualify as an alternate core cooling method during a transient (with scram) condition, several criteria are essential:

(1) Procedures must call out these systems and adequately describe their use (it is additionally useful if there is appropriate training on use of the systems and if procedures define the time order in which each system implementation should be attempted).

(2) The ability to deliver a flow rate of at least 200 gpm to the reactor must exist.

(3) The time required to establish flow from these systems is consistent with cooling requirements.

Appropriate systems, particularly the Control Rod Drive (CRD) and HPSW, are considered in the Peach Bottom analysis as alternate core cooling systems.

7. HUMAN RELIABILITY ANALYSIS

The treatment of human action is an important aspect of any Probabilistic Risk Assessment (PRA). Given the high degree of hardware reliability and redundant design associated with nuclear power plant systems, human interfaces with the system are often significant contributors to system unavailability. The human actions may involve errors that range from a failure to restore the equipment to operability following test and maintenance tasks to errors in manipulating the equipment in response to accident situations. On the other hand, operators may take action to correct misalignments of equipment or to overcome failures under accident conditions.[4,37] This section describes the methodology used to identify potential human errors in response to accidents, and to quantify the most significant of these.

7.1 Human Reliability Concepts, Assumptions and Limitations

The basic concepts and most of the assumptions and limitations pertinent to the human reliability analysis (HRA) methodology described in this section can be found in the Accident Sequence Evaluation Program Human Reliability Analysis Procedure, hereafter known as the ASEP HRA Procedure,[35] upon which the HRA methodology presented here is based.

The HRA methodology is divided into separate methodologies for pre-accident tasks and post-accident tasks. Pre-accident tasks considered are those which, if performed incorrectly, could result in the unavailability of systems or components to respond appropriately to an accident. Post-accident tasks evaluated are those which are intended to cope with an abnormal event, that is, to return the plant systems to a safe condition. A brief synopsis of the concepts pertinent to the pre-accident and post-accident methodologies are presented in the next two paragraphs and they are discussed in more detail in the appropriate subsections.

The pre-accident HRA methodology emphasizes restoration errors, i.e., errors involving returning components to their normal states after completion of maintenance, calibration, or testing. It is based on the use of a generic human error probability (HEP, the probability that an error will occur when a given task is performed) of 0.03 as the basic human error probability (BHEP, the probability that an error will occur when a given task, which is not influenced by a previous task, is performed). The BHEP is a combination of errors of commission (ECOM, incorrect performance of a task or performance of an extraneous task) and errors of omission (EOM, failure to perform a task). Credit is given for recovery factors (RFs, factors that limit or prevent the undesirable consequences of a human error). Dependence, the situation in which the probability of failure (or success) of an activity is different, depending upon the success or failure of another activity, is assessed. Provision is made for a reassessment of the BHEP of 0.03 on the basis of a more detailed analysis of the plant administrative control procedures and their implementation.

The post-accident HRA methodology employs the diagnosis model from NUREG/CR-1278.[36] Diagnosis involves defining the actions required to cope with a disruption in the normal conditions of the plant. This is accomplished by identifying the system or components whose status can be changed to reduce or eliminate the disruption. Special allowances are made for the practice of recognizing deviations of critical parameters related to reactor/containment integrity. In the context of this document, the critical parameters are those variables pertaining to the protection of the reactor core that control room operators are trained to monitor and to which they respond. Less conservative (presumably more realistic) HEPs and credit for more than one person are allowed for the post-diagnosis actions, and emphasis is placed on measurement (rather than estimation) of simulated response times.

One of the assumptions of probabilistic risk assessments (PRAs) is that sufficiently accurate quantitative estimates of human performance can be made. A limitation is that such estimates often have a substantial uncertainty. Uncertainty in this context includes random variability in some parameter or measurable quantity and an imprecision in the analyst's knowledge about models, their parameters, or their predictions. It is difficult to predict human behavior, particularly combined with complex systems. Additionally, there are no large collections of data available to use in quantitative estimates of human behavior. Therefore, the estimates for human error probabilities (HEPs) and response times (i.e., the times required to perform some task) tend to err on the conservative side, i.e., if an error of estimation occurs, the estimates of HEPs and response times are larger rather than smaller than the "true" situation.

Each estimated HEP is assumed to represent a median value on a lognormal distribution of HEPs. As discussed in Chapter 7 of NUREG/CR-1278,[36] it is recognized that other distributions often occur but, for PRA work, it is convenient to assume a lognormal distribution and, within wide bounds, it does not matter too much whether the distribution is exactly lognormal.

The shape of the lognormal distribution reflects the estimated uncertainty in the estimation of an HEP. This uncertainty includes the variability of people and conditions and the uncertainty of the analyst in assigning HEPs to a task. The error factor (EF) is the square root of the ratio of the 95th percentile to the 5th percentile of the lognormal distribution. Some of the EFs in this HRA methodology section represent EFs for estimated total failure probabilities that are based on several HEPs. These EFs were calculated by the computer procedure described in Appendix B of the ASEP HRA Procedure.[35] For more detail on the uncertainty distributions and EFs, see Chapter 2 of the ASEP HRA Procedure.

This procedure is a simplified approach to HRA. Care must be taken when low numbers and combinations of numbers are derived. Screening values (e.g., .5 and 1.0) are used to assure that cut sets with potentially important human errors are not lost in the initial screening of sequences. For post-accident HRA values, a review and justification is required when a single basic event value falls below 1E-3 and when multiple basic event values in a cut set fall below 1E-4.

Only human actions related to mistakes made in the performance of assigned tasks are considered. Deliberate acts of sabotage are not considered. It is assumed that all plant personnel act in a manner they believe to be in the best interests of the plant. It is assumed that the tasks are performed by licensed, qualified plant personnel who are experienced, i.e., to have functioned in their present positions for at least six months. The environment in the control room is not adverse, the levels of illumination and sound and the provisions for physical comfort are adequate.

7.2 Pre-Accident Human Reliability Development

The pre-accident tasks of interest consist of routine and corrective maintenance, calibration, surveillance tests, and restoration (i.e., the returning of components and systems to their normal conditions following maintenance, calibration, or testing). These tasks are performed by operations personnel, instrumentation and control personnel, and maintenance personnel under non-accident conditions. The pre-accident tasks can affect the availability of safety systems needed for coping with an accident sequence.

Some potential errors in the maintenance of components are not included in the HRA analysis because such errors have already been counted in the failure rate estimates for components, and it would be inappropriate to count human errors twice. These kinds of maintenance errors usually refer to repairs or adjustments. Maintenance errors not usually part of the failure rate data are those involving post-maintenance (PM) and post-calibration (PC) testing to see that a component works properly after maintenance or calibration. It is imperative that the analyst identify those component failures which testing would not detect. The methodology allows for this occurrence as well as the possibility that the PM or PC test is done incorrectly.

The ASEP HRA Procedure presents a simplified model of human behavior for pre-accident tasks. The model included a generic basic human error probability (BHEP) of 0.03 that can be used for all pre-accident tasks as well as rules to adjust this BHEP for the effects of recovery factors.

A series of three tables (Tables 7.2-1, 7.2-2, and 7.2-3) were constructed to document the ASEP HRA Procedure methodology used to obtain nominal human error probabilities (NHEP) and appropriate distributions for the pre-accident basic events. A nominal HEP is one in which the best (i.e., most accurate) estimate of the failure probability is used, as distinguished from a conservative (i.e., deliberately high) estimate. The ASEP HRA methodology documented by the tables is described in the following steps, which are illustrated in Figure 7.2-1.

Step 7.1. Obtain Information for Pre-Accident Analysis

A plant visit is part of the Plant Familiarization Analysis task. During this visit, observations are made of pre-accident tasks. These observations should include some actual calibration tasks and post-calibration and post-maintenance tests as well as talking through several pre-accident procedures as they are being performed, emphasizing

Table 7.2-1
Dependence Effects For Pre-Accident HRA

Systems (1)	Task (2)	Activities (3)	Multiple Components (4)	Series/ Parallel (5)	Time Reference (6)	Location Reference (7)	Written Requirements (8)	Generel Location (9)	Dependence ECOM EOM (10)	Comments Source Of Information (11)

Table 7.2-2
Identification of Recovery Factors

Systems	Task	Activities	Compelling	Post-Main/	Written	Written	Total RF		Comments/
(1)	(2)	(3)	Signals	Calib. Test	Verification	Daily/Shiftly	Credit	EF	Source Of Information
			(4)	(5)	(6)	(7)	(8)	(9)	(10)

Table 7.2-3
Post-Maintenance or Post Calibration HEPs

Systems	Task	Activities	Comp	BHEP	RF	Series	Parallel				NHEP	EF	Comments/Source
(1)	(2)	(3)	(n)	(5)	(6)	EOM/ECOM	ECOM	EOM			(8)	(9)	Of Information
			(4)			ZD	ZD	ZD	CD	HD			(10)
						n(BHEP*RF)	$(ECOM*RF)^n$	$(EOM*RF)^n$	(EOM*RF)	$(EOM*RF)(.5)^{n-1}$			
						<--------------------------		(7)		---------------------------->			

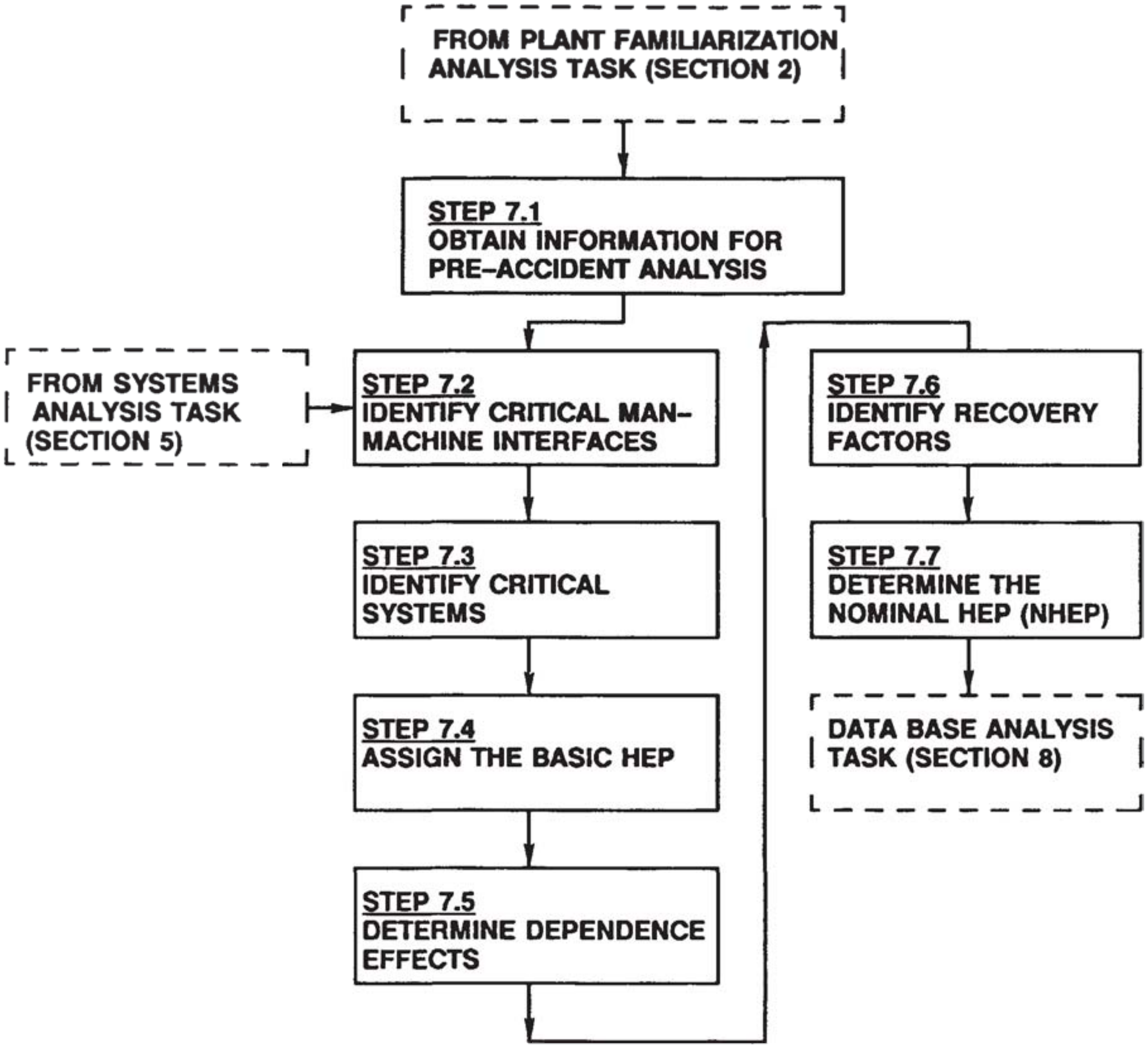

FROM PLANT FAMILIARIZATION ANALYSIS TASK (SECTION 2)
STEP 7.1 OBTAIN INFORMATION FOR PRE-ACCIDENT ANALYSIS
FROM SYSTEMS ANALYSIS TASK (SECTION 5)
STEP 7.2 IDENTIFY CRITICAL MAN-MACHINE INTERFACES
STEP 7.3 IDENTIFY CRITICAL SYSTEMS
STEP 7.4 ASSIGN THE BASIC HEP
STEP 7.5 DETERMINE DEPENDENCE EFFECTS
STEP 7.6 IDENTIFY RECOVERY FACTORS
STEP 7.7 DETERMINE THE NOMINAL HEP (NHEP)
DATA BASE ANALYSIS TASK (SECTION 8)

Figure 7.2-1. Step Relationship for Pre-Accident Human Reliability Analysis

restoration tasks. Discussions should be held with operating personnel who actually perform the tasks. Relevant written procedures and other documentation that spell out operating sequences and rules are collected.

This includes administrative, surveillance, calibration, testing and maintenance procedures, and system descriptions, plant layout drawings and technical specifications.

Step 7.2. Identify Critical Man-Machine Interfaces

The critical man-machine interfaces have been identified in the Systems Analysis Task. This identification has not been a one-time endeavor but a continuously evaluated and re-evaluated one. This procedure is done to assure that no failures due to human error have been overlooked.

Step 7.3. Identify Critical Systems

The information obtained in Steps 7.1 and 7.2 is used to define the critical systems and associated tasks and activities. These are then documented as the first three items on Tables 7.2-1, 7.2-2, and 7.2-3. A description of these items follows.

1. Systems. The critical system under investigation is listed.
2. Task. A description of what is being done or has not been done by the human component in the system is inserted.
3. Activities. The specific action that must be done to complete the task and restore the system to its correct configuration is described.

Step 7.4. Assign the Basic HEP

A basic HEP of 0.03 was selected as a conservative HEP for pre-accident tasks as part of the developmental effort in the Risk Methods Integration and Evaluation program (RMIEP, NUREG/CR-4832). This basic HEP was also adopted for the ASEP HRA Procedure, and for the methodology presented in this document. The 0.03 basic HEP (BHEP) was based on some HRAs and additional reviews of pre-accident procedures at the LaSalle nuclear power plant. For more detailed information, see Chapter 3 of the ASEP HRA Procedure.[35]

The BHEP of 0.03 is for performance of pre-accident actions, exclusive of recovery factors (RFs), and represents a combination of a generic HEP of 0.02 assessed for an EOM and a generic HEP of 0.01 assessed for an ECOM, with the conservative assumption that an ECOM is always possible if an EOM does not occur. Therefore, the total failure term (or probability) for a one-component system is 0.03*. Reference to the tables in Chapter

* If it is not possible to observe pre-accident tasks (or to receive talk-throughs of these tasks) or if administrative control procedures cannot be evaluated adequately, the ASEP HRA Procedure requires the use of a 0.05 BHEP in place of the 0.03 BHEP.

20 of NUREG/CR-1278[36] show that the 0.03, and its constituents of 0.02 and 0.01, represent conservatism in that these HEPs are larger than many of the basic HEPs in NUREG/CR-1278 that are related to pre-accident actions.

No downward adjustment of the BHEP value of 0.03 should be made without performing a more thorough HRA.

Step 7.5. Determine Dependence Effects

The BHEP of 0.03 must be modified for the effects of dependence. Rules are defined for assessing the effects of within person dependence, that is, dependence between the activities performed by one person. A new dependency model and associated rules of application for systems analysts who do not have a formal background in HRA were developed and presented in the ASEP HRA Procedure and used in this methodology.

Table 7.2-1 documents the dependency between the activities for each task. The information collected to determine dependency effects is documented in items 4 through 9. The assignment of the dependencies is documented in item 10. A description of these items follows.

4. Multiple Components. Components manipulated in the performance of the task and associated activities are listed. If only one component is manipulated, there is no dependence and Table 7.2-1 is not necessary.

5. Series/ Parallel. Dependency effects are treated differently for parallel systems and series systems. A parallel system is one in which failure occurs only if all components in a system are unavailable; system success occurs as long as at least one of the components are available. A series system is one in which system success occurs only if all components in a system are available; the failure of only one component renders the entire system unavailable.

6. Time Reference. The relative time for performing each activity is determined. A decision is made on whether the activities occur closely in time, i.e., the between-activity interval for each pair of related actions is less than 2 minutes. The two-minute rule was adopted as a conservative modification of the one-minute guideline discussed under the heading "Functional Relationships Among Tasks" in NUREG/CR-1278.

7. Location Reference. Any two components are considered to be in the same visual frame of reference if the operator can see one of them without moving his head as he is performing some action on the other. In the analysis of the Grand Gulf Nuclear Power plant reported in Volume 6 of NUREG/CR-4550,[5] the same frame of reference was defined as components being within four feet of each other. While this definition is not as conservative as the one above, the difference is probably not important, and the within four feet rule is easier to apply.

8. Written Requirements. For those components not in the same visual frame of reference, is the operator required to record some information pertaining to each component in question, not just make a checkmark or record one's initials?

9. General Location. For those components not in the same visual frame of reference and with no requirements for written information about each component, note whether they are in the same general area. The same general area is defined as four feet apart.

10. Dependence. The ASEP dependence model has three levels of positive dependence: zero dependence (ZD), high dependence (HD), and complete dependence (CD). For the development and a complete description of these, see NUREG/CR-1278, a working description follows.

Zero Dependence is assessed for both the EOMs and ECOMs if the activities are on different components that constitute a series system.

Zero Dependence is assessed for the ECOMs if the activities are on different components that constitute a parallel system.

Zero Dependence is assessed for the EOMs if the activities are on different components that constitute a parallel system and for which one of the following conditions applies:

- The activities do not occur in the same time reference (i.e., not within two minutes).

- The activities occur within the same time reference (i.e., within two minutes) but the components are not in the same visual frame of reference (i.e., not within four feet of each other) and the operator is required to record information.

Complete Dependence is assessed for the EOMs if the activities are on different components that constitute a parallel system and the activities occur within the same time and visual frame of reference (i.e., within two minutes and within four feet of each other).

High Dependence is assessed for the EOMs if the activities are on different components that constitute a parallel system and the activities occur within the same time reference (i.e., within two minutes), but not in the same visual frame of reference (i.e., not within four feet) and the operator is not required to record information.

Step 7.6. Identify Recovery Factors

To assess the effects of recovery factors (RFs) on the BHEP of 0.03, a conservative approach is taken. First, each RF is applied to the 0.03 value rather than being applied separately for EOMs and ECOMs, a major conservatism. Second, the number of RFs considered in the methodology is limited. Third, if there is more than one component to be checked in a group of components being treated as a system for analysis purposes, the relevant RFs are applied to the components as a group, rather than to each component individually. This means that each RF is treated independently of the number of components in a system; each RF is counted only once to be conservative and, also, to account for the possibility that not all RFs will be employed on every occasion in which they should be employed. The recovery factor includes the effects of between person dependence between the person originally performing the task and the second person or other RF performer. Dependence between the tasks performed by one person is included in the dependency effects determination (see Step 7.5).

The RFs are identified and documented as items 4 through 7 in Table 7.2-2. A description of the items follows.

4. Compelling Signals. Activities for which errors can be assessed as fully recoverable by compelling signals are defined. Compelling signals are some kind of signal to the operator that is demanding of attention. There are usually one or more annunciators that must be cleared when a maintenance or calibration task is completed or before normal power operation can be resumed.

5. Post-Maintenance/Calibration Test. Activities for which errors will be recovered by a post-maintenance or post-calibration test if the test is performed correctly are defined. Just because a test is scheduled does not guarantee that it will be performed and performed correctly.

6. Written Verification Determine for which activities, (1) a second person is required to directly verify component status after completion of the actions by the original person, or (2) the original person is required to make a separate check of component status at a different time and place from his original performance. No recovery credit is given for either check unless a written checkoff list is used during the check.

7. Written Daily/Shiftly. Determine for which activities there is a requirement for a shiftly or daily check of component status in or outside of the control room, using a written list. No recovery credit is given for either check unless a written checkoff list is used during the check.

8. Total RF Credit. The total failure probability, F_T, is documented as the Total RF Credit. There are two tables used in the determination of F_T, Table 7.2-4 and Table 7.2-5. Table 7.2-4 is used to ascertain which set of conditions, basic or optimum, applies to the activity under investigation, and for the restrictions on the number of RFs to use.

A distinction is made between the basic conditions in which no RFs are presumed to be available and the optimum conditions in which allowable RFs are present. In the Table of RFs (Table 7.2-4), each numbered basic condition has its same numbered complementary optimum condition. For a case in which all of the basic conditions apply, the BHEP of 0.03 is assessed as the human-caused failure of some critical safety component or system that is unavailable. Recall from Step 7.4 a BHEP of 0.02 for each EOM and 0.01 for each ECOM have been assigned. The assumption has been made that an ECOM is always possible if an EOM does not occur. Therefore, for each critical action, a total BHEP of 0.03 is assigned. For a case in which all of the optimum conditions apply, the total failure probability is considered to be negligible because of the

Table 7.2-4. Basic and Optimum Conditions for the HRA of Pre-Accident Tasks
(Revised copy of Table 5-2 from ASEP HRA Procedure.[35])

Note 1: "Basic Conditions" refer to the absence of error recovery factors (RFs). "Optimum Conditions" refer to the presence of RFs. Each numbered Basic Condition has its same numbered complementary Optimum Condition.

Basic Conditions

1. No "compelling signal" exists indicating unavailable component status in the control room.

2. Post-maintenance (PM) or post-calibration (PC) tests do not verify the component status.

3. Written verification is not required.

4. Written daily or shiftly checks of component status (in or outside of the control room) are not required.

Note 2: If all of the basic conditions apply (i.e., there are no RFs), the basic HEP of 0.03 with an EF of 5 is assessed.

Optimum Conditions

1. A compelling signal exists indicating unavailable component status in the control room. A negligible HEP of 1E-5 is assessed due to the excellence of the RFs.

2. PM or PC tests verify component status. If done correctly, full recovery of any related error is assumed. An HEP of 0.01 is assessed for failure to perform the test correctly (including failure to do the test).

3. Written verification is required. An HEP of 0.1 is assessed for failure of this RF to catch an error by the original task performer. This RF is presumed to be inoperative if a required PM or PC test (see 2. above) is not performed correctly, such failure indicates inadequate quality assurance.

4. Written daily or shiftly checks of component status (in or outside of the control room) are required. An HEP of 0.1 is assessed for the failure of such a check to detect the unavailable status. For the initial nominal HRA, this RF may be used only once per error. If this conservatism results in a task having a material effect in the system analysis, perform a more detailed analysis, giving credit for the daily or shiftly schedule, per NUREG/CR-1278.

Note 3: If all of the optimum conditions apply, a negligible HEP of 1E-5 is assessed due to the excellence of the RFs.

Table 7.2-5. Cases Applicable to Critical Activities (Revised copy of Table 5-3 from ASEP HRA Procedure.[35])

Note 1: For each case below, the total failure probability, F_T, is listed with its error factor (EF) in parentheses. The F_T is the product of the basic HEP of 0.03 and the probabilities of failure of the relevant RFs.

Note 2: In the first four cases, there is no "compelling signal" as feedback. In addition, the post-maintenance (PM) or post-calibration (PC) test is not effective in the sense that, even if performed correctly, it will not catch the original error.

Case I - PM or PC Test not effective; no other RFs used:

a. All Basic Conditions apply.
b. BHEP = 0.03 = F_T. (EF = 5).

Case II - No compelling signal feedback; PM or PC Test not effective; both other RFs used:

a. Basic Conditions 1, 2 apply.
b. Optimum Conditions 3, 4 apply.
c. F_T = 0.03 x 0.1 x 0.1 = 0.0003. (EF ~ 16).

Case III - No compelling signal feedback; PM or PC Test not effective; second person or other immediate RF used:

a. Basic conditions 1, 2, 4 apply.
b. Optimum Condition 3 applies.
c. F_T = 0.03 x 0.1 = 0.003. (EF ~ 10).

Case IV - No compelling signal feedback; PM or PC Test not effective; periodic check is made:

a. Basic Conditions 1, 2, 3 apply.
b. Optimum Condition 4 applies.
c. F_T = 0.03 x 0.1 = 0.003. (EF ~ 10).

Table 7.2-5. Cases Applicable to Critical Activities (Continued)

Note 3: In the last five cases, the PM or PC Test is effective, i.e., if performed correctly, it will detect the original error.

Case V - Original error is annunciated; other optimum conditions are immaterial:

a. At least Optimum Condition #1 applies.
b. F_T = negligible. (Assess UB of 0.00001).

Case VI - PM or PC Test is effective if performed correctly; no other RFs used:

a. Basic Conditions 1, 3, 4 apply.
b. Optimum Condition 2 applies.
c. Probability of not performing or not performing correctly required PM or PC Test = 0.01
d. $F_T = 0.03 \times 0.01 = 0.0003$. (EF ~ 10).

Case VII - No compelling signal feedback; PM or PC Test is effective if performed correctly; both other RFs are used:

a. Basic Condition 1 applies.
b. Optimum Conditions 2, 3, 4 apply.
c. $F_T = 0.03 \times 0.01 \times 1.0 \times 0.1 = 0.00003$. (EF ~ 16).

Note: The 1.0 means no recovery credit is given for Optimum Condition 3 if the PM or PC Test is not done or done correctly per Optimum Condition 2.

Case VIII - No compelling signal feedback; PM or PC Test is effective if performed correctly; second person or other immediate RF is used:

a. Basic Conditions 1, 4 apply.
b. Optimum Conditions 2, 3 apply.
c. $F_T = 0.03 \times 0.01 \times 1.0 = 0.0003$. (EF ~ 10).

Case IX - No compelling signal feedback; PM or PC Test is effective if performed correctly; periodic check is made:

a. Basic Conditions 1, 3 apply.
b. Optimum Conditions 2, 4 apply.
c. $F_T = 0.03 \times 0.01 \times 0.1 = 0.00003$. (EF ~ 16).

multiplicity of RFs. For intermediate conditions, procedures are provided.

Table 7.2-5 is consulted using the basic and optimum conditions associated with each activity to determine which of nine cases applies to the activity under review. The appropriate F_T value is taken from the table. The case associated with each activity will be used in Step 7.7.

9. EF. The error factor documented in this item is the EF value from Table 7.2-5 that is paired with the F_T value in item 8.

Step 7.7. Determine the Nominal HEP (NHEP)

The information required to calculate the nominal human error probability (NHEP) is collected and documented in items 4 through 9 which are described below.

4. Comp (n). The number of components (n) in the system are listed.

5. BHEP. Recall from Step 7.4, a BHEP of 0.02 for each EOM and 0.01 for each ECOM have been assigned. A total BHEP of 0.03 is assigned for each critical action.

6. RF. This is the Total RF credit from Table 7.2-2, item 8, without the BHEP of 0.03 included.

7. Series or Parallel. The critical human actions are performed in the context of a parallel or series system. The dependency effects were discussed in Step 7.5 and documented in Table 7.2-1, items 5 and 10. These are recalled and the nominal human error probability values calculated. The NHEPs are determined in the manner described in the following paragraphs.

The upper and lower bounds are calculated by multiplying and dividing the NHEPs by the error factors. The EFs were calculated using the UCBs propagation method described in Appendix B of the ASEP HRA Procedure.

<u>Series System, ZD Assessed for EOMs and ECOMs</u>

$$\text{NHEP} = n[0.03 * \text{RF}]$$

The basic HEP value is 0.03, which is a combination of EOM (HEP = 0.02) and ECOM (HEP = 0.01) for one component.

Parallel System, ZD Assessed for ECOMs

Assume ZD regardless of conditions.

Parallel System, ZD Assessed for EOMs

$$NHEP = [0.03 * RF]^{n}$$

The basic HEP value is 0.03 which is a combination of EOM (HEP = 0.02) and ECOM (HEP = 0.01) for one component.

Parallel System, CD Assessed for EOMs

$$NHEP = 0.02 * RF$$

The ECOMs are ignored since they do not contribute materially to the NHEP.

Parallel System, HD Assessed for EOMs

$$NHEP = 0.02 * RF * 0.5^{n-1}$$

The 0.5 value is the conditional HEP for the second or more human actions following the basic EOM. The ECOMs are ignored since they do not contribute materially to NHEP.

The NHEPs calculated by the technique just described are summarized in Table 7.2-6 for 1 to 5 components. The table refers to the case numbers associated with each task; see Step 7.6.

8. NHEP. The NHEP is equal to the ECOM and EOM values documented in item 7.

9. EF. The error factor documented in this item is the EF value from Table 7.2-6 that is paired with the NHEP in items 7 and 8.

Table 7.2-6
Nominal Human Error Probabilities for Pre-Accident Activities

		Parallel System			Series System
	Number of Activities/	Zero Dependence	Complete Dependence	High Dependence	Zero Dependence
Case Number	Components	NHEP(EF)	NHEP(EF)	NHEP(EF)	NHEP(EF)
Case I	1	3E-2(5)	3E-2(5)	3E-2(5)	3E-2(5)
	2	9E-4(5)	2E-2(5)	1E-2(6)	6E-2(4)
	3	3E-5(5)	2E-2(5)	5E-3(7)	9E-2(3)
	4	negligible	2E-2(5)	3E-3(7)	1.2E-1(3)
	5	negligible	2E-2(5)	1E-3(8)	1.5E-1(2)
Case II	1	3E-4	3E-4(10)	3E-4(10)	3E-4(10)
	2	negligible	2E-4(10)	1E-4(8)	6E-4(5)
	3	negligible	2E-4(10)	5E-5(9)	9E-4(4)
	4	negligible	2E-4(10)	3E-5(10)	1.2E-3(4)
	5	negligible	2E-3(10)	1E-5(11)	1.5E-3(3)
Case III	1	3E-3(10)	3E-3(10)	3E-3(10)	3E-3(10)
	2	negligible	2E-3(10)	1E-3(11)	6E-3(7)
	3	negligible	2E-3(10)	5E-4(12)	9E-3(6)
	4	negligible	2E-3(10)	3E-4(13)	1.2E-2(5)
	5	negligible	2E-3(10)	1E-4(14)	1.5E-2(4)
Case IV	1	3E-3(10)	3E-3(10)	3E-3(10)	3E-3(10)
	2	negligible	2E-3(10)	1E-3(11)	6E-3(7)
	3	negligible	2E-3(10)	5E-4(12)	9E-3(6)
	4	negligible	2E-3(10)	3E-4(13)	1.2E-2(5)
	5	negligible	2E-3(10)	1E-4(14)	1.5E-2(4)
Case V	1-5	negligible	negligible	negligible	negligible

Table 7.2-6
Nominal Human Error Probabilities for Pre-Accident Activities (Continued)

		Parallel System			Series System
		Zero Dependence	Complete Dependence	High Dependence	Zero Dependence
Case Number	Number of Activities/ Components	NHEP(EF)	NHEP(EF)	NHEP(EF)	NHEP(EF)
Case VI	1	3E-4(10)	3E-4(10)	3E-4(10)	3E-4(10)
	2	negligible	2E-4(10)	1E-4(8)	6E-4(5)
	3	negligible	2E-4(10)	5E-5(9)	9E-4(4)
	4	negligible	2E-4(10)	3E-5(10)	1.2E-3(4)
	5	negligible	2E-4(10)	1E-5(11)	1.5E-3(3)
Case VII	1	3E-5(16)	3E-5(16)	3E-5(16)	3E-5(16)
	2	negligible	2E-5(16)	1E-5(14)	6E-5(9)
	3	negligible	2E-5(16)	negligible	9E-5(7)
	4	negligible	2E-5(16)	negligible	1.2E-4(6)
	5	negligible	2E-5(16)	negligible	1.5E-4(6)
Case VIII	1	3E-4(10)	3E-4(10)	3E-4(10)	3E-4(10)
	2	negligible	2E-4(10)	1E-4(8)	6E-4(5)
	3	negligible	2E-4(10)	5E-5(9)	9E-4(4)
	4	negligible	2E-4(10)	3E-5(10)	1.2E-3(4)
	5	negligible	2E-4(10)	1E-5(11)	1.5E-3(3)
Case IX	1	3E-5(16)	3E-5(16)	3E-5(16)	3E-5(16)
	2	negligible	2E-5(16)	1E-5(14)	6E-5(7)
	3	negligible	2E-5(16)	negligible	9E-5(7)
	4	negligible	2E-5(16)	negligible	1.2E-4(6)
	5	negligible	2E-5(16)	negligible	1.5E-3(6)

7.3 Post-Accident Human Reliability Development

Post-accident tasks pertain to activities performed by operations personnel after annunciation of some abnormal event has occurred (e.g., manually initiating a system, aligning and actuating a system for injection, switching the system from injection to recirculation, recovering a failed system). Typically, the post-accident tasks are performed by the reactor operators stationed in the control room, but they can obtain assistance from other plant personnel.

Post-accident tasks are divided into diagnosis tasks and post-diagnosis tasks, both of which are intended to maintain or ensure reactor protection once some abnormal event has occurred. Diagnosis is the identification and evaluation of an abnormal event to the level required to identify those systems or components whose status can be changed to reduce or eliminate the disruption. In short, diagnosis merely means figuring out what to do when an abnormal event has been recognized.

Diagnosis involves knowledge-based behavior, i.e., behavior applied to unfamiliar situations in which personnel have to interpret, diagnose, or use some level of decision making. Post-diagnosis tasks are those actions taken which logically follow a correct diagnosis of the abnormal event. Post-diagnosis actions involve skill-based or rule-based behavior. Skill-based behavior consists of the performance of more or less subconscious routines based on stored patterns of behavior. It does not directly depend on the complexity of the task, but rather on the level of training and the degree of practice in performing the task. While different factors may influence the specific behavior of a particular individual, a group of highly trained operators would be expected to perform skill-based tasks expeditiously or even mechanically with a minimum of mistakes. Rule-based behavior is used to denote behavior that requires a more conscious effort (than is the case for skill-based behavior) in following memorized (or written) rules. If these rules are not well practiced, they must be consciously recalled or checked. This leads to mistakes and less timely responses. The operator may not recall the procedure correctly, may be unwilling to check each step in a procedure or may not perform the steps in the proper sequence, all of which increase the potential for error.

The post-accident HRA methodology developed in the ASEP HRA Procedure employs a simplified version of the model for human behavior from NUREG/CR-1278.[36] One of the major simplifications is to ignore the entire area of specific misdiagnosis. Instead, it is conservatively assumed that any failure to correctly diagnose an abnormal event within the allowable time will result in failure to take a corrective action. No analysis is made of the possible kinds of erroneous diagnosis (i.e., misdiagnosis) that might be made for any abnormal events.

Another simplification is to segment the estimated total time available for coping with an abnormal event into artificially independent parts. The total allowable time for coping with an abnormal event is specified by systems analysts and is divided into an allowable diagnosis time and an allowable post-diagnosis time. This approach involves the estimation of two separate time-dependent probabilities: the probability of performing the correct diagnosis within its allowable time, and the probability of performing the correct post-diagnosis actions within their allowable time. The product of these two probabilities is taken to be the probability that a correct diagnosis will be made and that the correct post-diagnosis actions will be completed within the total allowable time. This is not literally true because different combinations of time-dependent probabilities for the two time periods are not considered. It appears that this simplification can result in very conservative estimates of the total failure probabilities of coping successfully with abnormal events. Nevertheless, in the absence of data which would permit full consideration of time dependencies, this simplification is considered to be acceptable.

Another simplification is the assumption that there is only one correct sequence of activities in coping with any specified post-accident sequence. The correct sequence is selected from the emergency operating procedures (EOPs) for an abnormal event. Note that this assumption does not prevent the analyst from analyzing several different sequences of activities for an abnormal event if appropriate time and resources are available. An analysis is required for each different post-accident sequence.

The methodology used to estimate the nominal human error probabilities (NHEPs) is discussed in this section. A step format, illustrated by Figure 7.3-1, is used to present the order in which the methodology is applied. A series of eleven tables (Table 7.3-1 through Table 7.3-11, pages 7-43 through 7-48) were developed to document the methodology. The tables are described in the appropriate steps.

Step 7.8 Obtain Information for Post-Accident Analysis

A visit to the plant by the analysts was accomplished during the Plant Familiarization Analysis Task (see Section 2). During this visit, for those post-diagnosis actions that are performed in the control room area, an attempt is made to measure travel time and manipulation time required by the operator. This is done through use of the training simulator or a timed walk-through in the plant control room. For travel and manipulation times outside the control room, use simulated measures (e.g., walk-throughs) to estimate the time required to get to the appropriate location and to perform the necessary post-diagnosis actions. Discussions should be held with operating personnel who actually perform the actions. Relevant written procedures and other documentation that delineate operating sequences and rules are collected. The principal procedures collected are the Emergency Operating Procedures (EOPs). The documentation includes system descriptions and plant layout drawings.

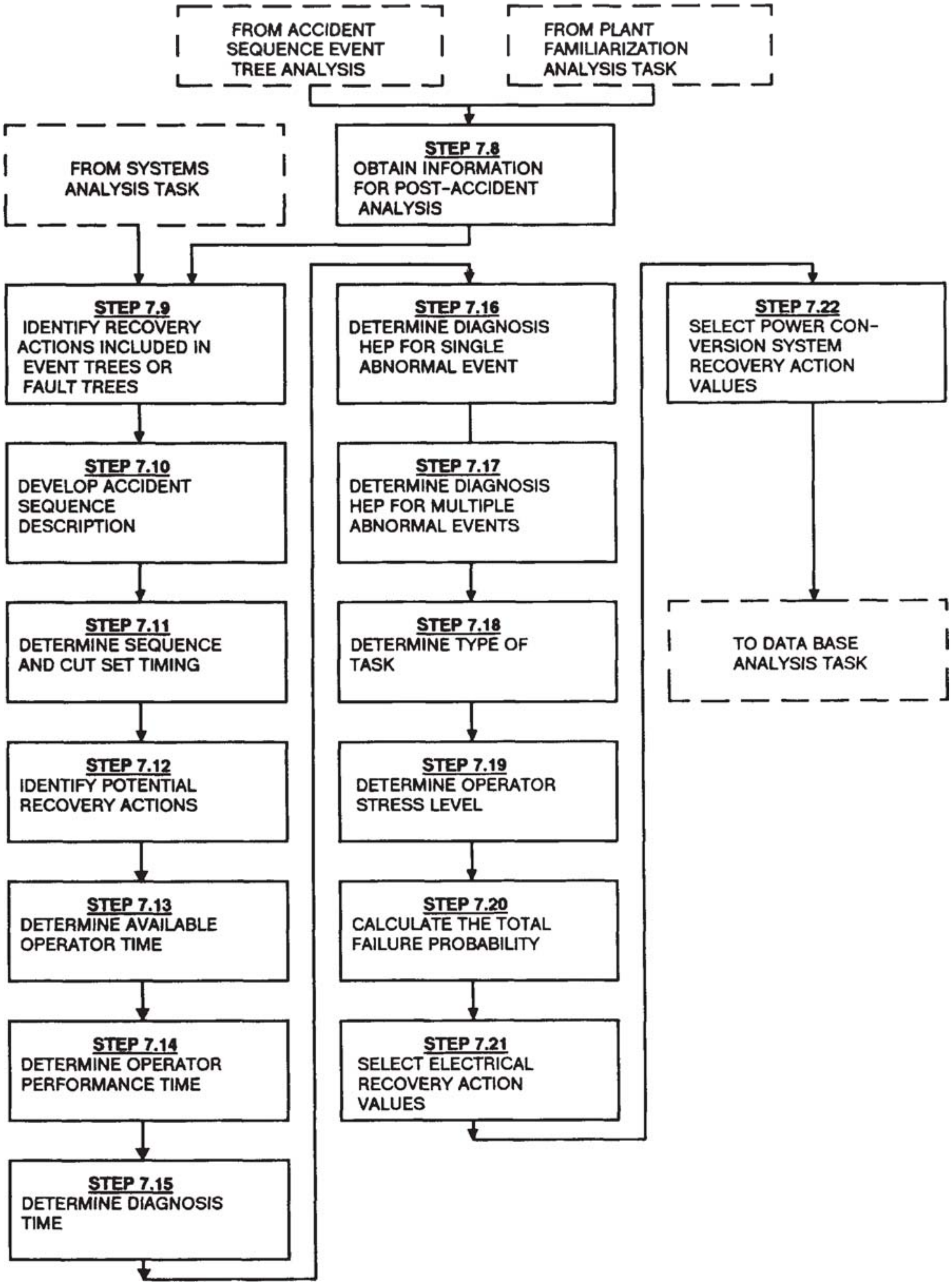

FROM ACCIDENT SEQUENCE EVENT TREE ANALYSIS
FROM PLANT FAMILIARIZATION ANALYSIS TASK
FROM SYSTEMS ANALYSIS TASK
STEP 7.8 OBTAIN INFORMATION FOR POST-ACCIDENT ANALYSIS
STEP 7.9 IDENTIFY RECOVERY ACTIONS INCLUDED IN EVENT TREES OR FAULT TREES
STEP 7.10 DEVELOP ACCIDENT SEQUENCE DESCRIPTION
STEP 7.11 DETERMINE SEQUENCE AND CUT SET TIMING
STEP 7.12 IDENTIFY POTENTIAL RECOVERY ACTIONS
STEP 7.13 DETERMINE AVAILABLE OPERATOR TIME
STEP 7.14 DETERMINE OPERATOR PERFORMANCE TIME
STEP 7.15 DETERMINE DIAGNOSIS TIME
STEP 7.16 DETERMINE DIAGNOSIS HEP FOR SINGLE ABNORMAL EVENT
STEP 7.17 DETERMINE DIAGNOSIS HEP FOR MULTIPLE ABNORMAL EVENTS
STEP 7.18 DETERMINE TYPE OF TASK
STEP 7.19 DETERMINE OPERATOR STRESS LEVEL
STEP 7.20 CALCULATE THE TOTAL FAILURE PROBABILITY
STEP 7.21 SELECT ELECTRICAL RECOVERY ACTION VALUES
STEP 7.22 SELECT POWER CON- VERSION SYSTEM RECOVERY ACTION VALUES
TO DATA BASE ANALYSIS TASK

Figure 7.3-1. Step Relationship for Post Accident Human Reliability Analysis

Step 7.9. Identify Recovery Actions Included in Event Trees or Fault Trees

Some recovery actions can be included in the event trees and fault trees. The post-accident recovery actions included in the trees are identified in the Systems Analysis task and included directly in the system model. The recovery actions included in the trees are the high-level procedural actions, which are prescribed in the Emergency Procedures Guidelines (EPGs) of the plant. There are two basic types of prescribed actions that should be considered for inclusion in the event trees and fault trees. They are:

(1) Those actions that direct the control room operators to start, or to verify the start of, automatically actuated systems when the operators reach that checkpoint in the EPGs, and

(2) Those actions that direct the control room operators to start manually actuated systems when specified conditions exist.

An example of a type (1) action is: verify the start of the high pressure core spray (HPCS) system given that the water level in the reactor vessel has reached the setpoint for automatic initiation of the HPCS system. An example of a type (2) action is, initiate cooling to the suppression pool when the suppression pool temperature exceeds a predetermined setpoint.[77]

Step 7.10. Develop Accident Sequence Description

The specific abnormal events (accident types) were identified in the Systems Analysis Task (see Section 5). They included such events as Loss of Offsite Power (LOSP), loss of coolant accidents (LOCAs), anticipated transients without scram (ATWS), loss of AC or DC bus and loss of component cooling water (CCW). The dominant accident sequences, i.e., those accident sequences determined to be of significance in the analysis (see Section 10), associated with the abnormal events are identified. Once the analyst identifies these accident sequences, the accident scenarios are developed. Table 7.3-1 was developed to document the accident sequences and associated scenarios. For convenience, this table and all others related to post-accident analysis are grouped at the end of Section 7.3 (Page 7-46). A description of the seven items used in this documentation follows:

1. **Event Tree.** The event tree identification for the accident sequence is listed.

2. **Sequence Number.** The event tree sequence number is listed.

3. **Sequence Designator.** The designator used to identify the sequence is listed.

4. **Sequence Description.** A narrative description of the accident sequence under investigation is placed here. This should include which systems are functioning successfully and which are failing. Also included are the phenomena occurring due to the failure or success of the systems, the resultant effect of this success or failure and the final outcome.

5. **Accident Type.** The specific abnormal event or type of accident is described.

6. **Accident Conditions.** A description of what is occurring at the nuclear power plant due to the abnormal event and accident sequence is placed here.

7. **Applicable Procedures.** The operator is led to specific procedures due to the accident conditions described in item 6. All relevant procedures, Emergency Operating Procedures (EOPs) or others, are listed.

Step 7.11. Determine Sequence and Cut Set Timing

The analyst determines the time at which the operator is aware that an abnormal event has occurred. The abnormal event and associated accident sequences were defined in Step 7.10. An accident sequence consists of numerous cut sets. The analyst reviews these cut sets to define the specific failures. This information is then used to determine the time that annunciation (or other compelling signal) of the abnormal event (this time is referred to as T_o) occurs. Table 7.3-2 was developed to document this procedure, items 1 through 4 are described in the following paragraphs.

1. **Cut Sets.** The cut set(s) under investigation is listed. Cut sets that result in identical accident conditions and lead to identical procedures can be grouped together.

2. **Event/ Occurrence.** A description of what is occurring at the nuclear power plant due to the cut sets (item 1) being investigated are listed here.

3. **Time. (T_o)** The time from the occurrence of the abnormal event (i.e., initiator) to the occurrence of the event (item 2) is documented here.

4. **Annunciator/ Indication.** There are several questions asked. Is there an indicator that announces a change of state has occurred? Is it alarmed? What events (item 2) are annunciated?

Step 7.12. Identify Potential Recovery Actions

The analyst identifies the actions required to successfully cope with the abnormal event, once a correct diagnosis has been made. Table 7.3-3 has been developed to document this procedure. Items 1 through 6, which make up Table 7.3-3, are described in the following paragraphs:

1. **Description of Event.** A general description of the cut sets and the types of failures occurring are placed here.

2. **Symptoms.** The system failures or the symptoms occurring due to the cut set under investigation are documented here.

3. **Abnormal Event.** The number of abnormal events, i.e., events that disrupt the normal conditions in a plant, are listed. An event is defined to be more than one abnormal event when the operator must use a different procedure from the one previously used. For each procedure change the operator makes, the number of abnormal events is increased by one. If there is an additional abnormal event which occurs later in time (i.e., 15-20 minutes after the first event) it can be judged that the control room personnel are no longer actively engaged in diagnosing and/or planning the responses to cope with the first event. Therefore, the additional abnormal event is considered to be a first abnormal event.

4. **Possible Recovery Actions.** Possible recovery actions an operator can take (whether or not there is a procedure) are identified and documented here. A recovery action is an action taken to cope with some abnormal event.

5. **Activities Required to Perform the Action and Proceduralized.** The activities that an operator must perform to accomplish the recovery action (item 4) are described. If there is a procedure for the recovery action, it is noted. Only major performance type activities (e.g., open trip and throttle valve, start high pressure service water (HPSW) pumps) are analyzed.

   Decision/indication type activities (e.g., "Is the water level decreasing?") that are in the procedures are not analyzed in terms of obtaining a failure probability. It is generally assumed that the operator successfully performs the decision/indication type activities. However, if these decision/ indication type activities have an answer to the question that involves conflicting signals (e.g., "Is the water level decreasing?" has an answer of yes from one signal and no from another) while performing a task away from the normal location or some other unusual situation, it could be considered a major activity.

6. **Comments/ Source of Information.** Any comments or information that will provide clarification or aide in keeping track of the other items in this table are documented here. If any of the activities are skill-based or rule-based, they are identified and documented as such. Section 7.3 defines rule-based and skill-based behavior.

Step 7.13. Determine Available Operator Time

The maximum amount of time, T_m, to correctly diagnose an abnormal event and to complete the necessary human actions following the annunciation (or other compelling signal) of an abnormal event (T_o, see Step 7.11) is determined. This requires determining the amount of time available to the operator for the performance of necessary actions in order to prevent core damage (T_{cd}). The maximum time, T_m, is the difference between T_{cd} and T_o. Table 7.3-4, consisting of items 1 through 5, has been developed to document this procedure, a description follows.

If the potential recovery actions identified in Step 7.12 are recovery of electrical faults or Power Conversion System (PCS) faults, Steps 7.14 through Step 7.20 do not apply, skip to Step 7.21.

1. **Action.** The possible recovery actions are listed.

2. **Time by which Operator Must Act to Prevent Subsequent Core Damage (T_{cd}).** The maximum amount of time available during which, if the necessary human actions are completed, subsequent core damage is prevented based on thermal hydraulic analysis.

3. **Time at which Operator is Alerted that Symptom has Occurred (T_o).** The time from the occurrence of an abnormal event to the annunciation of the event, i.e., when the operator is alerted that the failure (or symptom) has occurred. This is identical to Item 3, Table 7.3-2.

4. **Maximum Time Available to Perform the Identified Operator Activities (T_m).** T_m = T_{cd} (item 2) - T_o (item 3).

Step 7.14. Determine Operator Performance Time

The time it takes the operator to perform the activities required for each recovery action is determined (this time is referred to as T_a). T_a is a combination of the estimated time needed to get to a particular location (T_ℓ) and the time needed to perform required actions once a diagnosis of an initiating event has been made (T_p).

There are several techniques used in establishing appropriate estimates of T_ℓ and T_p. For post-diagnosis actions to be performed in the control room area, attempt to measure travel time and manipulation time on the training simulator or by means of a timed walk-through in the plant control room. To the extent that such measurements are not possible, employ the following rules:

1. If there is a requirement to use written procedures, i.e., the human actions to be performed can not be assumed to be committed to memory, assess a five-minute delay, after correct diagnosis, before the first of the required post-diagnosis actions will be initiated.

2. Assess one minute as the required travel and manipulation time combined for each control room (CR) control action taken on the primary operating panels which are normally in visual access of the CR operator. An example is activation of the manual trip button.

3. For required control actions on other than the primary CR operating panels, assess two minutes as the required travel and manipulation time for each such control action.

4. Consider the effects of planned assignments of personnel to monitor particular panels for specified abnormal events.

5. If estimates of time are obtained from operating personnel, double them.

For travel and manipulation times outside the control room, use simulated measures (e.g., walk-throughs) to estimate the time required to get to the appropriate location and to perform the necessary post-diagnosis actions. If estimates from operating personnel must be used, double them.

Table 7.3-5 has been developed to document this procedure. A description of the items on the table follows.

1. **Action.** The possible recovery actions are listed here. This is identical to Table 7.3-2, item 1.

2. **Activities.** The activities an operator must perform to accomplish the recovery action (item 1) are listed.

3. **Location.** The physical location to which the operator must travel in order to perform the activities listed in item 2 is described here.

4. **Travel Time (T_ℓ).** The estimated time it takes the operator to travel to the location described in item 3 is placed here. It is assumed that the operator knows where the location is and goes directly there.

5. **Performance Time (T_p).** The estimated time it takes the operator to perform the activities listed in item 2 is placed here. It is assumed that the operator knows how to perform the activity. If there is any complexity or difficulty involved in performing the activity, it should be factored into the time.

6. **Total Time (T_a).** $T_a = T_\ell$ (item 4) + T_p (item 5). If there are numerous activities involved, T_a is calculated for each activity. These T_a values are then summed to yield a total T_a value for the recovery action.

Step 7.15. Determine Diagnosis Time

The estimated time available to the operator for a correct diagnosis which will still permit sufficient time to perform required post-diagnosis actions within the total allowable time, T_m, is calculated. The procedure is documented in Table 7.3-6. A description of the items in the table follows:

1. **Sequence/ Cut Set.** The sequence or cut set under investigation is listed. This is identical to item 1, Table 7.3-2.

2. **Symptom.** The symptoms or system failures, occurring due to the cut set under investigation, that require diagnosis by the operator are listed.

3. **Maximum Time Available (T_m).** The maximum time available to correctly diagnose the abnormal event and complete the necessary human actions following annunciation of an abnormal event is calculated in Table 7.3-4, the item 4 value is recorded here.

4. **Total Action Time (T_a).** The estimated time it takes the operator to perform the activities required for each recovery action is calculated in Table 7.3-5, the item 6 value is recorded here.

5. **Time Available to Diagnose (T_d).** The allowable time for a diagnosis which permits the performance of the required actions within the total allowable time is calculated. $T_d = T_m$ (item 3) - T_a (item 4).

Step 7.16. Determine Diagnosis HEP for Single Abnormal Event

The nominal diagnosis human error probability, HEP_{sd}, is the probability of misdiagnosis given a single abnormal event occurs. This diagnosis HEP is a joint HEP representing the performance of the entire control room crew. Diagnosis HEPs assume that any novice operator (i.e., one with less than six months' experience) would be replaced by a more experienced one. To make it easier to describe the procedure used in the determination of HEP_{sd} Table 7.3-7, which was developed to document the procedure, is used to describe the procedure as well as the documentation. Six items make up the table.

1. **Action (Symptom).** The symptoms from Table 7.3-6, item 2 assessed to be one abnormal event (see Step 7.12, item 3) are listed here.

2. **Diagnosis Negligible.** If the probability of the operator failing to diagnose the event is negligible, it is so stated here and the remainder of the table is not applicable. Reasons for considering the diagnosis errors negligible are discussed in the comment column, item 6.

   An assessment of a negligible probability of a diagnosis error can be made if it can be determined that all control room operators are trained to quickly initiate a manual scram signal with the SCRAM switches when the annunciation of an automatic scram has occurred, or when an immediate indication of a failure to scram has occurred, given that the operator must commit the procedure to memory.

   In some cases, especially during the first 30 minutes into the abnormal event, task analysis information may indicate that the diagnosis HEPs, even the lower uncertainty bounds, are unduly conservative. The analyst may judge that the diagnosis aspect of some particular event is negligible because of an established combination of training and procedures.

3. **Failure to Diagnose.** Using the diagnosis time value, T_d, calculated in Step 7.15 (item 5), the appropriate HEP is selected from Figure 7.3-2. Figure 7.3-2 contains nominal (median), upper bound and lower bound values for misdiagnosis. The

diagnosis HEP is adjusted upwards or downwards based on the following rules.

Use the upper bound if:

- the event is not covered in training, or
- the event is covered but not practiced except in the initial training of operators for becoming licensed, or
- the talk-through and discussions indicate that not all the operators know the pattern of stimuli associated with the event.

Use the lower bound if:

- The event is a well-recognized classic type and the operators have practiced the event in the simulator requalification exercises, and
- the talk-throughs and discussions indicate that all the operators have a good recognition of the relevant stimulus patterns and know what to do or which written procedures to follow.

Use the nominal (median) HEP if:

- the only practice of the event is in simulator requantification exercises and all operators have had this experience, or
- none of the rules for use of the upper or lower bound apply.

4. **Skill-Based.** If the behavior of the operator in response to the abnormal event is skill-based, it is stated here. A description of skill-based, knowledge-based and rule-based behavior can be found in Section 7.3.

5. **Adjustment in Final HEP.** If symptom-oriented EOPs are available and if the criteria itemized below are met, adjust the diagnosis HEP downwards by using HEPs from the lower bound of the nominal diagnosis curve (Figure 7.3-2) as the new set of nominal HEPs.

   - The initiating event in question is covered in these EOPs.

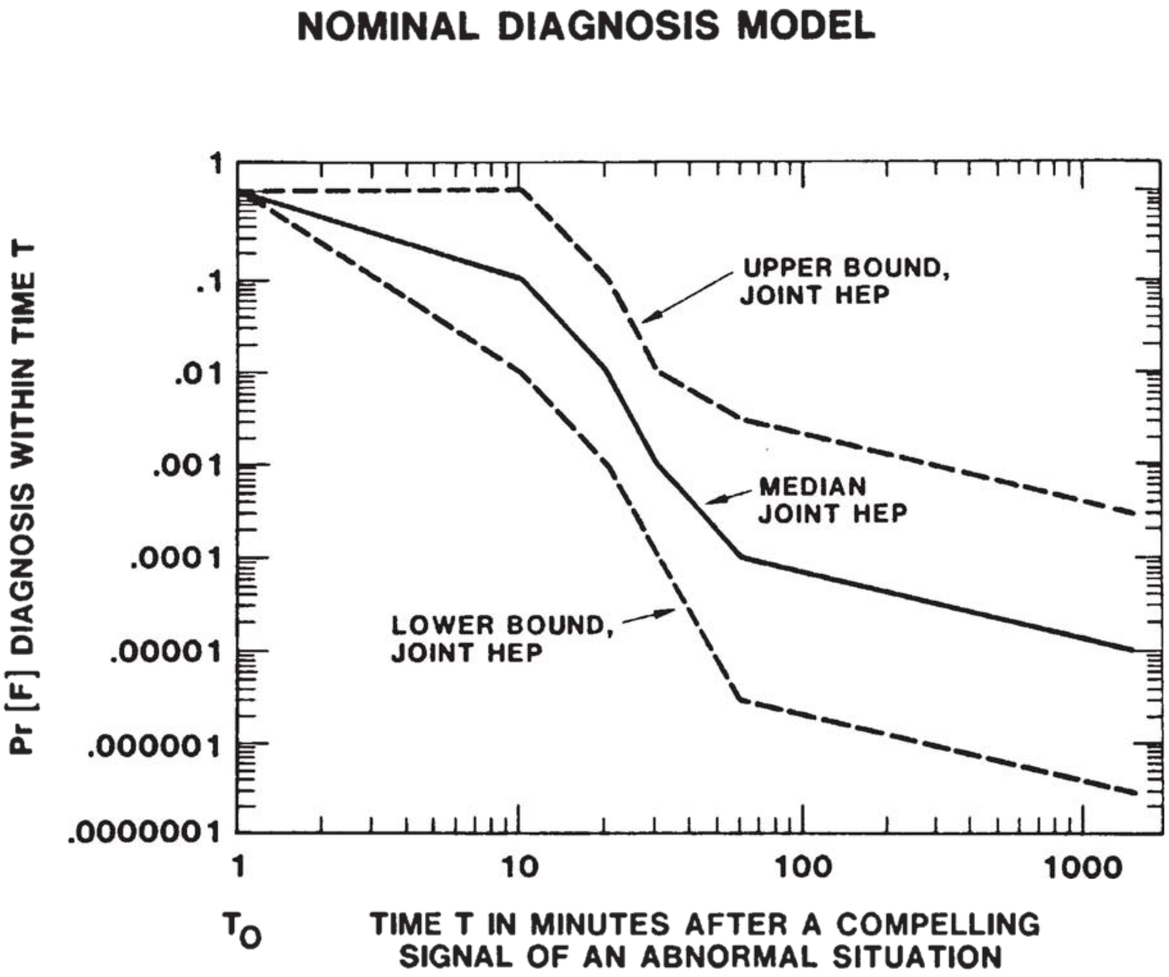


Figure 7.3-2. Nominal Model of Estimated Diagnosis HEPs for a Single Abnormal Event

(Revised version of Figure 12-4 from NUREG/CR-1278.[36] Extracted from ASEP HRA Procedure.[35])

- The appropriate control room operators have been trained in the use of symptom-oriented EOPs.

- Credit for symptom-oriented EOPs is to be given only for the percentage of operators estimated to actually use these EOPs rather than trust to their memory. If there is no other basis to use to estimate this percentage, assess a 0.5 probability that the appropriate operator will use the symptom-oriented EOPs in a step-by-step manner, rather than depend on his memory. For the fraction of operators assessed as depending on memory, give no credit for symptom-oriented EOPs.

- The EOPs are well designed. There are no gaps, inconsistencies, potentially misleading or confusing statements or paths, or requirements to follow more than one path simultaneously without prompts from one path to another.

For the diagnosis HEP for reactor vessel/ containment critical parameters which operating personnel must commit to memory, use the lower bound values in Figure 7.3-2 if the recognition of these parameters can be classified as skill-based behavior (see item 4).

The error factor associated with the final HEP_{sd} value is the largest of the error factors used in the determination of HEP_{sd}. This is considered to be a reasonably conservative estimate. If a technique for calculating the error factor is desired, see NUREG/CR-1278.[36]

6. **Comments/ Source of Information.** Any comments or information that will provide clarification or aide in keeping track of the other items in this table are documented here.

Step 7.17. Determine Diagnosis HEP for Multiple Abnormal Events

The nominal diagnosis human error probability, HEP_d, is the probability of misdiagnosis resulting in a core damage accident given multiple abnormal events occur. This diagnosis HEP is a joint HEP representing the performance of the entire control room crew. Diagnosis HEPs assume that any novice operator (i.e., one with less than six months' experience) would be replaced by a more experienced one. The HEP_d consists of a summation of two probabilities; the annunciator HEP and the failure to diagnose HEP. The annunciator HEP, HEP_{ann}, is the probability that the signal of second and subsequent abnormal events will indeed be noticed. The failure to diagnose HEP, HEP_{d-ann}, is the probability of a misdiagnosis for the second or subsequent simultaneously occurring abnormal events. To make it easier to describe the procedure used in the determination of HEP_d Table 7.3-8, which was developed to document the procedure, is used to describe the procedure as well as the documentation. Eight items make up the table.

1. **Action (Symptom).** The symptoms from Table 7.3-6, item 2 assessed to be more than one abnormal event (see Step 7.12, item 3) are listed.

2. **Diagnosis Negligible.** If the probability of the operator failing to diagnose the event is negligible, it is so stated here and the remainder of the table is not applicable. Reasons for considering the diagnosis errors negligible are discussed in the comment column, item 8.

   An assessment of a negligible probability of a diagnosis error can be made if it can be determined that all control room operators are trained to quickly initiate a manual scram signal with the SCRAM switches when the annunciation of an automatic scram has occurred, or when an immediate indication of a failure to scram has occurred, given that the operator must commit the procedure to memory.

   In some cases, especially during the first 30 minutes into an abnormal event, task analysis information may indicate that the diagnosis HEPs, even the lower uncertainty bounds, are unduly conservative. The analyst may judge that the diagnosis aspect of some particular event is negligible because of the combination of training and procedures.

3. **Number of Abnormal Event.** The number of abnormal events, i.e., events that disrupt the normal conditions in a plant, are listed here. This value was documented in Table 7.3-3, item 3.

4. **Annunciator HEP (HEP_{ann}).** The Annunciator Response Model (Table 7.3-12, page 7-49) is used to estimate the probability that the signal of second and subsequent abnormal events will indeed be noticed (HEP_{ann}). The total number of annunciators that alarm at the time of the second and subsequent abnormal events in an accident sequence is determined. Once this is done, Table 7.3-12 can be used to get the HEP_{ann} value. This value is documented here.

5. **Failure to Diagnose ($HEP_{d\text{-}ann}$).** When the operator is in a situation with more than one abnormal event occurring closely in time (i.e., within ten minutes) Table 7.3-13 is used to estimate the diagnosis HEP for the second or subsequent simultaneously occurring abnormal event ($HEP_{d\text{-}ann}$). The time available for diagnosis, T_d, is retrieved from Table 7.3-6, item 5 and used with Table 7.3-13 (page 7-50) to get the $HEP_{d\text{-}ann}$ values. The diagnosis HEP is adjusted upwards (upper bound) or downwards (lower bound) using the error factor depending on the following rules.

   Use the upper bound if:

   - the event is not covered in training, or

   - the event is covered by not practiced except in the initial training of operators for becoming licensed, or

   - the talk-through and discussions show that not all the operators know the pattern of stimuli associated with the event.

   Use the lower bound if:

   - the event is a well-recognized classic type and the operators have practiced the event in the simulator requalification exercises, and

   - the talk-throughs and discussions indicate that all the operators have a good recognition of the relevant stimulus patterns and know what to do or what written procedures to follow.

   Use the nominal HEP if:

   - the only practice of the event is in simulator requantification exercises and all operators have had this experience, or

   - none of the rules for use of upper or lower bound apply.

6. **Skill-Based.** If the behavior of the operator in response to the abnormal event is skill-based, it is so stated here. A description of skill-based, knowledge-based and rule-based behavior can be found in Section 7.3.

7. **Adjustment in Final HEP (HEP_d).** The failure to diagnose HEP, HEP_{d-ann}, can be adjusted for reactor/containment critical parameters which operating personnel must commit to memory. The lower bound values in Table 7.3-13 are used if recognition of these parameters can be classified as skill-based behavior, see item 6.

The total HEP for the operator misdiagnosing multiple events, HEP_d, is the summation of HEP_{ann} (item 4) and the final adjusted value for HEP_{d-ann}. $HEP_d - HEP_{ann} + HEP_{d-ann}$. The HEP_d value is documented here.

The error factor associated with the final HEP_d value is the largest of the error factors used in the determination of HEP_d. This is considered to be a reasonably conservative estimate. If a technique for calculating the error factor is desired, see NUREG/CR-1278.

Step 7.18. Determine Type of Task

This section begins the determination of the post-diagnosis tasks. Recall from Section 7.3, post-diagnosis tasks are those actions taken which logically follow a correct diagnosis of the abnormal event. The activities of the task are classified as step-by-step or dynamic. A step-by-step task is a routine, procedurally guided set of steps performed one step at a time without a requirement to divide the operator's attention between the task in question and other tasks. With high levels of skill and practice, a step-by-step task may be performed reliably without recourse to written procedures. A dynamic task is one that requires a higher degree of interaction between the people and the equipment in a system than is required by routine, procedurally guided tasks. Dynamic tasks may include decision making (i.e., choosing among alternative diagnosis and choosing which actions to carry out after a diagnosis has been made), keeping track of several functions, controlling several functions, or any combination of these. In assessing whether a task is step-by-step or dynamic, the analyst should also determine whether operator behavior is rule-based or skill-based.

Skill-based behavior consists of the performance of more or less subconscious routines based on stored patterns of behavior. It does not directly depend on the complexity of the task, but rather on the level of training and the degree of practice in performing the task. While different factors may influence the specific behavior of a particular individual, a group of highly trained operators would be expected to perform skill-based tasks expeditiously or even mechanistically with a minimum of mistakes. Rule-based behavior is used to denote behavior that requires a more conscious effort (than is the case for skill-based behavior) in following memorized (or written) rules. If these rules are not well practiced, they must be consciously recalled or checked. This leads to mistakes and less timely responses. The operator may not recall the procedure correctly, may be unwilling to check each step in a procedure or may not perform the steps in the proper sequences, all of which increase the potential for error.

Table 7.3-9 has been developed to document the determination of the type of task the operator is performing. Items 1 through 5, which make up Table 7.3-9, are described in the following paragraphs.

1. **Action.** The possible recovery actions are listed. This is identical to Table 7.3-4, item 1.

2. **Safety Systems Failed.** Any safety systems that were functioning initially and subsequently fail are included here.

3. **EOPs, Training, Use EOPs, Well-Designed EOPs.** If symptom-oriented EOPs are available and if the criteria itemized below are not met, indicate so here.

   - The initiating event in question is covered in these EOPs.

   - The appropriate control room operators have been trained in the use of symptom-oriented EOPs.

   - The operators actually use the EOPs rather than trust to their memory.

   - The EOPs are well designed. There are no gaps, inconsistencies, potentially misleading or confusing statements or paths, or requirements to follow more than one path simultaneously without prompts from one path to another in the EOPs.

4. **Operator Performs ≥ One Activity.** If an operator performs more than one activity involving more than one function without good indications for when a shift must be made from one activity to another, indicate so here.

5. **Dynamic or Step-by-Step.** The activity is classified as dynamic if; some safety system fails (see item 2) after the operating crew is using the EOP, the criteria itemized in item 3 are not met, or if the condition described in item 4 is met. Otherwise, the activity is classified as step-by-step.

Step 7.19. Determine Operator Stress Level

The post-diagnosis tasks are assessed as being performed under moderately high stress or extremely high stress. Disruptive stress is the tension resulting from the response to a stressor (i.e., any external or internal force that causes bodily or mental tension) that threatens, frightens, worries or angers a person or increases that person's uncertainty, so that tasks are performed at a decreased level of effectiveness or efficiency. Moderately high stress is a level of disruptive stress that will result in a moderate deteriorization in performance effectiveness of system-oriented behavior for most people. The onset of an abnormal event indicated by annunciators or other compelling signals is usually classified as resulting in at least a moderately high stress level. Extremely high stress is a level of disruptive stress in which the performance of most people will deteriorate drastically. This is likely to occur when the onset of the stressor is sudden and the stressing situation persists for long periods. This level of high stress is associated with the feeling of threat to one's physical well-being or to one's self-esteem or professional status. Extremely high stress levels can be avoided by considerable practice on potential abnormal events so that the response tasks can be classified as rule-based or skill-based actions.

Table 7.3-10 has been developed to document the determination the stress level of the operator performing the task. Items 1 through 6, which make up Table 7.3-10, are described in the following paragraphs.

1. **Action.** The possible recovery actions are listed here. This is identical to Table 7.3-4, item 1.

2. **T_m < 2h After IE.** If the time available to diagnose and perform the activities (see Table 7.3-6, item 3, T_m) is less than two hours, indicate so here.

3. **Recirculation Phase in a Large LOCA** If a large loss-of-coolant accident (LOCA) is occurring, indicate so here.

4. **More than Two Safety Systems Fail.** If more than two primary safety systems fail to function, indicate so here.

5. **Operator Familiar W/Sequence.** If it can be determined that frequent simulator training has made control room personnel very familiar with the accident sequence under investigation, indicate so here.

6. **Stress Level.** Extremely high stress is assessed for the operator if; the maximum time available is less than two hours (see item 2), a large LOCA is occurring (see item 3), or if more than two primary safety systems fail (see item 4).

For a large loss-of-coolant accident, moderately high stress is assessed when recirculation is established.

If control room personnel are familiar with the accident sequence (see item 5), moderately high stress is assessed.

If time stress is present, i.e., an operator is required to take some corrective action in moderately to extremely high stress conditions with very limited time available to take the corrective action, the doubling rule is employed. If the first action performed by the operator is ineffective, the HEP for each succeeding corrective action doubles (up to the limit of 1.0). The doubling rule applies to repeated attempts to perform the same task as well as to related tasks done by the same person.

For any situation not described, moderately high stress is assessed. A more extensive explanation of levels of stress and their effects on performance can be found in Chapter 17 of NUREG/CR-1278.

Step 7.20. Calculate the Total Failure Probability

The estimated total failure probability, F_T, is the probability of failing to perform the post-diagnosis task under investigation. It is the summation of the diagnosis HEP and the HEP for carrying out the required post-diagnosis action. Recall that the diagnosis HEP is the HEP for the operator misdiagnosing multiple events, Table 7.3-8, item 7 or the HEP for the operator misdiagnosing a single abnormal event, Table 7.3-7, item 5. The required post-diagnosis action HEP and the total failure probability are determined in this section.

A human error probability of 1.0 is assessed for F_T when no written procedures are immediately available for a critical skill-based or rule-based action. This assessment is used even though it may be required for personnel to have memorized these actions. In this situation, it is likely that the written procedures are referred to at a later time during the usual checking to see that all immediate emergency actions had been performed correctly.

Task analysis is an analytical process for determining the specific behaviors required of the human components in a man-machine system (for more information, see Chapter 4 of NUREG/CR-1278). If sufficient information can be obtained by means of a task analysis, use the data tables in Chapter 20 of NUREG/CR-1278, and error recovery factors per the search scheme presented in Chapter 20, to determine the post-diagnosis action HEP. These tables have been adjusted for the effects of dependence, stress, and other performance shaping factors (PSFs, any factor that influences human behavior). If the level of information required for this analysis is unavailable because of scheduling or other restrictions, use the technique described in the items of Table 7.3-11.

Table 7.3-11 has been developed to document the total failure probability and post-diagnosis action HEP. Items 1 through 6 are described in the following paragraphs.

1. **Action.** The possible recovery actions are listed here. This is identical to Table 7.3-4, item 1.

2. **Activities.** The activities an operator must perform to accomplish the recovery action, item 1, are listed here.

3. **Original Operator HEP (HEP_{op}).** The failure probability of the original operator to correctly perform a critical post-diagnosis procedural action (HEP_{op}) is documented here. The HEP_{op} is based on whether the activity is step-by-step, dynamic (refer to Table 7.3-9, item 5), moderately high stress or extremely high stress (refer to Table 7.3-10, item 6). Table 7.3-14 (page 7-51) is used in conjunction with the data retrieved from Table 7.3-9 and 7.3-10.

4. **Supervisor Fails to Correct Operator HEP (HEP_{r2}).** The failure probability for a second person failing to correct the original operator if recovery of the activity is possible (HEP_{r2}) is documented here. The HEP_{r2} is based on whether the activity is step-by-step, dynamic (refer to Table 7.3-9, item 5), moderately high stress or extremely high stress (refer to Table 7.3-10, item 6). Table 7.3-14 is used in conjunction with the data retrieved from Table 7.3-9 and 7.3-10.

5. **Third Independent Check/ Correction HEP (HEP_{r3}).** The failure probability for a third independent check to correct the error made by the original operator and second person (HEP_{r3}) is documented here. The HEP_{r3} is based on whether the activity is step-by-step, dynamic (refer to Table 7.3-9, item 5), moderately high stress or extremely high stress (refer to Table 7.3-10, item 6). Table 7.3-14 is used in conjunction with the data retrieved from Table 7.3-9 and 7.3-10.

6. **Total HEP.** The HEP_{op} value, item 3, is multiplied with the HEP_{r2}, item 4, and HEP_{r3}, item 5, values to yield a human error probability for each activity. ($HEP_{op}*HEP_{r2}*HEP_{r3} = HEP_{act}$). The HEP values for each activity are added for each task ($\Sigma(HEP_{act}) = HEP_{task}$). This yields a human error probability for the task under investigation.

   The estimated total failure probability, F_T, is calculated by adding the HEP_{task} value to the HEP_d value from Table 7.3-8, item 7 or to the HEP_{sd} value from Table 7.3-7, item 5, depending on whether there are multiple events or a single abnormal event occurring in the task. The error factor used is based on the error factors of the $HEP_{task,}$ HEP_d and HEP_{sd} values and engineering judgment. The EF should represent the range of values for F_T.

Step 7.21. Select Electrical Recovery Action Values

Some of the potential recovery actions identified in Step 7.12 as recovery of electrical faults are evaluated by a different technique than that used for non-electrical faults. This difference is due to the availability of actual plant experience. If sufficient plant-specific experience and data are available, a more accurate presentation of the plant is possible.

Table 8.2-8 contains a variety of AC and DC electric power failure rates collected from a variety of sources. Table 8.2-10 contains operator action failure rates for hardware, test and maintenance, actuation and common mode failures of diesel generators (DGs), and hardware and common mode failures of DC power. The Station Blackout Study[27] is the source used for all of these values except for the DG actuation, which was based on engineering judgment. The plant-specific timing, T_m, is used to determine the appropriate non-recovery probability value. Recall that T_m is the maximum amount of time available to the operator to recover before core damage occurs. The T_m value was determined in Step 7.13 and documented in Table 7.3-4, item 4.

A loss of offsite power (LOSP) recovery curve is generated for every plant. A composite model for LOSP that is very general was developed in NUREG/CR-5032.[20] This model can be made site-specific by making adjustments for switchyard configuration and weather differences. A complete description of the model can be found in NUREG/CR-5032. Figure 7.3-3 is the LOSP curve generated using the composite model with site-specific adjustments for the Peach Bottom nuclear power plant. The horizontal axis is the time, in hours, available to recover power, T_m. Using the LOSP curve and T_m value the probability that it takes longer than T_m hours to restore offsite power, i.e., the probability of failing to restore power within T_m hours, is determined. Engineering judgment is used to determine whether a conservative estimate (upper bound, which

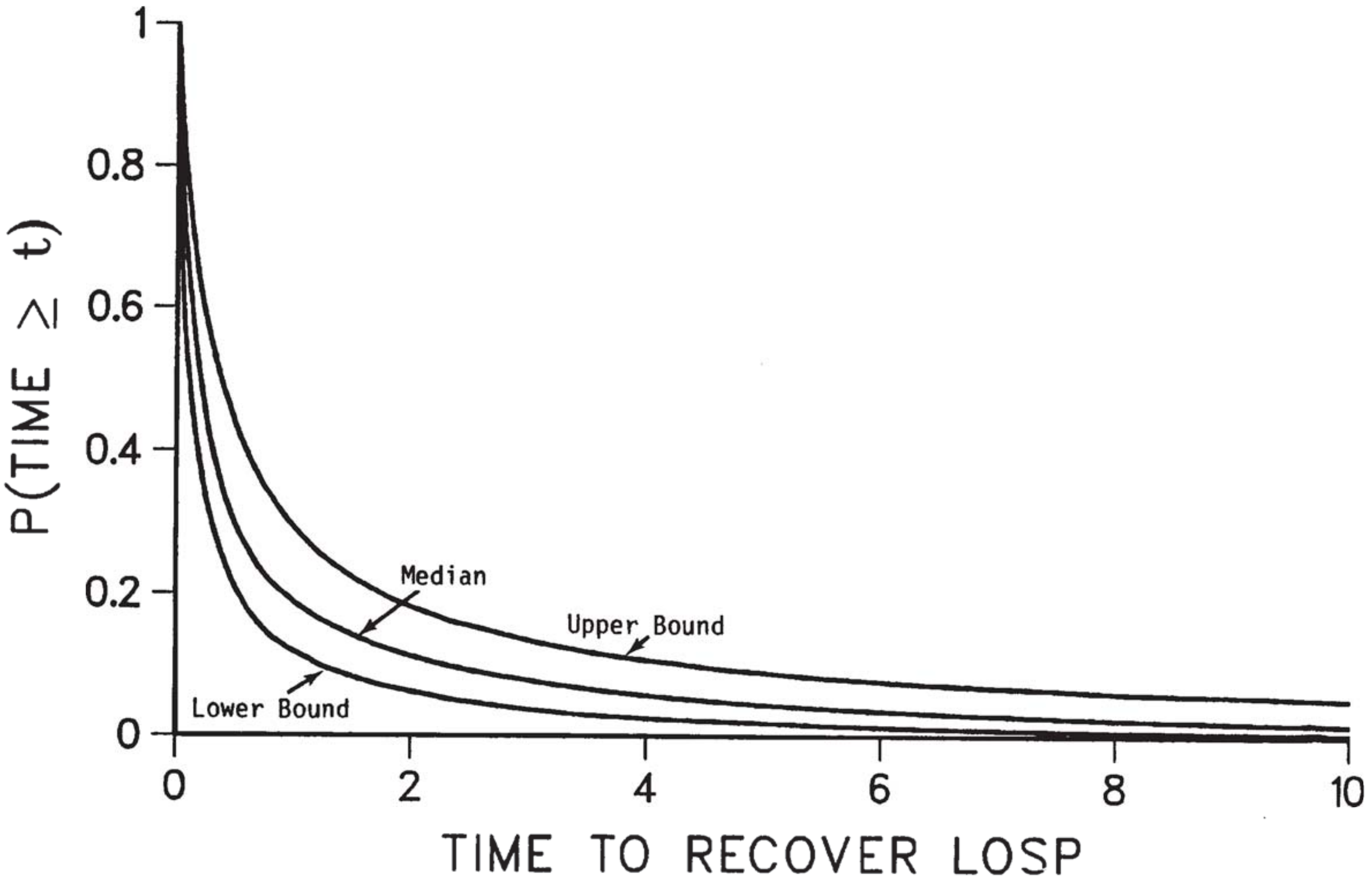


Figure 7.3-3. Loss of Offsite Power Recovery Curve for Peach Bottom

represents the .95 quantile) value is appropriate or whether the median or lower bound (the .05 quantile) values more accurately represent the cut set under investigation.

Step 7.22. Select Power Conversion System Recovery Action Values

The potential recovery actions for loss of the Power Conversion System (PCS) were identified in Step 7.12. Table 8.2-10 contains operator action failure rates for the PCS. These values are based on a cubic spline fit on the data for the PCS non-recovery values in NUREG-0666.[25] The plant-specific timing, T_m, is used to determine the appropriate probability value. Recall that T_m is the maximum amount of time available to the operator to perform the necessary recovery actions before core damage occurs. The T_m value was determined in Step 7.13 and documented in Table 7.3-4, item 4.

7.4 Human Reliability Recommended Reporting

The documentation of an HRA analysis should provide as much detail as is necessary to allow an individual not involved in the original analysis to trace and understand the justification for the derivation of the human error probabilities (HEPs). The scope of the analysis, i.e., the assumptions made and limitations imposed on the HRA methodology used, are documented. The format used to document the pre-accident and post-accident task analysis has been presented in Sections 7.2 and 7.3. The table format was developed for convenience, other formats may be developed that better suit an HRA analysis for a particular plant.

7.5 Example of Human Reliability Analysis

The following pre-accident and post-accident human reliability analysis examples have been taken from the Peach Bottom study.[4] The methodology used to quantify the pre-accident and post-accident task examples is described utilizing the step format and table documentation discussed in Sections 7.2 and 7.3.

7.5.1 Pre-Accident Human Reliability Example

The pre-accident HRA example is presented in Steps 7.1 through 7.7. Pre-accident failures include all human action errors prior to the start of the accident.

Step 7.1. Obtain Information for Pre-Accident Analysis

Information gathered in the Plant Familiarization Analysis task (Section 2) for the Peach Bottom front-line and support systems was reviewed for potential human errors. Errors of interest are found in routine and corrective maintenance activities, calibration, surveillance tests, and restoration (i.e., the returning of components and systems to their normal conditions following maintenance, calibration, or testing).

Procedures were reviewed to provide a thorough understanding of these tasks and to identify potential human errors which could result in equipment being inoperable when called upon.

Table 7.3-1
Accident Sequence Description

Event Tree (1):

Sequence Number (2):

Sequence Designator (3):

Sequence Description (4):

Accident Type (5):

Accident Conditions (6):

Applicable Procedures (7):

Table 7.3-2
Sequence and Cut Set Timing

Cut Sets (1):

Event/Occurrence (of most interest) (2)	Time (T_o) (3)	Annunciator/Indication (4)	Comments/ Source of Information

Table 7.3-3
Cut Set Failure and Potential Operator Action

Cut Sets: (See Table 7.3-2)

Description of Event (1)	Symptoms (2)	Abn. Event (3)	Possible Recovery Actions (4)	Activities (Tasks) Required to Perform Action and Proceduralized (5)	Comments/ Source of Information (6)

Table 7.3-4
Sequence and Cut Set Available Time

Cut Sets: (See Table 7.3-2)

Action (1)	Time by Which Operator Must Act To Prevent Subsequent Core Damage (Tcd) (2)	Time at Which Operator is Alerted that Symptom has Occurred (To) (3)	Maximum Time Available to Perform the Identified Operator Activities (Tm) (4)	Comments/ Source of Information (5)

Table 7.3-5
Operator Action Performance Time

<u>Cut Sets</u>: (See Table 7.3-2)

Action (1)	Activities (2)	Location (3)	Travel Time (T_l) (4)	Performance Time (T_p) (5)	Total Time (T_a) (6)	Comments/ Source of Information

Table 7.3-6
Diagnosis Time of Sequence and Cut Set

Sequence/Cut Set (1)	Symptom (2)	Maximum Time Available (Tm) (3)	Total Action Time (T_a) (4)	Time Available to Diagnosis (Td) (5)	Comments/ Source of Information

Table 7.3-7
Diagnosis Analysis--One Abnormal Event

Cut Sets: (See Table 7.3-2)

Action	Diagnosis	Failure to	Skill-Based	Adjustment	Comments/
(Symptom)	Negligible	Diagnose	(4)	in Final HEP	Source of Information
(1)	(2)	(Figure 7.3-2)		(HEP_{sd})	(6)
		(3)		(5)	

Table 7.3-8
Diagnosis Analysis--More than One Abnormal Event

Cut Sets: (See Table 7.3-2)

Action	Diagnosis	Number	Annunciator	Failure to	Skill-Based	Adjustment	Comments/
(Symptom)	Negligible	of Abn.	HEP	Diagnose	(6)	in Final HEP	Source of
(1)	(2)	Event	(Table 7.3-12)	(Table 7.3-13)		(HEP_d)	Information
		(3)	(HEP_{ann})	(HEP_{d-ann})		(7)	(8)
			(4)	(5)			

Table 7.3-9
Post-Diagnosis Action-Type Identification

<u>Cut Sets</u>: (See Table 7.3-2)

Action (1)	Safety Systems Failed (2)	EOPs, Training, Use EOPs Well-Designed EOPs (3)	Operator Performs ≥ One Activity (4)	Dynamic or Step-by-Step (5)	Comments/ Source of Information (6)

Table 7.3-10
Post-Diagnosis Stress-Level Identification

<u>Cut Sets</u>: (See Table 7.3-2)

Action (1)	T_m <2h After IE (2)	Recirc. Phase in Large LOCA (3)	More Than Two Safety Systems Fail (4)	Operator Familiar W/Sequence (5)	Stress Level (6)	Comments/ Source of Information (7)

Table 7.3-11
Post-Diagnosis Analysis

<u>Cut Sets</u>: (See Table 7.3-2)

Action (1)	Activities (2)	Original Operator HEP (HEP_{op}) (3)	Supervisor Fails to Correct Operator HEP (HEP_{r2}) (4)	Third Independent Check/Correction HEP (HEP_{r3}) (5)	Total HEP (6)	Comments/ Source of Information (7)

Table 7.3-12. The Annunciator Response Model: Estimated HEPs* for Multiple Annunciators Alarming Closely in Time**

(Table 20-23 from NUREG/CR-1278,[36] as revised September 1, 1985; edited version extracted from ASEP HRA Procedure.[35])

Number of ANNs	HEP_{ann}
	(k)
1	.0001
2	.0006
3	.001
4	.002
5	.003
6	.005
7	.009
8	.02
9	.03
10	.05
11-15	.10
16-20	.15
21-40	.20
>40	.25

* The HEPs are for the failure to initiate some kind of intended corrective action as required. The action carried out may be correct or incorrect and is analyzed using other tables. The HEPs include the effects of stress and should not be increased in consideration of stress effects.

An EF of 10 is assigned to each HEP. Based on computer simulation, use of an EF of 10 for the HEP yields approximately correct upper bounds for the 95th percentile. The corresponding lower bounds are too high; they are roughly equivalent to 20th-percentile rather than the usual 5th percentile bounds. Thus, use of an EF of 10 for the HEP values provides a conservative estimate since the lower bounds are biased high.

** "Closely in time" refers to cases in which two or more annunciators alarm within several seconds or within a time period such that the operator perceives them as a group of signals to which he must selectively respond.

Table 7.3-13. Nominal Model of Estimated HEPs and EFs for Diagnosis Within Time T by Control Room Personnel of Abnormal Events Annunciated Closely in Time.*

(Table 20-3 from NUREG/CR-1278[36] with appropriate changes to figure and table numbers; revised version extracted from ASEP HRA Procedure.[35])

T (Minutes** after T_o^+)	Median joint HEP_{d-ann} for diagnosis of a single or the first event	EF	T (Minutes** after T_o^+)	Median joint HEP_{d-ann} for diagnosis of the second event	EF	T Minutes** after T_o^+)	Median joint HEP_{d-ann} for diagnosis of the third event++	EF
1	1.0	--	1	1.0	--	1	1.0	--
10	.1	10	10	1.0	--	10	1.0	--
20	.01	10	20	.1	10	20	1.0	--
30	.001	10	30	.01	10	30	.1	10
			40	.001	10	40	.01	10
						50	.001	10
60	.0001	30	70	.0001	30			
1500	.00001	30				80	.001	30
			1510	.00001	30			
						1520	.00001	30

* "Closely in time" refers to cases in which the annunciation of the second abnormal event occurs while the control room personnel are still actively engaged in diagnosing and/or planning the responses to cope with the first event. This is situation-specific, but for the initial analysis, use "within 10 minutes" as a working definition of "closely in time."

Note that this model pertains to the control room crew rather than to one individual.

** For points between the times shown, use the medians and EFs from Figure 7.3-2 for the first event, and interpolate between the tabulated values for the second or third events.

+ T_o is a compelling signal of an abnormal situation and is usually taken as a pattern of annunciators. A probability of 1.0 is assumed for observing that there is some abnormal situation.

++ The HEP_{d-ann} for diagnosis of the third event has been judged sufficiently conservative to employ for any additional abnormal events assessed as occurring "closely in time." [ASEP HRA Procedure]

Table 7.3-14
Operator Performance HEPs*

	Step-by-Step Moderate Stress		Step-by-Step Extreme Stress		Dynamic Moderate Stress		Dynamic Extreme Stress	
Operator	HEP	EF	HEP	EF	HEP	EF	HEP	EF
HEP_{op}	0.02	5	0.05	5	0.05	5	0.25	5
HEP_r**	0.2	5	0.5	5	0.5	5	0.5	5

* The HEPs are for independent actions or independent sets of actions in which the actions making up the set can be judged to be completely dependent. Other levels of dependence among actions can be assessed by the analyst, using one or more methods for assessing dependence described in Chapter 10 of NUREG/CR-1278.

** If there are error recovery factors (RFs) in addition to those listed in this row, the influence of these RFs must be assessed separately. If a post-diagnosis immediate emergency action for the reactor vessel/containment critical parameters is performed, and (a) it can be judged to have been committed to memory, (b) it can be classified as a skill-based action, and (c) there is a backup written procedure, an HEP_r value of .001, EF of 10 is assessed. Assume no immediate RF from a second person for each such action.

This table is a revision of Table 8-5, ASEP HRA Procedure.[35]

Step 7.2. Identify Critical Man-Machine Interfaces

Each system for the Peach Bottom study was analyzed to identify components that might require maintenance while the plant is at power or that may have had maintenance while the plant was shut down. Manual valves were assumed to be maintained infrequently and were not considered. Sensors were analyzed for potential miscalibration errors. The sensors were grouped as to type and location; e.g., all condensate storage tank low level sensors were put in one group, and all high drywell pressure sensors were put in another group. Each group was treated as an entity.

For each component identified, the evaluation of the operator failure to perform the required task (e.g., restore a pump after maintenance) was considered. All activities (e.g., closing valves to isolate the component, pulling pump breakers, etc.) associated with performing each task were identified. Systems requiring realignment after testing were also identified.

Step 7.3. Identify Critical Systems

The information collected in Steps 7.1 and 7.2 is reevaluated and the critical systems, along with the associated tasks and activities that are to be quantified for the Peach Bottom analysis, were identified. Only those activities which could influence the ability to safety shut down the plant were considered.

There were six critical tasks identified for the Low Pressure Core Spray (LPCS or LCS) system; failure to restore motor-operated valve (MOV or MV) 11A after maintenance, failure to restore MOV 12A after maintenance, failure to restore pump train A (2AP37) after maintenance, failure to restore pump train B (2BP37) after maintenance, failure to restore pump train C (2CP37) after maintenance and failure to restore pump train D (2DP37) after maintenance.

This example follows the analysis and documentation of the failure to restore MOV 11A after maintenance task. The first three items documented on Tables 7.5-1, 7.5-2 and 7.5-3 (these were discussed in Section 7.2 as Tables 7.2-1, 7.2-2, and 7.2-3) are described in the following paragraphs.

1. Systems. The Low Pressure Core Spray system (LPCS or LCS) is the critical system under investigation.

2. Task. Failure to restore MOV 11A after maintenance is the task evaluated.

3. Activities. In order to place LPCS in its correct configuration, the operator must restore MOV 11A to its original position.

Step 7.4. Assign the Basic HEP

A basic HEP (BHEP) of 0.03 is assigned to the activity described in Step 7.3, item 3, restore MOV 11A to original position. This BHEP represents a combination of a generic HEP of 0.02 assessed for an EOM and a generic HEP of 0.01 assessed for an ECOM.

Step 7.5 Determine Dependence Effects

The BHEP of 0.03 must be modified for the effects of dependence. Table 7.5-1 documents the dependency between the activities for each task. The information collected to determine dependency effects is documented in items 4 through 9. The assignment of the dependencies is documented in item 10.

4. Multiple Components — The components the operator manipulates in order to restore MOV 11A to its original position are MOV 11A, MOV 12A, manual valve (XV) 63A, XV63C and MOV 26A (see Figure 5.5-2). MOV 12A, XV 63A, XV 63C and MOV 26A must be closed before maintenance can be performed on MOV 11A.

5. Series/ Parallel. — The activity is considered a series system since failure of the operator to properly restore any one of the components renders the entire LPCS system unavailable.

6. Time Reference. — The time necessary to restore MOV 11A to its original position and to restore the multiple components (item 4) requires more than two minutes. Therefore, the time reference is >2 minutes.

7. Location Reference. — MOV 11A, MOV 12A, MOV 26A, XV 63A and XV 63C are not within 4 feet of one another.

8. Written Requirements. — The operator is required to record some information pertaining to MOV 11A, MOV 12A, MOV 26A, XV 63A and XV 63C.

9. General Location. — The multiple components (item 4) are not in the same visual frame of reference, but there are record requirements (see item 8) for each component, therefore, this item is not applicable.

10. Dependence. — Zero Dependence (ZD) is assessed for both the EOMs and ECOMs since the activities on the different components are for components that constitute a series system (see item 5).

TABLE 7.5-1

LOW PRESSURE CORE SPRAY DEPENDENCE EFFECTS OF TEST AND MAINTENANCE ACTIVITIES

SYSTEMS (1)	TASK (2)	ACTIVITIES (3)	MULTIPLE COMPONENTS (4)	SERIES/ PARALLEL (5)	TIME REFERENCE (6)	LOCATION REFERENCE (7)	WRITTEN RQMNTS (8)	GEN LOC (9)	DEPENDENCE ECOM EOM (10)	COMMENTS (11)
LCS	(2) Failure to restore MOV11 (A or B) after maintenance		MV11A, MV12A, XV63A, XV63C, MV26A for MV11A (MV11B similar)	Series	> 2 min	Not Within 4 feet	Yes	NA	ZD	
		(3) Restore valve to original position								
LCS	(2) Failure to restore pump train after maintenance		MV7A, MDPA, MV5A, CV10A, XV63A for 2AP37 (2BP37, 2CP37, 2DP37 similar)	Series	> 2 min	NA	Yes	NA	ZD	
		(3) Restore valves and breaker to original position								

Step 7.6. Identify Recovery Factors

The recovery factors (RFs) are identified and documented in Table 7.5-2, items 4 through 7.

4. **Compelling Signals.** There are no compelling signals for any of the components. No signals are alarmed in the control room indicating incorrect instrumentation adjustments or component restorations before normal power operation can be resumed.

5. **Post-Maintenance/ Calibration Test.** It is possible to restore MOV 11A if a post-maintenance test is performed correctly.

6. **Written Verification.** For each component, there is a written checkoff list used during the check of the component by a second person verifying the status after the maintenance task.

7. **Written Daily/ Shiftly.** There is no shiftly or daily check on component status using a written checkoff list.

8. **Total RF Credit.** The Table of RFs (Table 7.2-4) is consulted to ascertain which set of basic and optimum conditions apply to the activity, restoring MOV 11A to its original position. Table 7.5-2 and Table 7.2-4 show that the applicable basic conditions are 1 and 4, the optimum conditions are 2 and 3.

   Table 7.2-5 is consulted to determine which of nine cases applies to the activity. Case VIII, no compelling signal feedback; PM or PC Test is effective if performed correctly; second person or other immediate RF is used, is the applicable case for the activity. The appropriate total failure probability (F_T) is; $F_T = 0.03 \times 0.01 \times 1.0 = 0.0003$ (EF ~10).

9. **EF.** The error factor value from Table 7.25 paired with $F_T = 0.0003$ (Case VIII) is 10.

Step 7.7. Determine the Nominal HEP (NHEP)

The information required to calculate the nominal human error probability (NHEP) is collected and documented as items 4 through 9 on Table 7.5-3.

4. **Comp (n).** The five components that make up the system and task under investigation are: MOV 11A, MOV 12A, XV 63A, XV 63C, and MOV 26A.

TABLE 7.5-2

LOW PRESSURE CORE SPRAY IDENTIFICATION OF RECOVERY FACTORS

			COMPELLING	POST-MAIN/	WRITTEN	WRITTEN	TOTAL RF		
SYSTEMS	TASK	ACTIVITIES	SIGNALS	CALIB. TEST	VERIFICATION	DAILY/SHIFTLY	CREDIT	EF	COMMENTS
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(11)
LCS	[See Table 7.5-1]	[See Table 7.5-1]	No	Yes	Yes	No	.03 x .01 x 1.0 = 0.0003	10	
LCS	[See Table 7.5-1]	[See Table 7.5-1]	No	Yes	Yes	No	.03 x .01x 1.0 = 0.0003	10	

TABLE 7.5-3

LOW PRESSURE CORE SPRAY POST-MAINTENANCE OR POST-CALIBRATION HEPs

						SERIES	PARALLEL						
						EOM/ECOM	ECOM	EOM					
			COMP			ZD	ZD	ZD	CD	HD			
SYSTEMS	TASK	ACTIVITIES	(n)	BHEP	RF	n(BHEP*RF)	$(ECOM*RF)^n$	$(EOM*RF)^n$	(EOM*RF)	$(EOM*RF)(.5)^{n-1}$	NHEP	EF	COMMENTS
(1)	(2)	(3)	(4)	(5)	(6)	<------------	------------	---(7)---	------------	------------>	(8)	(9)	(10)
LCS	[See Table 7.5-1]	[See Table 7.5-1]	5	0.03	0.01	0.0015					1.5E-3	10	Mean = 3.99E-3
LCS	[See Table 7.5-1]	[See Table 7.5-1]	4-6	0.03	0.01	0.0012 to 0.0018					1.5E-3 (Typical of range)	12	Mean = 4.70E-3

5. BHEP. A BHEP of 0.02 for each EOM and 0.01 for each ECOM have been assigned. A total BHEP of 0.03 is assigned for the critical activity.

6. RF. The RF credit, exclusive of the BHEP of 0.03 is 0.01 x 1.0 = 0.01 (see Table 7.5-2, item 8).

7. Series or Parallel. Table 7.5-1 documents the type of system, series or parallel (item 5) and the dependence effects (item 10). This information is necessary to determine the NHEP. The critical activity is a series system with zero dependence (ZD), therefore, NHEP - n (0.03 x RF), or NHEP - 5 (0.03 x 0.01) - 0.0015.

   As an alternative, NHEP values are summarized in Table 7.2-6; for case VIII, series system, ZD with five components, NHEP - 0.0015. Note that the NHEP is a median, not a mean value.

8. NHEP. The NHEP is equal to the EOM and ECOM values documented in item 7, 0.0015.

9. EF. Table 7.2-6 has an associated EF with each NHEP value, in this case the EF is 3.0. Engineering judgment was used to increase the EF to 10. This is a conservative estimate that was deemed to be more representative of the uncertainty in the task.

7.5.2 Post-Accident Human Reliability Example

The post-accident HRA example is presented in Steps 7.8 through 7.22. Post-accident human errors are those operator actions performed by the operator after the accident has started.

Step 7.8. Obtain Information for Post-Accident Analysis

Information gathered in the Plant Familiarization Analysis task (Section 2) was reviewed for potential human post-accident errors. Only those actions specifically addressed in the plant procedures were credited and evaluated. These included such actions as manually initiating a system, aligning and actuating a system for injection, and recovering a failed system.

Step 7.9. Identify Recovery Actions Included in Event Trees or Fault Trees

When developing the system models, any post-accident operator action required for the system to successfully function when demanded was identified and added directly to the system model. This process identifies the action or task (e.g., manually align CRD for full flow) but does not identify the individual activities required in order to accomplish the task.

By identifying human action errors in the system models, the potential for more than one human action event to appear in a cut set existed when linking the system models to form the accident sequence. This occurrence presents a problem when the actions are dependent. Only independent human actions can be multiplied together. Since the failures (which dictate the conditions under which the operator is working) are identified in the sequence cut sets, it is impossible to evaluate the human error probabilities for post-accident human errors at the system model level. Therefore, these actions were assigned a screening value, generally 0.5.

Step 7.10. Develop Accident Sequence Descriptions

One of the abnormal events identified in the Systems Analysis Task (Section 5) for the Peach Bottom Study was loss of long-term decay heat removal. The dominant accident sequences associated with this abnormal event were identified in Section 10. Table 7.5-4 is used to document the accident sequences and associated scenarios for the loss of long-term decay heat removal abnormal event. These sequences are labeled W sequences. A description of the documentation technique utilizing the seven items on the table follows.

1. Event Tree. Any W type sequence in the Peach Bottom event trees is quantified by the technique documented by Tables 7.5-4 through 7.5-14. (These were discussed in Section 7.3 as Tables 7.3-1 through 7.3-11.)

2. Sequence Number. The event trees contained numerous branches with the W sequences described in item 1, there are too many to list.

3. Sequence Designator. The acronym used for each sequence listed in item 2 includes AV2W1W3..., S2U1W1W3..., etc.

4. Sequence Description. The type of accident sequences under investigation are those where core cooling is being maintained but, because the Power Conversion System (PCS) is unavailable, core heat is dumped to containment. This results in a failure to remove heat from containment leading to temperature and pressure rises which may ultimately cause containment failure and the possible loss of core injection. The operator must put the RHR system into some mode of containment cooling or ultimately vent the containment should pressure get very high (~100 psig).

TABLE 7.5-4

W SEQUENCES ACCIDENT SEQUENCE DESCRIPTION

EVENT TREE(1): Any "W" type sequence (may be AWs, SWs, TWs-NON-ATWS)

SEQUENCE NUMBER(2): Numerous

SEQUENCE DESIGNATOR(3): Examples include: $A\overline{V2}W1W3...$, $AV2\overline{V3}W1W3...S1U1\overline{X1}V2V3\overline{V4}W1W3...$,
$S2\overline{U1}W1W3...$, $T1P_1U1\overline{U2}W1W3...$, $T2U1U2\overline{X1V1}W1W2W3...$

SEQUENCE DESCRIPTION(4):

Variety of types of sequences where core cooling is being maintained but because the Power Conversion System (PCS) is unavailable, core heat is dumped to containment. Failure to remove heat from containment causes temperature and pressure rises in containment which ultimately could cause containment failure leading to possible loss of core injection. The operator must put the RHR system into some mode of containment cooling or ultimately vent the containment should pressure get very high (~100 psig).

ACCIDENT TYPE(5):

Loss of long-term decay heat removal.

ACCIDENT CONDITIONS(6):

Variety of initiators
Reactor scram is successful
PCS not available
Containment control required if have a torus temperature >95°F or drywell pressure >2 psig or drywell temperature >145°F.

APPLICABLE PROCEDURES(7):

Procedures of interest for these human actions are: T-102-containment control, T-200-containment venting, T-100-Scram, T-99-Post-Scram.

5. Accident Type. The basic accident type is loss of long-term decay heat removal.

6. Accident Conditions. There are a variety of initiators which may have caused the accident (e.g., a large LOCA, event tree heading A, an intermediate LOCA, event tree heading S1, a small LOCA, event tree heading S2, loss of offsite power, event tree heading T1, and a transient without the PCS initially available, event tree heading T2). The reactor has been successfully scrammed. The Power Conversion System is not available. Containment control will be required if the torus temperature is greater than 95°F, the drywell pressure is greater than 2 psig, or the drywell temperature is greater than 145°F.

7. Applicable Procedures. The Accident Conditions described in the previous paragraph direct the operator to four procedures: T-102 - Containment Control, T-200 - Containment Venting, T-100 - Scram, and T-99 - Post-Scram.

Step 7.11. Determine Sequence and Cut Set Timing

The time at which the operator is aware that a loss of long-term decay heat removal has occurred is determined and documented in Table 7.5-5.

1. Cut Sets. The W accident sequences contain cut sets that result in similar events. Those of interest contain the event, ESF-XHE-FO-RHRAT (failure of the operator to align the RHR cooling mode), or a combination of two events, ESF-XHE-FO-RHRAT and PCV-XHE-FO-PCV (failure of the operator to vent).

2. Event/ Occurrence. There are four conditions that are eventually generated as a result of the W sequences; the suppression pool temperature exceeds 95°F, the drywell pressure exceeds 2 psig, the drywell temperature exceeds 145°F and the drywell/ wetwell pressure is approximately 100 psig. This example will address the first condition, the suppression pool temperature exceeding 95°F. The other conditions are described in the tables but will not be used in the example unless the first condition can not be used.

3. Time (T_o). The time from the occurrence of the initiator to the time that the suppression pool temperature exceeds 95°F is approximately less than 15 minutes, depending on what the initiator was.

TABLE 7.5-5

W SEQUENCES SEQUENCE AND CUT SET TIMING

CUT SETS(1):
(1) Ones of interest are: ...ESF-XHE-FO-RHRAT... or ...PCV-XHE-FO-PCV*ESF-XHE-FO-RHRAT...

EVENT/OCCURRENCE (of most interest) (2)	TIME (T_0) (3)	ANNUNCIATOR/INDICATION (4)	COMMENTS/ SOURCE OF INFORMATION
Suppression pool temperature >95°F	~<15 mins (depending on initiator)	All conditions indicated, alarms on 2 psig	Timing based on runs with LTAS [Reference 4 in Peach Bottom Report]
Drywell pressure >2 psig	~few to 30 mins (depending on initiator)		
Drywell temperature >145°F	~1-10 hrs (depending on initiator)		
Drywell/wetwell pressure ~100 psig (for venting) -Procedure T-200	~few to >24 hrs (depending on initiator) Intermediate indications along the way continue to remind the operator to establish some form of containment cooling		

4. Annunciator/ Indication. The suppression pool temperature is indicated in the control room when the temperature exceeds 95°F.

5. Comments/ Source of Information. The time from the occurrence of the initiator to the time that the suppression pool temperature exceeds 95°F is based on a thermal hydraulic analysis. The analysis was done using LTAS, a BWR code developed by Oak Ridge National Laboratory, which was modified for Peach Bottom

Step 7.12. Identify Potential Recovery Actions

The actions required to successfully cope with the loss of long-term decay heat removal event once a correct diagnosis has been made were determined and documented in Table 7.5-6.

1. Description of Event. The cut sets under investigation involve a failure of the operator to place the RHR/HPSW systems in a containment cooling mode and an additional failure of the operator to vent containment. This example will not describe the additional failure.

2. Symptoms. The resulting symptom or system failure for the cut sets under investigation is failure of containment cooling.

3. ABN Event. For normal-type shutdowns, RHR cooling is required as part of the T-100/T-99 procedure. If other than a normal-type shutdown occurs, the T-100/T-99 procedure is followed and subsequently leads to the T-102 procedure. For each procedure change an operator makes, the number of abnormal events is increased by one, therefore, this is a first (1) or second (2) abnormal event

4. Possible Recovery Actions. Recovery actions the operator could do are restore containment cooling or restore the PCS. Restoring PCS is considered an independent action; therefore, generic ASEP data is used for this action.

5. Activities Required to Perform Action and Procedur-alized. The activities the operator performs to recover the operator failure to place the RHR/HPSW system in the containment cooling mode event are; start the RHR/HPSW pumps, and align the systems for containment cooling.

TABLE 7.5-6

W SEQUENCES CUT SET FAILURE AND POTENTIAL OPERATOR ACTIONS*

CUT SETS: See Table 7.5-5

DESCRIPTION OF EVENT (1)	SYMPTOMS (2)	ABN EVENT (3)	POSSIBLE RECOVERY ACTIONS (4)	ACTIVITIES REQUIRED TO PERFORM ACTION AND PROCEDURALIZED (5)	COMMENTS/ SOURCE OF INFORMATION (6)
Operator fails to place RHR/HPSW in a containment cooling mode (may be SPC, SDC, CSS)	Containment cooling fails	1 or 2*	Restore containment cooling or restore PCS (considered an independent action)--will use ASEP data for this action	Start RHR/HPSW pumps. Line up for containment cooling and start cooling. (Proceduralized)	Some skill-based; generally rule-based.
Operator also fails to vent containment	Containment cooling fails	3*		Turn containment bypass switch in control room to bypass. Open 2" wetwell and drywell vent lines. If pressure continues to rise, open 6" ILRT line (proceduralized)	

*Normal-type shutdowns call for RHR cooling as part of T-100/T-99. Otherwise T-102 then used (second event) or T-200 (third event).

6. Comments/ Source of Information. Some of the activities identified in item 5 are skill-based, i.e., governed by memory, but generally they are rule-based, i.e., governed by rules.

Step 7.13. Determine Available Operator Time

The maximum amount of time available for the operator to correctly diagnose the loss of long-term decay heat removal event and to complete the necessary human actions following the annunciation of the event was determined and documented in Table 7.5-7.

1. Action. The operator must align the RHR cooling mode in order to recover from the ESF-XHE-FO-RHRAT event.

2. Time by Which Operator Must Act to Prevent Subsequent Core Damage (Tcd). The maximum amount of time available to the operator by which the RHR cooling mode must be aligned (i.e., the shortest time in which the operator has to act) is approximately two hours for a large LOCA initiator and approximately 30 hours for a transient initiator.

3. Time at Which Operator is Alerted that Symptom has Occurred (T_o). The time at which the operator is alerted to the four symptoms are: for the SRVs cycling, within a few minutes; for the pool temperature exceeding 95°F, within a few minutes; for the drywell pressure exceeding 2 psig, within a few to 30 minutes; and for the drywell temperature exceeding 145°F, within 1 to 10 hours.

4. Maximum Time Available to Perform the Identified Operator Activities (Tm). The operator has approximately two hours (for large loss of coolant accidents) from the time at which he has been alerted that the SRVs are cycling (if they cycle at all) to when the RHR system must be aligned in cooling mode; Tm = Tcd [item (2)] - To [item (3)] = 2 hrs - 2 mins ~2 hrs

Step 7.14. Determine Operator Performance Time

The time it takes the operator to perform the activities for each recovery action was determined and documented in Table 7.5-8.

1. Action. The operator must align the RHR cooling mode in order to recover from the ESF-XHE-FO-RHRAT event.

TABLE 7.5-7

W SEQUENCES SEQUENCE AND CUT SET AVAILABLE TIME

CUT SETS: See Table 7.5-5

ACTION (1)	TIME BY WHICH OPERATOR MUST ACT TO PREVENT SUBSEQUENT CORE DAMAGE (Tcd) (2)	TIME AT WHICH OPERATOR IS ALERTED THAT SYMPTOM HAS OCCURRED (To) (3)	MAXIMUM TIME AVAILABLE TO PERFORM THE IDENTIFIED OPERATOR ACTIVITIES (Tm) (4)	COMMENTS/ SOURCE OF INFORMATION (5)
The operator must align the RHR cooling mode in order to recover from the ESF-XHE-FO-RHRAT event	Shortest time is ~1-2 hrs for large LOCAs, will use: ~2 hrs (large LOCAs) ~>30 hrs (for transients)	SRVs cycling--few mins	~2 hrs for large LOCAs ~30 hrs for transients	
		Pool temperature >95°F--few mins	As above	
		Drywell pressure >2 psig--few to 30 mins	As above	
		Drywell temperature >145°F--~1-10 hrs	~1 hr for Large LOCA ~20 hrs for transients	
PCV-XHE-FO-PCV	~2 hrs for large LOCAs ~>30 hrs for transients	100 psig reached in containment--~2 to >30 hrs	Established at <1/2 hr for large LOCAs and ~1 hr or more for transients except if only low pressure cooling systems are operating (i.e., no CRD), will need to vent before 100 psig is reached or SRVs close and core damage is likely to occur before 100 psig is reached.	

TABLE 7.5-8

W SEQUENCES OPERATOR ACTION PERFORMANCE TIME

CUT SETS: See Table 7.5-5

ACTION (1)	ACTIVITIES (2)	LOCATION (3)	TRAVEL TIME (T_ℓ) (4)	PERFORMANCE TIME (T_p) (5)	TOTAL TIME (Ta) (6)	COMMENTS/ SOURCE OF INFORMATION
The operator must align the RHR cooling mode in order to recover from the ESF-XHE-FO-RHRAT event	See Table 7.5-6, Item (5)	Control Room	1 min	<10 mins	~10 mins	
PCV-XHE-FO-PCV	See Table 7.5-6	Control Room and local for ILRT (Integrated Leak Rate Test) line set up before 100 psig is reached.	~1 min	~15 mins	~15 mins	ILRT line is set up and opened before 100 psig is reached. When the time to vent is reached, all actions are in the control room.

2. Activities. The major activities to be analyzed are identical to those listed in Table 7.5-6, item 5.

3. Location. The operator performs the activities listed in item 5 of Table 7.5-6 in the control room. It is assumed that the operator knows the proper location.

4. Travel Time. (T_ℓ). The time it takes the operator to travel to the location of the activity is one minute.

5. Performance Time (T_p). The time it takes the operator to actually perform the activity is less than 10 minutes.

6. Total Time (Ta). The total time (Ta) is the sum of the travel time T_ℓ, item 4 and the performance time T_p, item 5, T_a = 1 min + < 10 min ~10 minutes.

Step 7.15. Determine Diagnosis Time

The estimated amount of time the operator has to correctly diagnose the loss of long-term decay heat removal event was determined and documented in Table 7.5-9.

1. Sequence/ Cut Set. The cut sets under investigation are those containing the event ESF-XHE-FO-RHRAT, see Step 7.11, Table 7.5-5, item 1.

2. Symptom. The resulting symptoms or system failures that need to be diagnosed are: Safety Relief Valves (SRVs) cycle, pool temperature >95°F, drywell pressure >2 psig and drywell temperature >145°F.

3. Maximum Time Available (Tm). The maximum time available to correctly diagnose the loss of long-term heat removal and to realign the RHR cooling mode was documented in Table 7.5-7, item 4. For the SRVs cycling, pool temperature or drywell pressure symptoms, there is approximately two hours given that a large LOCA is the initiating event and approximately 30 hours given a transient initiating event.

4. Total Action Time (Ta). The estimated time it takes the operator to start the RHR/HPSW pumps, line up for containment cooling and start cooling was documented in Table 7.5-8, item 6, approximately 10 minutes.

TABLE 7.5-9

W SEQUENCES DIAGNOSIS TIME OF SEQUENCE AND CUT SET

SEQUENCE/CUT SET (1)	SYMPTOM (2)	MAXIMUM TIME AVAILABLE (Tm) (3)	TOTAL ACTION TIME (Ta) (4)	TIME AVAILABLE TO DIAGNOSIS (Td) (5)	COMMENTS/ SOURCE OF INFORMATION
Cut Sets Containing ESF-XHE-FO-RHRAT	SRVs cycle	~2 hrs for large LOCAs ~30 hrs for transients	~10 mins	Nearly 2 hrs to ~30 hrs	
	Pool temp >95°F	As above		As above	
	Drywell pressure >2 psig	As above		As above	
	Drywell temp. >145°F	~1 hr for large LOCAs ~20 hrs for transients		~3/4 hr to ~20 hrs	
Cut Sets Containing PCV-XHE-FO-PCV		<30 mins for large LOCAs	~15 mins	~15 mins to 3/4 hr (except operator will actually be monitoring all along)	Need to act before 100 psig reached if SRVs reclose and CRD unavailable
		~1 hr for transients unless SRVs reclose and CRD unavailable-then must vent before 100 psig reached			

5. Time Available to Diagnosis (T_d). The allowable time available for a diagnosis is Tm [item (2)] - Ta [item (3)]
   - 2 hrs - 10 mins ~2 hrs (Large LOCA)
   - 30 hrs - 10 mins ~30 hrs (transients)

Step 7.16. Determine Diagnosis HEP for Single Abnormal Event

The nominal diagnosis human error probability, HEP_{sd}, was determined and documented in Table 7.5-10.

1. Action (Symptom). Since the symptom example, suppression pool temperature exceeding 95°F, is treated as a multiple abnormal event, not a single abnormal event, Step 7.16 is not applicable. The symptom, drywell temperature exceeding 145°F is used to illustrate this step since it is considered one abnormal event.

2. Diagnosis Negligible. Table 7.5-7, item 3, documents that the symptoms; SRVs cycling and the pool temperature >95°F alert the operator of their occurrence within a few minutes with the drywell temperature >145°F symptom occurring one to ten hours later. The probability of the operator failing to diagnose the loss of long-term decay heat removal event when the SRVs are cycling and/or if the pool temperature is >95°F is <3E-6 (see Table 7.5-11, Step 7.17). Since the probability associated with these symptoms is small and when combined with the probability associated with the drywell temperature >145°F symptom becomes even smaller, the diagnosis failure is negligible and the remainder of the table is not applicable.

   Because these three symptoms were coupled, Step 7.17 occurs before Step 7.16, for symptoms not coupled this it not the case.

Step 7.17. Determine Diagnosis HEP for Multiple Abnormal Events

The nominal diagnosis HEP, HEP_d, was determined and documented in Table 7.5-11.

1. Action (Symptom). The symptoms from Table 7.5-9, item 2, that are considered to be more than one abnormal event are: (i) SRVs cycle, (ii) pool temperature >95°F, perhaps (iii) drywell pressure >2 psig and (iv) drywell temperature >145°F.

TABLE 7.5-10

W SEQUENCES DIAGNOSIS ANALYSIS--ONE ABNORMAL EVENT

CUT SETS: See Table 7.5-5.

ACTION (SYMPTOM) (1)	DIAGNOSIS NEGLIGIBLE (2)	FAILURE TO DIAGNOSE (Figure 7.2-3) (3)	SKILL-BASED (4)	ADJUSTMENT IN FINAL HEP (HEP$_{sd}$) (5)	COMMENTS/ SOURCE OF INFORMATION (6)
Drywell temperature >145°F	Yes				Not worth evaluating since diagnosis failure on first event already ~<3E-6
PCV event	Will conservatively assume complete dependence on PCV event given failure of RHR containment cooling for diagnosis				It must vent before 100 psig is reached--Figure 8-1 [ ] suggests 1.0 failure. However, operators will have watched pressure rise before this and prepared venting. Will use 0.5 for failure to recognize that venting early is necessary so SRVs can be reopened.

TABLE 7.5-11

W SEQUENCES DIAGNOSIS ANALYSIS--MORE THAN ONE ABNORMAL EVENT

CUT SETS: See Table 7.5-5.

ACTION (Symptom) (1)	DIAGNOSIS NEGLIGIBLE (2)	NUMBER OF ABN EVENT (3)	ANNUNCIATOR HEP (Table 7.3-12) (HEP_{ann}) (4)	FAILURE TO DIAGNOSE (Table 7.3-13) (HEP_{d-ann}) (5)	SKILL-BASED (6)	ADJUSTMENT IN FINAL HEP (HEP_d) (7)	COMMENTS/ SOURCE OF INFORMATION (8)
SRVs cycle and pool temp >95°F and perhaps drywell pressure >2 psig (occur closely in time with initiator)	--	1 or 2 per Table 7.5-6 (will use 2 for conservatism)	Normal response annunciations not required at first	Per Table 7.3-13 for second event. 0.0001 to 0.00001, EF=30	Skill-based	<3E-6 to 3E-7	For reactor vessel/ containment critical parameters which operating personnel must commit to memory, the lower bound value is used only if the recognition of these parameters can be classified as skill-based behavior.
Drywell temperature >145°	--	Use 1 per item 9.b.2 of Table 8-1 of HRA guide [ ]	See Table 8 in HRA Guide [ ]				
PCV event	--	Use 1 per item 9.b.2 of Table 8-1 of HRA guide [ ]	See Table 8 in HRA Guide [ ]				

2. **Diagnosis Negligible.** If the probability of the operator failing to diagnose the event is negligible, the remainder of the table is not applicable. For the symptoms i, ii and iii listed in item 1, this is not the case.

3. Number of ABN Event. The number of abnormal events previously documented in Table 7.5-6, item 3 are repeated here. Two abnormal events were used as a conservative estimate.

4. Annunciator HEP (HEP_{ann}) If there is more than one abnormal event, there is a probability that the operator will fail to recognize an additional occurrence of an event. Therefore, the probability that subsequent abnormal events are not noticed must be estimated. At the time of the second abnormal event, the total number of annunciators is determined; in this example, the normal response annunciators are not required initially.

5. Failure to Diagnose (HEP_{d-ann}). Table 7.3-13 is used to estimate the diagnosis HEP for the second or subsequent simultaneously occurring abnormal event. The time available to diagnose, T_d, is retrieved from Table 7.5-9, item 5; 2 hrs to 30 hrs (120 minutes to 1800 minutes). The T_d value is the T value on Table 7.3-13. Using the table, a median joint HEP_{d-ann} for diagnosis of a second event is 0.0001 to 0.00001 (EF = 30). This was an adequate approximation since the range is large. Interpolation could have been done to find the HEP for 120 minutes and 1800 minutes.

6. Skill-Based. The behavior required of the operators consists of the performance of more or less subconscious routines based on stored patterns of behavior, therefore, it is classified as skill-based.

7. Adjustment in Final HEP. (HEP_d). The final HEP is the addition of the annunciator HEP [HEP_{ann}, item 4] and the failure to diagnose HEP [HEP_{d-ann}, item 5] after both have been adjusted downward or upward using the associated error factor. The adjustment in this example is downward since the recognition of the reactor vessel/containment critical parameters which operating personnel must commit to memory can be classified as skill-based behavior. Therefore, the HEP is 0.0001/30 to 0.00001/30

(<3E-6 to 3E-7). Note that there is no contribution from the annunciator HEP, if there had been, it would also have been adjusted down.

Step 7.18. Determine Type of Task

Table 7.5-12 documents the type of task the operator is performing.

1. Action. The actions listed here are identical to those in Table 7.5-7, item 1. The operator must align the RHR cooling mode in order to recover from the ESF-XHE-FO-RHRAT event.

2. Safety Systems Failed. Any safety systems that were functioning and subsequently fail are included here. In this example, there were none.

3. EOPs, Training, Use EOPs, Well-Designed EOPs. The answer is yes since the following conditions are met:

   (a) The initiating event in question is covered in the EOPs.
   (b) The operators have been trained using the symptom-based EOPs.
   (c) The operators use the EOPs rather than trusting to their memory.
   (d) The EOPs are well designed.

4. Operator Performs ≥ One Activity. The operator does not perform more than one activity involving more than one function in this case, without good indications (cues) for when a shift must be made from one activity to another.

5. Dynamic or Step-By-Step. The action, operator realigning RHR to cooling mode is classified as a Step-by-Step task since it is a routine, procedurally guided, set of steps performed one at a time.

Step 7.19. Determine Operator Stress Level

The stress level of operators performing the task is determined and documented in Table 7.5-13.

1. Action. The actions listed here are identical to those in Table 7.5-7, item 1. The operator must align the RHR cooling mode in order to recover from the ESF-XHE-FO-RHRAT event.

TABLE 7.5-12

W SEQUENCES POST-DIAGNOSIS ACTION-TYPE IDENTIFICATION

CUT SETS: See Table 7.5-5.

ACTION (1)	SAFETY SYSTEMS FAILED (2)	EOPs, TRAINING, USE EOPs, WELL-DESIGNED EOPs (3)	OPERATOR PERFORMS ≥ ONE ACTIVITY (4)	DYNAMIC OR STEP-BY-STEP (5)	COMMENTS/ SOURCE OF INFORMATION
The operator must align the RHR cooling mode in order to recover from the ESF-XHE-FO-RHRAT	Not related to this	Yes	No	Step-by-step	
PCV-XHE-FO-PCV	Yes--some core cooling has failed but cooling still under control with CRD (if not CRD--using 0.5 for PCV failure--see Table 8 comment [ ])	Yes	No	Step-by-step	

TABLE 7.5-13

W SEQUENCES POST-DIAGNOSIS STRESS-LEVEL IDENTIFICATION*

CUT SETS: See Table 7.5-5.

ACTION (1)	T_m <2h After IE (2)	RECIRC. PHASE IN LARGE LOCA (3)	MORE THAN TWO SAFETY SYSTEMS FAIL (4)	OPERATOR FAMILIAR W/SEQUENCE (5)	STRESS LEVEL (6)	COMMENTS/ SOURCE OF INFORMATION
The operator must align the RHR cooling mode in order to recovery from the ESF-XHE-FO-RHRAT event.	No	--	No	Yes	Moderately high stress	
PCV-XHE-FO PCV		--	Could be	Moderately	Extremely high stress	

2. T_m < 2h After IE. The maximum time available to diagnose and perform the actions, T_m (see Table 7.5-9, item 3) is not less than 2 hours.

3. Recirc. Phase In Large LOCA. This item is only applicable for PWRs. Peach Bottom is a BWR. Note that in a PWR analysis, a large LOCA is assumed as extremely high stress until such time as recirculation is established, then moderately high stress is assessed.

4. More Than Two Safety Systems Fail. In the course of the sequence, more than two safety systems do not fail for this example.

5. Operator Familiar w/Sequence. The operator is very experienced in the sequence regardless of the circumstances.

6. Stress Level. Since control room personnel are familiar with the accident sequence, moderately high stress is assessed.

Step 7.20. Calculate the Total Failure Probability

The total failure probability and post-diagnosis action HEP is determined and documented in Table 7.5-14.

1. Action. The actions listed here are identical to those in Table 7.5-7, item 1. The operator must align the RHR cooling mode in order to recover from the ESF-XHE-FO-RHRAT event.

2. Activities. The activities listed here are identical to those in Table 7.5-6, item 5.

3. Original Operator HEP (HEP_{op}). The HEP_{op} value is based on a step-by-step (see Table 7.5-12, item 5), moderately high stress (see Table 7.5-13, item 6) task. This information is used in conjunction with Table 7.3-14 to yield an HEP_{op} value of 0.02 (EF - 5). The lower bound value is used since lots of time is available to the operator, 0.02/5 - 4E-3.

4. Supervisor Fails to Correct Operator HEP (HEP_{r2}). The HEP_{r2} value is based on a step-by-step (see Table 7.5-12, item 5), moderately high stress (see Table 7.5-13, item 6) task. This information is used in conjunction with Table 7.3-14 to yield an HEP_{r2} value of 0.2 (EF - 5). The lower bound value is used since lots of time is available to the operator, 0.2/5 - 4E-2.

TABLE 7.5-14

W SEQUENCES POST-DIAGNOSIS ANALYSIS*

CUT SETS: See Table 7.5-5.

ACTION (1)	ACTIVITIES (2)	ORIGINAL OPERATOR HEP (HEP_{op}) (3)	SUPERVISOR FAILS TO CORRECT OPERATOR HEP (HEP_{r2}) (4)	THIRD INDEPENDENT CHECK/CORRECTION HEP (HEP_{r3}) (5)	TOTAL HEP (6)	COMMENTS/ SOURCE OF INFORMATION
The operator must align the RHR cooling mode in order to recover from the ESF -XHE-FO-RHRAT event. --		0.02, EF=5 from Table 7.3-14 (step-by-step, moderate stress). But, lots of time available, therefore use lower bound 4E-3.	.2, EF=5 from Table 7.3-14 (step-by-step, moderate stress). But, lots of time available, therefore, use lower bound 4E-2.	Large LOCAs: .2, EF=5 Transients: .2, EF=5 from Table 7.3-14 (step-by-step, moderate stress). But lots of time available, therefore, use lower bound .04.	~3E-5 for large LOCAs; ~6E-6 (used 1E-5 in the cut sets) for transients (diagnosis small) EF = 10	
PCV-XHE-FO-PCV	--	=0.5 item 4 of Table 8-5 of HRA guide[25]	=.5 item 7 of Table 8-5[35]	Third party will really play a role on whether to vent--=.5 per item 7 of Table 8-5[35]	~.01 (diagnosis small) except when CRD is not available and must vent early-- then using .5	

5. Third Independent Check/Correction HEP (HEP_{r3}). The HEP_{r3} value is based on a step-by-step (see Table 7.5-12, item 5), moderately high stress (see Table 7.5-13, item 6) task. This information is used in conjunction with Table 7.3-14 to yield an HEP_{r3} value of 0.2 (EF = 5). The lower bound value is used for transient initiators since lots of time is available to the operator, .2/5 = 4E-2. This is not the case for large LOCA initiators; therefore, its HEP_{r3} value remains 0.2.

6. Total HEP. The HEP_{op} value (item 3, 0.004) is multiplied with the HEP_{r2} (item 4, 0.04) and HEP_{r3} (item 5, 0.2 for large LOCAs and 0.04 for transients).

HEP_{act} = (0.004)(.04)(0.2) = 3.2E-5 ~3E-5
(for large LOCAs)

HEP_{act} = (0.004)(0.04)(0.04) = 6.4E-6 ~6E-6
(for transients)

The HEP_{d} value from Table 7.5-11, item 7, <3E-6 to 3E-7 is added to the HEP_{act} (which is equivalent to the HEP_{task} value) to yield the total failure probability, F_{T}.

Recall that the large LOCA is a single abnormal event, therefore, the F_{T} value is ~3E-5. The transient is a multiple abnormal event, therefore, the F_{T} value is ~6E-6 + 3E-6 = 9E-6 ~1E-5.

Based on engineering judgment, an error factor of 10 was used. It was judged that this value conservatively represented the range of F_{T}.

8. DATA BASE ANALYSIS

This section describes the methodology used to develop the data base for the analysis. The methodology is based on the Probabilistic Risk Assessment (PRA) Procedures Guide[37] and the Interim Reliability Evaluation Program Procedures Guide.[7] In general, data are required for initiating events and basic events. In this section the basic events of interest involve hardware failures (i.e., a device or component cannot perform its function when required) and component (or system) unavailability because of test and maintenance outages. Dependent failures (e.g., common cause) of components and systems are discussed in Section 6 and human errors and their analysis are discussed in Section 7. Several different component failure modes are possible for the same component type. Failure probabilities for each mode of hardware failure and for test and maintenance failures are developed from the collection and analysis of plant-specific and industry wide data. This data base of initiating event and basic event parameter estimates, along with the data on dependent failures and human error, form the basis for the subsequent quantification of the accident sequence frequencies.

8.1 Data Base Assumptions and Limitations

The parameters of interest in PRA include failure rates, failure probabilities, mission times, test intervals, etc. Parameter value uncertainties are modeled by defining a probability distribution for the value of each parameter. The distribution is such that the nth percentile of the distribution represents the value below which the analyst has a degree of belief of n/100 that the true parameter value lies. This subjective approach to the representation of uncertainty makes the propagation of parameter value uncertainty through to the evaluation of the core damage frequency mathematically straightforward using constrained Monte Carlo (e.g., Latin Hypercube Sample) or other sampling techniques. The uncertainty ranges characterized by the distributions vary in origin. If an estimate is based on plant-specific data, the range should be characteristic of the statistical uncertainty of the data. If an estimate is generic (or non-plant specific) the range should be characteristic of those factors which may affect the failure properties of the component in the different uses and environments from which the data for the estimate have been gathered.

Plant-specific parameter uncertainties for the NUREG/CR-4550 analyses were based on a statistical uncertainty analysis of the data (often chi square). This determined the range within which a parameter estimate would be expected to lie. Parameter estimate probability distributions were defined such that the 0.05th and 0.95th probability quantiles were within the statistical 0.05th and 0.95th confidence limits. These distributions are often taken to be lognormal. However, other types of distributions may be used if they are deemed more appropriate.

Plant-specific component failure data containing a small population of component demands or short component exposure times do not allow for an accurate evaluation of the likelihood of component failure. The generic data represent a larger record of component performance leading to a broadly based estimate of the failure probabilities of such components.

Therefore, component failure models based on generic data analyses were used when plant-specific data were deemed inadequate for analysis. However, if the quality of plant specific data is good, but the quantity is insufficient for the development of probability distributions, this data can still be incorporated into the generic distributions through the application of Bayesian statistical inference [Reference 78]. This allows the generic models to be adjusted to account for good plant specific data.

The fundamental tool of Bayesian statistics is Bayes theorem, which can be used to define a posterior probability distribution in terms of a prior probability distribution and a sampling model which incorporates the data. The prior distribution represents the state of knowledge or ignorance of a parameter value before the data has been analyzed. The posterior distribution represents the updated version of the state of knowledge in view of the data. Generic distributions of expert judgment of parameter values are examples of prior distributions and, indeed, posterior distributions can become prior distributions to be updated as new data are collected and analyzed.

If the data support the hypothesis represented in the prior distribution, then the posterior distribution should reflect an increased confidence in the previous notions encompassed by the prior model. If the data do not support the hypothesis of the prior model, then the posterior model will reflect a weighted consideration of both the prior assessment and the current data.

8.2 Data Base Development

The development of a data base for component failures or outages is a multistep process involving the development of both plant-specific and generic data. The plant-specific and generic data are developed in parallel and are combined to yield a finalized data base for a particular plant as illustrated in Figure 8.2-1 and discussed below. The finalized data base specifies the parameter estimates to be used in the quantification of the fault trees and accident sequences.

Step 8.1. Define Data Needs

In this step the analyst defines the data requirements. This data on component performance will be used to estimate the parameters values required to quantify the basic event failure probabilities. Failure probabilities or frequencies will be quantified for three types of events: (1) initiating events, (2) component failure events, and (3) test and maintenance outage events. The analyst must define the particular parameters required to quantify each type of event and therefore, the data that will be required.

The parameters of interest and for which data must be collected generally include the following:[38]

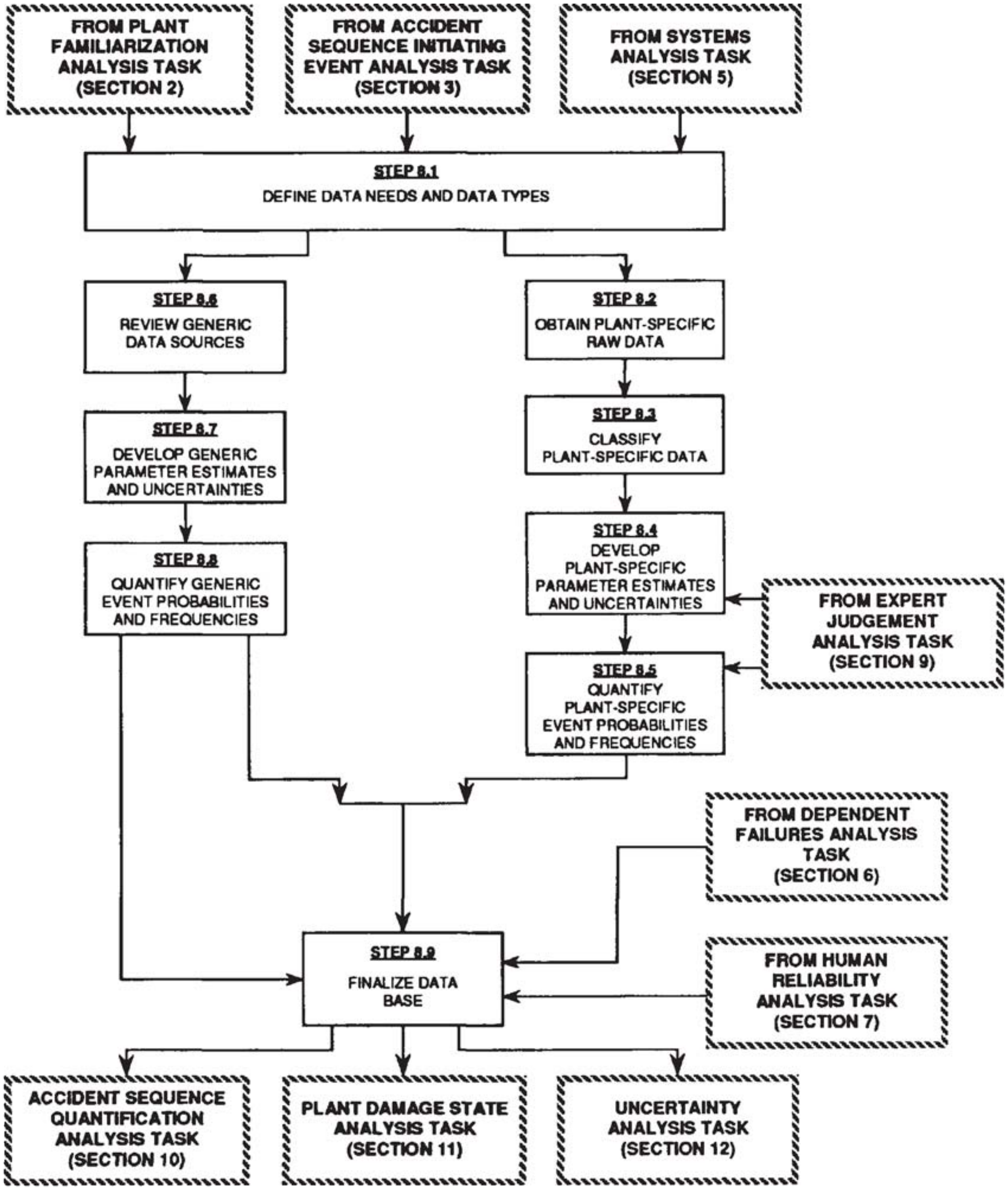

FROM PLANT FAMILIARIZATION ANALYSIS TASK (SECTION 2)
FROM ACCIDENT SEQUENCE INITIATING EVENT ANALYSIS TASK (SECTION 3)
FROM SYSTEMS ANALYSIS TASK (SECTION 5)
STEP 8.1
DEFINE DATA NEEDS AND DATA TYPES
STEP 8.6
REVIEW GENERIC DATA SOURCES
STEP 8.7
DEVELOP GENERIC PARAMETER ESTIMATES AND UNCERTAINTIES
STEP 8.8
QUANTIFY GENERIC EVENT PROBABILITIES AND FREQUENCIES
STEP 8.2
OBTAIN PLANT-SPECIFIC RAW DATA
STEP 8.3
CLASSIFY PLANT-SPECIFIC DATA
STEP 8.4
DEVELOP PLANT-SPECIFIC PARAMETER ESTIMATES AND UNCERTAINTIES
FROM EXPERT JUDGEMENT ANALYSIS TASK (SECTION 9)
STEP 8.5
QUANTIFY PLANT-SPECIFIC EVENT PROBABILITIES AND FREQUENCIES
FROM DEPENDENT FAILURES ANALYSIS TASK (SECTION 6)
STEP 8.9
FINALIZE DATA BASE
FROM HUMAN RELIABILITY ANALYSIS TASK (SECTION 7)
ACCIDENT SEQUENCE QUANTIFICATION ANALYSIS TASK (SECTION 10)
PLANT DAMAGE STATE ANALYSIS TASK (SECTION 11)
UNCERTAINTY ANALYSIS TASK (SECTION 12)

Figure 8.2-1. Step Relationship for Data Analysis

XIE - Number of initiating events,
T - Time period over which initiating events occur,
Q_d - Demand failure probability,
λ_s - Standby failure rate,
T_t - Average time between tests that would detect a standby failure,
λ_r - Running failure rate of an operating component,
T_m - Mission time following demand that component must operate,
λ_m - Frequency of unscheduled maintenance outage,
T_{rt} - Average repair time for components from unscheduled maintenance,
λ_t - Frequency of scheduled testing,
T_{to} - Average test outage time,
λ_{ms} - Frequency of scheduled maintenance, and
T_{rts} - Average repair time for components from scheduled maintenance.

To be responsive to the needs of the systems analysts, the data requirements must be based upon the various types of component failures specified as basic events in the fault trees. Thus, the data analyst must identify: (1) the system components of interest (e.g., auxiliary feedwater pump, service water motor operated valve), (2) the failure type of interest (e.g., hardware), (3) the applicable failure modes (e.g., fails to start), and (4) the operational mode (e.g., standby).

Step 8.2. Obtain Plant-Specific Raw Data

In this step the analyst identifies and reviews the data sources for developing the plant-specific data base. Unfortunately, few, if any, utilities keep records for the specific purpose of compiling data for risk assessments. Potential sources of information for parameter estimates are discussed below. The parameters of interest fall into one of three categories:

(1) Component Failure Rates,
(2) Test and Maintenance Unavailabilities, or
(3) Initiating Event Frequencies.

<u>Component Failure Rates</u>

Plant operating history is reviewed for a list of plant specific failures for systems and components. The sources include:

- Licensee Event Reports (LERs),
- Operator/control room logs,
- Diesel generator start logs,
- Engineering data,
- Expert judgment of plant personnel, and
- Nuclear Regulatory Commission (NRC) Gray Book.

Test and Maintenance Unavailabilities

Plant technical specifications and maintenance records are reviewed to ascertain the maintenance and test intervals for systems and components. Other sources of information include:

- Plant logs,
- Maintenance work orders,
- Diesel generator start logs, and
- Plant personnel.

Information from the latter is essential to define test durations and maintenance frequencies for systems and components.

Initiating Event Frequencies

Plant specific information is reviewed to establish initiating event frequencies for the initiating event groups identified in Section 3. The sources include:

- LERs,
- post-trip analysis reports,
- operating reports,
- expert judgment of plant personnel, and
- NRC Gray Book.

Step 8.3. Classify Plant-Specific Data

In this step the data collected in the preceding step is classified and evaluated. This involves four activities which are performed for each component type (e.g., motor operated valve) as follows:

- The data are classified by failure type and segregated into one of three categories; component failures, test and maintenance outages, and initiating events. The data being classified are the recorded failures, number of unscheduled maintenance activities, etc., defined in Step 8.1.

- Next the data are classified by the specific component failure modes involved (e.g., hardware -- motor operated valve fails to open, pump fails to start, etc). Thus, for each failure type, the data are separated by the various component failure modes.

- The data are then classified according to the operational mode of the component. That is, will the data be used to compute a failure rate for a standby component or a normally running component.

- Finally, the available data are evaluated for relevance to the analysis. Not all the equipment problems reported necessarily result in the failure or unavailability of a component to perform its function; this must be evaluated in this step.

It should be noted that the level of detail of component failures initially defined in the systems analysis model may not be compatible with the available data. For example, the systems analyst may have defined the following failure modes for a basic event: (1) valve-fails-to-close because of a broken stem, (2) valve-fails-to-close because of a cracked yoke, (3) valve-fails-to-close because motor bearings failed. When the data analyst examines the plant-specific and generic information the only thing recorded is, valve-fails-to-close. The specific cause of the failure is not noted. Therefore, a single event would have to be modeled by the systems analyst: valve-fails-to-close because of hardware faults.

Step 8.4. Develop Plant-Specific Parameter Estimates and Uncertainties

In this step the analyst takes the data from Step 8.3 and, for each component, calculates the required parameters as defined earlier for each failure type and each failure mode. The equations used to determine the point estimates of these parameters are discussed below.

Component failures can be either demand related, time related (also referred to as rate related since a rate parameter is involved) or both. A demand type failure is one wherein a component is demanded to function and it fails. No account is taken of elapsed time between demands. A time related failure is one wherein the time period over which the demands and failures occur is considered. The parameter value, whether the event is demand related or time related, must be estimated.

If a component is normally operating, hardware failures are always modeled as time related failures. If a component is a standby component, hardware failures can be either demand or time related. Maintenance outages can be either demand or time related regardless of the operational status of the component (i.e., normally operating or standby). For these cases, the determination is made based upon the plant records. If the plant records show failures and demands (the latter both successful and unsuccessful), then a demand related parameter is calculated. However, if the records only indicate the number of failures, and not the number of demands, then a time related parameter is computed based upon the period of operating time over which the failures occurred.

Based upon this information the parameters are calculated as follows:

Demand Related Parameters

Demand related parameters take the form:

$$Q_d(f/d) = X/Y$$

where X is the number of failures on demand and Y is the total number of opportunities for failure (i.e., the total number of demands and tests on the component type). Therefore, for each component and failure mode, the analyst is using the number of failures and number of component demands to estimate the demand failure probability.

Time Related Parameters

Time related parameters take the form:

$$\lambda(f/hr) = W/Z$$

where W is the number of failures of interest and Z is the total amount of operating time over which these failures occurred. In order to calculate event probabilities with these failure rates, a time parameter associated with the failure rate must also be estimated. These parameters are estimated as follows:

Standby Hardware Failure Rate - λ_s

$$\lambda_s = W_s/Z_s$$

where W_s = number of failures to start,
Z_s = total amount of time component is in standby.

- Average Time Between Tests - T_t

  This is the time between the component or system tests during which an undetected failure could occur. The time period is established by the Technical Specifications.

- Running Failure Rate - λ_r

$$\lambda_r = W_r/Z_r$$

where: W_r = number of failures while operating,
Z_r = total amount of time component operating time.

- Mission Time - T_m

This is the time period for which the component must operate in response to off-normal conditions. This time is determined by the accident sequence analyst.

- Frequency of Unscheduled Maintenance - λ_m

$$\lambda_m = W_m/Z_m$$

where: W_m = Number of unscheduled maintenance activities on a particular component,
Z_m = Time period over which the unscheduled maintenance occurred.

- Average Repair Time - T_{rt}

This time is determined from the plant maintenance records and is simply the average time that is required to repair the component during unscheduled maintenance.

- Frequency of Scheduled Maintenance - λ_{ms}

$$\lambda_{ms} = W_{ms}/Z_{ms}$$

where: W_{ms} = Number of scheduled maintenance activities on a particular component, and
Z_{ms} = Time period over which the scheduled maintenance occurred.

- Average Repair Time (T_{rts})

This time is determined from the plant maintenance records and is simply the average time required to repair the component during scheduled maintenance.

- Frequency of Scheduled Testing λ_t

$$\lambda_t = W_t/Z_t$$

where: W_t = number of tests conducted,
Z_t = total amount of time over which testing occurred.

This frequency may also be specified by technical specifications for some components.

- Average Test Outage (T_{to})

This is the amount of time the component is out of service for a single test (i.e., the average time to test the component).

The point estimates are assumed to be the mean values of the underlying probability distributions for the parameters. A probability distribution (typically lognormal) is chosen such that the probabilistic uncertainty is bounded by the classical statistical confidence limits for the parameter data. Therefore, at the conclusion of this step, all of the plant-specific parameter estimates will have been established and each will have an associated probability distribution.

Step 8.5. Quantity Plant-Specific Event Probabilities and Frequencies

In this step the analyst uses the plant-specific parameter estimates and uncertainties from Step 8.4 to quantify event probabilities and frequencies. The probability distributions for the demand related basic events are exactly the same as those for the corresponding parameter estimate. For time dependent basic events, the distribution of the underlying parameter is simply scaled by the time parameter. No uncertainty is associated with the time parameter, so the shape of the distribution is not changed by the scaling. Therefore, at the conclusion of this step all of the plant-specific failure probabilities have an associated distribution.

These events fall into categories that are identical to those for which items of information were gathered in Step 8.2.

(a) Component Failure Probabilities,
(b) Test and Maintenance Unavailabilities, or
(c) Initiating Event Frequencies.

The equations used to calculate the point estimates of these categories are presented below.

Component Failure Probabilities

- Demand Related Probabilities

$$Q_d = X/Y \qquad (8.1)$$

where Q_d = probability of failure on demand,
X = number of failures,
Y = number of demands.

- Time Related Probabilities

$$P_f = \lambda_s * T_t/2 \qquad (8.2)$$

$$P_{fr} = \lambda_r * T_m \qquad (8.3)$$

where P_f = probability of failure on demand
P_{fr} = probability of failure to operate T_m hours
λ_s = standby failure rate,
T_t = average time between tests that could detect a failure,
λ_r = operating failure rate,
T_m = mission time following demand over which component is required to operate.

The selection of the appropriate equation is dependent upon the nature of the data and the circumstances being modeled. Equations 8.1 and 8.2 can be used to model the same component failure mode; failure of standby component to switch to operational mode upon demand. The choice of equation 8.1 or 8.2 depends upon the analyst's belief as to whether the data better supports the development of demand related parameters or time related parameters in Step 8.4. It should be noted that equation 8.2 should be used only if the faulted condition of a component which would result in failure on demand can be detected only when the component is demanded or tested. If a component faulted condition is immediately known to the plant staff, then the component outage should be modeled as a maintenance unavailability described below. Equation 8.3 is relevant for modeling the probability of a component failing to operate over the time period required to respond to the accident conditions.

Test and Maintenance Unavailabilities

- Rate Related Probabilities

$$P_{um} = \lambda_m * T_{rt} \qquad (8.4)$$

$$P_{ums} = \lambda_{ms} * T_{rts} \qquad (8.5)$$

$$P_{to} = \lambda_t * T_{to} \qquad (8.6)$$

where: P_{um} = unavailability from unscheduled maintenance,
P_{ums} = unavailability from scheduled maintenance,
P_{to} = unavailability from testing
λ_m = frequency of unsched'iled maintenance,
λ_{ms} = frequency of scheduled maintenance,
λ_t = frequency of scheduled testing,
T_{rt} = average repair time from unscheduled maintenance,
T_{rts} = average repair time from scheduled maintenance,
T_{to} = average test outage time.

Equations 8.4 through 8.6 are used for both standby and normally operating components.

Initiating Event Frequencies

Initiating Event frequencies vary from plant to plant. The plant specific initiating frequencies are based on the operating history of the plant. The occurrences of the initiating events recorded from the data collection in Step 8.2 are now divided by the number of reactor years that the plant has operated.

$$IEF = X_{IE}/T$$

where IEF = initiating event frequency,
X_{IE} = number of initiating events of a specific type,
T = reactor years of operation over which the events occurred.

Probability Distributions

The probability distributions for the demand related basic events are exactly the same as for the corresponding parameter estimate. For time dependent basic events, the distributions of the underlying parameters is simply scaled by the time parameter. No uncertainty is associated with the time parameter, so the shape of the distribution is not changed by the scaling.

Step 8.6. Compile Generic Data

In this step the analyst compiles a set of generic parameter values and associated estimates of uncertainty for those parameters defined in Step 8.1. These generic values are obtained by a review of past PRAs, reports, and studies which may include expert judgment on failure rates and probabilities. This following discussion is based on the work done in the Approaches to Uncertainty Analysis in Probabilistic Risk Assessment document.[38]

The available nuclear power component data sources may be categorized as follows:

(1) Collections of actual failure events,
(2) Statistical analyses of data,
(3) Generic failure rate data bases.

The analyst must be aware that many sources of component failure characteristics are, in fact, just reanalyses of existing data and thus are not new or independent data sources. This situation must always be kept in mind when reviewing the literature for appropriate generic failure rates for use in a PRA. The more important sources of reliability data for nuclear power plant components are categorized and summarized below.

As mentioned above, the number of actual data collections (Category 1) is relatively small. Historically, the most important in the United States are the Licensee Event Reports. Summaries of these reports and associated statistics for different component types are contained in reports generated at the Idaho National Engineering Laboratory. More recently, the In-Plant Reliability Data System Program at the Oak Ridge National Laboratory has been collecting and summarizing failure data from U.S. plants in a systematized format. A third source of data is the Nuclear Plant Reliability Data System operated by the Institute for Nuclear Power Operations. In addition, there have been a number of special purpose data collections related to loss of offsite power, anticipated transients without scram, and diesel generator reliability. A summary of such data collections is presented in Table 8.2-1.

The second category of reliability data sources consist of reports that have analyzed failure event data from one or more of the above sources, and produced data-based estimates of the failure or unavailability rates for different components. Reports often differ as to the assumptions regarding number of demands, plant down-time or method of statistical analysis, and thus different reports can arrive at different failure rates using the same base of failure events. Table 8.2-2 lists a number of such studies which have been found useful. They differ from the reports in Category 1 in that sufficient information for reanalysis of the data under different assumptions is not usually available.

The final category consists of compilations of generic component failure rates and associated estimates of uncertainty. These generic values are usually obtained by review of two or more Category 1 or 2 sources, and may also include expert judgment on component failure rates or probabilities derived from other (non-nuclear) experience. Table 8.2-3 lists the more important generic data bases in use today.The user is cautioned again that these various generic data bases should never be construed as being independent, as in no case is this true. Further, considerable expert judgment has been used in choosing appropriate generic values.

Step 8.7. Develop Generic Parameter Estimates and Uncertainties

In this step the analyst reviews the parameter values and estimates collected in Step 8.6 for each component failure mode of concern. A

Table 8.2-1
Collections and Summaries of Actual Failure Events

Title	Source	Reference
1. Licensee Event Reports	USNRC	
2. Licensee Event Report Summaries	Idaho National Engineering Laboratory	
Valves		NUREG/CR-1363[11]
Pumps		NUREG/CR-1205[12]
Electrical Power		NUREG/CR-1362[40]
Circuit Breakers, Protective Relays		NUREG/CR-4212[41]
Initiating Events		NUREG/CR-3862[15]
Selected I&C Components		NUREG/CR-1740[42]
Control Rods and Drive Mechanisms		NUREG/CR-1331[43]
3. In-Plant Reliability Data Systems	Oak Ridge National Laboratory	
Pumps		NUREG/CR-2886[44]
Valves		NUREG/CR-3154[45]
Electrical Power Components (Diesels, Batteries, Chargers and Inverters)		NUREG/CR-3831[46]
4. Nuclear Plant Reliability Data System	Institute for Nuclear Power Operations	Quarterly Reports
5. Reactor Safety Study Section III - LER Data for 1972-1973	USNRC	WASH-1400[39]
6. ATWS: A Reappraisal	Electric Power Research Institute	EPRI NP-2230[13]
7. Loss of Offsite Power at Nuclear Power Plants	Electric Power Research Institute	EPRI NP-2301[47] NSAC-103[48]
8. Diesel Generator Reliability at Nuclear Power Plants	Electric Power Research Institute	EPRI NP-2433[49]
9. Classification and Analysis of Reactor Operating Experience Involving Dependent Events	Electric Power Research Institute	EPRI NP-3967[21]
10. PORV Failure Reduction Methods	Combustion Engineering	CEN-145[50]
11. Evaluation of Station Blackout Accidents at Nuclear Power Plants: Technical Findings Related to Unresolved Safety Issue A-44: Final Report	NRC	NUREG-1032[28]

Table 8.2-2
Statistical Analyses of Data

Title	Source	Reference
Probabilistic Safety Analysis of DC Power Requirements for Nuclear Power Plants	USNRC	NUREG-0666[25]
Reliability Data Book	Swedish Nuclear Power Inspectorate	RSK 85-25[51]
Statistical Analysis of Nuclear Power Plant Pump Failure Rate Variability-Preliminary Results	Los Alamos National Laboratory	NUREG/CR-3650[52]

In addition, items 2, 3, 5, 7, 8, 9, and 10 of Table 8.2-1 present analyses of reported data.

Table 8.2-3
Other Generic Failure Rate Data Bases

Title	Source	Reference
Reactor Safety Study	USNRC	WASH-1400[39]
Interim Reliability and Evaluation Program (IREP) Procedures Guide	Sandia National Laboratories	NUREG/CR-2728[7]
Reliability Data Book	Swedish Nuclear Power Inspectorate	RKS 85-25[51]
Station Blackout Accident Analyses - TAP A-44	USNRC	NUREG/CR-3226[27]

point estimate and probability distribution must be chosen that reasonably represent the state of knowledge of each component failure.

The sources of reliability information (see Step 8.6) can be used either individually or collectively. If it is believed that the data or a parameter estimate presented in a particular study is the best representation of knowledge available, the analyst may choose to use that specific information directly from the study. If no strong consensus exists as to which study represents the best information or the best analysis of data for a particular parameter, then the values from several studies can be used to define a range on the parameter estimate. A point estimate and a probability distribution must be selected that characterize the knowledge and uncertainty expressed by the difference among the various studies.

Step 8.8. Quantify Generic Event Probabilities and Frequencies

In this step the generic parameter estimates and uncertainties from Step 8.7 are used to quantify events which, as in Step 8.5 for the plant specific analysis, fit into one of three categories of information:

(1) Component Failure Rates,
(2) Test and Maintenance Unavailabilities, or
(3) Initiating Event Frequencies.

The equations used to calculate the point estimates of the component failure probabilities and test and maintenance unavailabilities are identical to those described in Step 8.5. At the conclusion of this step all of the generic events have a mean, median, and a probability distribution related to the parameter estimates.

Step 8.9. Finalize Data Base

In this step the analyst finalizes the data base. Ideally, the PRA of a particular plant would use only plant-specific data. This would be an accurate representation of the plant. But, the limited availability of data forces the analyst to merge the plant-specific parameter estimates with generically developed estimates. Because the generic data is based on the experience of a number of plants, the combination of generic and plant-specific data provides information on the full spectrum of events modeled in the PRA.

8.3 Data Base Recommended Reporting

There are a number of items from the data analysis which are reported in the PRA documentation. These include any combination of the following which describe an event:

- Identifier. This is a description of the component or event as it appears in the data base (e.g., ESW-MDP-MA-MDPA is an emergency service water motor-driven pump A out for maintenance).

- Failure Rate. The failure rate is given per demand or per hour and should have the associated error factor recorded.

- Mission Time. This specifies the time over which a given component or system is required to operate in response to an initiating event. For any given system this time may vary depending upon the initiating event.

- Failure Probability or Unavailability. The failure probability or unavailability for each event is listed with its median and mean values and its associated error factor.

- Description. The equation with which the event probability was quantified or any specific comments about the event are provided.

- Source/Comments. The source of the values assigned to the event is identified, (e.g., WASH-1400, plant specific) and any comments relevant to the event are discussed.

Not all sources are listed explicitly in the PRA report. Sources such as the LERs, operator logs, diesel generator start logs and the expert judgment of plant personnel are available to reviewers but usually are not printed in the final report.

The ASEP generic data base is presented in Tables 8.2-4 through 8.2-10 (pages 8-19 through 8-46). These tables include: initiating event frequencies, event hardware failure probabilities, test and maintenance event unavailabilities, common cause factors and human error probabilities. These tables are in slightly different format from that described above because they are generic and it is anticipated that the data would be evaluated and perhaps reformatted before use. However, the same information is presented.

8.4 Example of Data Base Analysis

The example for an analysis of plant-specific data is taken from the Surry plant analysis. For all other examples in this document, material was taken from the Peach Bottom analysis. An exception is being made here because the Surry plant has excellent maintenance records which allowed the Surry team to do plant-specific data analyses that were more extensive than those done on the other plants. This does not mean that the other plant teams did not adhere to the methods described in this chapter, but that the information available at the other plants limited the comprehensiveness of plant-specific data analysis.

8.4.1 Plant-Specific Data Analysis

The example chosen is taken from the analysis of the Surry Auxiliary Feedwater System (AFWS) motor driven pump data. The specific failure mode is fail-to-start.

Step 8.1. Define Data Needs

This step requires input from the systems analysis tasks. The systems analysis developed a model for the AFWS, among other systems. Several failure modes for the major system components were incorporated into the model. The two motor-driven AFWS pumps are modeled for fail-to-run, fail-to-start, out for maintenance, and common cause failure. We are interested here in the fail-to-start failure mode.

The parameter whose value we would like to estimate with data is the probability of failure to start, given that the pump is demanded - Q_d. We are interested only in hardware failures, as support failures and maintenance outages are modeled by other events and parameters. The last thing which must be verified is the operational mode of the AFW pumps which are readily identified from the systems analysis as standby components.

Step 8.2. Obtain Plant-Specific Raw Data

The sources of information which will be reviewed for data must be identified by communicating to the plant personnel what information is needed. The Surry plant maintains a computerized record of every maintenance activity ever performed on selected major components. Even though we are interested in a hardware component failure rate, the maintenance records are very relevant because all hardware problems result in a maintenance action to repair them.

A printout of approximately 60 maintenance activities for the two AFW pumps was generated from the Surry records. This information represented all of the maintenance activity, both scheduled and unscheduled, on both pumps for the operating history of the plant.

Step 8.3. Classify Plant-Specific Data

The Surry data analysts worked closely with the plant maintenance personnel to review the maintenance records so that data not relevant to the analysis was screened out. Two important pieces of information for the parameter Qd need to be found from the data - the number of demands on the AFW pumps, and the number of failures to start. To this end, the data was classified as follows:

<u>Failures of AFW Pump to Start</u> - The maintenance records on the AFW pumps were reviewed for two types of events - catastrophic failures and incipient failures. Catastrophic failures were maintenance events wherein from the description of the event it was obvious that the AFW pumps had failed to start. Incipient failures are less clear regarding the inability of the pump to supply sufficient water to the steam generators. An incipient failure would be an event where the AFW pumps were demanded under test situations, and the performance of a pump was less than satisfactory. For example, if the description of a maintenance event was "low vibration was observed, so the bearings were repacked..." then the event was reviewed along with the maintenance personnel. If it was concluded that the maintenance action was minor (such as repacking the bearings) and that the pump could have continued to function in a

real emergency, then the event was disregarded. If the event led to the replacement of a major component (e.g., shaft coupling), then it was counted as a failure. This process resulted in the identification of six failures-to-start for the AFW motor driven pumps.

Demands for a Motor Driven AFW Pump - The number of demands were estimated by reviewing the control room logs, plant logs, and maintenance records for three types of demands;

- actual demands (non-test situation)
- scheduled testing
- unscheduled test or maintenance which resulted in a demand

Plant maintenance personnel were consulted during the data review to ensure that an accurate estimate of demands was achieved. The result was an estimate of 960 demands for AFW motor driven pumps at Surry.

Step 8.4. Develop Parameter Estimates and Uncertainties

The data from the previous steps, six failures in 960 demands, results in a point estimate of:

$$\begin{aligned} Q_d &= 6/960 \\ &= 6.3E\text{-}3/d \end{aligned}$$

The chi square, one-sided upper confidence limit was calculated at 95%. The number of degrees of freedom chosen was 2n+2, where n is the number of failures, so the degrees of freedom were 14. The 95% chi square value for 14 degrees of freedom is 23.68, and the upper confidence limit is:

$$\begin{aligned} UCL &= \frac{\chi^{2}_{.95,14}}{2n} \\ &= \frac{23.68}{1920} \\ &= 1.2E\text{-}2/d \end{aligned}$$

The probability distribution for this parameter was assumed to be lognormal with a mean value equal to the point estimate, 6.0E-3/d and a 95th quantile equal to the upper confidence limit. The error factor, defined as the ratio of the 95th quantile to the 50th quantile of a lognormal distribution, is calculated using the following equations:

$$\mu = M\lambda_{.50}$$

$$EF = \frac{\lambda_{.95}}{\lambda_{.50}}$$

$$= \frac{\lambda_{.95}}{\mu} M$$

$$M = \mathrm{EXP}\left[\left(\frac{1}{1.645}\ell n[\mathrm{EF}]\right)^2/2\right]$$

where:

μ ≡ mean

$\lambda_{.x}$ ≡ the xth quantile

EF ≡ Error Factor

M ≡ The ratio of the mean to the median.

The analyst for Surry used these relationships to define the ratio of $\lambda_{.95}$ to μ as a function of EF. The non-linear equation,

$$f(\mathrm{EF}) = \frac{\mathrm{EF}}{M} = \frac{\mathrm{EF}}{\mathrm{EXP}\left[\left(\frac{1}{1.645}\ell n[\mathrm{EF}]\right)^2/2\right]} = \frac{\lambda_{.95}}{\mu}$$

was used to solve graphically for the unknown EF values. The y-axis of a graph plotted the $\lambda.95/\mu$ values while the x-axis plotted the corresponding value for the EF. The equations on page 8-17 are used with chosen EF values to create a graph. Then, using the actual values for $\lambda_{.95}$ and μ from the data analysis, the value for the error factor for this particular lognormal distribution was taken off the graph. The result was that the probability of a failure of the AFW motor driven pump to start was modeled as lognormal, mean of 6.3E-3/d, error factor of 2.2.

Step 8.5. Quantify Plant-Specific Event Probabilities and Frequencies

Both basic events, which involve failure-to-start of the motor driven pumps are quantified using the model for the parameter Qd derived from the data. The two events;

AFW-MDP-FS-FW3A, and
AFW-MDP-FS-FW3B;

are quantified in the systems analysis and accident sequence quantification as;

lognormal distribution
mean = 6.3E-3/d
EF = 2.2

Table 8.2-4
Initiating Event Frequencies

Initiator	Range from Other Sources	Data Sources	ASEP Mean Value	Distribution	Comments
Transient from Loss of a DC Bus	5E-4 to 6E-2/yr	8, 15, 25 30, 34	6E-3	Lognormal EF=3	The DC Power Study[25] value of 6E-3 was based on a review of operational experience. Although this value does not take into account an expanded Licensee Event Report data base and improved mechanistic analyses, such as improved test and maintenance practices and operator recovery actions, it represents a reasonable value to typify the range of values used by various studies.
Transient from Loss of an AC Bus	9E-4 to 6E-2/yr	8, 15, 30 34	5E-3/yr	Lognormal EF=3	ASEP used the NSAC Oconee Probabilistic Risk Assessment[34] value. Sufficient plant analyses have not been performed to support a generic application and the applicability of this initiator is very plant specific.
Transient from Loss of Offsite Power	--	20	See Comments	Plant Specific	No generic initiating event frequency for loss of offsite power was used for ASEP. Analyses were performed to determine plant specific frequencies as described in Reference 20.

Table 8.2-4
Initiating Event Frequencies (Continued)

Initiator	Range from Other Sources	Data Sources	ASEP Mean Value	Distribution	Comments
Transient w/o Loss of the Power Conversion System	3.7 to 7.1/yr	8, 13, 14, 15, 33, 53, 54, 55			The value used in ASEP was obtained by expanding on EPRI NP-2230[13], EPRI NP-801,[14] and NUREG/CR-3862.[15]
BWR (T3A, B)			4.7/yr(1)	Lognormal EF=3	(1) FW available, T3A. (2) FW not available, T3B. See Section 3 for grouping of individual initiating events.
			0.6/yr(2)	Lognormal EF=3	
PWR (T3)			7.1/yr	Lognormal EF=3	
Transient w/ Loss of the Power Conversicn System	1.8 to 5.2/yr	13, 14, 15, 33, 54, 55, 56			The value used in ASEP was obtained by expanding on EPRI NP-2230.[13] EPRI NP-801,[14] and NUREG/CR-3862.[15]
BWR (T2)			1.7/yr	Lognormal EF=3	See Section 3 for grouping of individual initiating initiating events.
PWR (T2)			1.2/yr	Lognormal EF=3	
Transient from Inadvertent Open Relief Valve (BWR)	0.2	13, 14, 15	0.1/yr	Lognormal EF=3	The value used in ASEP was obtained by expanding on EPRI NP-2230.[13] EPRI NP-801,[14] and NUREG/CR-3862.[15] See Section 3 for grouping of individual initiating events.

Table 8.2-4
Initiating Event Frequencies (Continued)

Initiator	Range from Other Sources	Data Sources	ASEP Mean Value	Distribution	Comments
Small Small LOCA					
BWR	2E-2/yr	8, 59	2E-2/yr	Lognormal EF=3	For BWRs, past PRAs were reviewed and a frequency selected based on the average of the range. The ASEP value for PWRs was based on a Nuclear Regulatory Commission (NRC) memo by Thomas E. Murley on Reactor Coolant Pump (RCP) seal failure.[59]
PWR	2E-2/yr	31, 33, 39, 53	2E-2/yr	Lognormal EF=3	
Small LOCA					
BWR	--	39	1E-3/yr	Lognormal EF=3	ASEP used the generic value from WASH-1400[39] for BWRs. For PWRs past PRAs were reviewed and a frequency selected based on a value typical of the range.
PWR	1E-4 to 1E-3/yr	31, 33, 34, 39, 53, 57 58	1E-3/yr	Lognormal EF=3	
Intermediate LOCA					
BWR	--	39	3E-4/yr	Lognormal EF=3	ASEP used the generic value from WASH-1400[39] for BWRs. For PWRs past PRAs were reviewed and a frequency selected based on a value typical of the range.
PWR	1E-4 to 2E-3/yr	31, 33, 34, 39, 53, 57, 58	1E-3/yr	Lognormal EF=3	

Table 8.2-4
Initiating Event Frequencies (Concluded)

Initiator	Range from Other Sources	Data Sources	ASEP Mean Value	Distribution	Comments
<u>Large LOCA</u>					
BWR	1E-4/yr	39	1E-4/yr	Lognormal EF=3	ASEP used the generic value from WASH-1400[39] for BWRs. For PWRs, past PRAs were reviewed and a frequency selected based on a value typical of the range.
PWR	1E-4 to 9E-4	31, 33, 34, 39, 53, 57, 58	5E-4/yr	Lognormal EF=3	

Table 8.2-5
Valve Failure Rates

Component Failure Mode	Range from Other Sources	Data Sources	ASEP Mean Value	Distribution	Comments
<u>Air Operated Valves</u>					
Failure to Operate	3E-4/D to 2E-2/D	11, 18, 31, 33, 39, 54, 55, 60, 61, 62, 63	2E-3/D	Lognormal EF=3	The ASEP value is from the NRC LER Data Summary.[11] There are two types of failures included in the failure rate: 1E-3 valve hardware faults, 1E-3 valve control circuit command faults.
Failure Due to Plugging	2E-5/D to 1E-4/D, 1E-7/yr	18, 31, 33, 39, 54, 55, 60, 61, 62, 63	1E-7/hr	Lognormal EF=3	The ASEP value is from the NRC LER Data Summary.[11]
Unavailability Due to Test and Maintenance	6E-5/D to 6E-3/D	18, 31, 33, 39, 54, 55, 60, 61, 62, 63	8E-4/D	Lognormal EF=10	A detailed multiple regression analysis was done using the plant test and maintenance motor operated valve responses to questions asked in NUREG-0737.[64]

Table 8.2-5
Valve Failure Rates (Continued)

Component Failure Mode	Range from Other Sources	Data Sources	ASEP Mean Value	Distribution	Comments
Air Operated Valves (cont.)					
Spurious Closure	--	--	1E-7/hr	Lognormal EF=3	The ASEP value is from the IREP Procedures Guide.[7]
Spurious Open	--	--	5E-7/hr	Lognormal EF=10	The ASEP value is from the IREP Procedures Guide.[7]
Pressure Regulator Valve					
Failure to Open	--	--	2E-3/D	Lognormal EF=3	The ASEP value is from the NRC LER Data Summary[11] for air operated valves.
Motor Operated Valves					
Failure to Operate	1E-3/D to 9E-3/D	11, 18, 31, 33, 39, 54, 55, 60, 61, 62, 63	3E-3/D	Lognormal EF=10	The ASEP value is from the Station Blackout Study.[27] There are two types of failures included in the failure rate: 5E-4 valve hardware faults, 2.5E-3 valve control circuit command faults.

Table 8.2-5
Valve Failure Rates (Continued)

Component Failure Mode	Range from Other Sources	Data Sources	ASEP Mean Value	Distribution	Comments
Failure Due to Plugging	2E-5/D to 1E-4/D	18, 31, 33, 39, 54, 55, 56, 61, 62, 63	1E-7/hr	Lognormal EF-3	The ASEP value is from the NRC LER Data Summary.[11]
Unavailability Due to Test and Maintenance	6E-5/D to 6E-3/D	18, 31, 33, 39, 54, 55, 56, 61, 62, 63	8E-4/D	Lognormal EF-10	A detailed multiple regression analyses was done using the plant test and maintenance motor operated valve responses to questions asked in NUREG-0737.[64]
Failure to Remain Closed	--	--	5E-7/hr	Lognormal EF-10	The ASEP value is from the IREP Procedures Guide.[7]
Failure to Remain Open	--	--	1E-7/hr	Lognormal EF-3	The ASEP value is from the IREP Procedures Guide.[7]
<u>Solenoid Operated Valves</u>					
Failure to Operate	1E-3/D to 2E-2/D	11, 18, 31, 39, 55, 61, 62, 63	2E-3/D	Lognormal EF-3	The ASEP value is from the NRC LER Data Summary[11] for air operated valves. There are two types of failures included in the failure rate: 1E-3 valve hardware faults, 1E-3 valve control circuit command faults.
Failure Due to Plugging	2E-5/D to 1E-4/D, 1E-7/yr	18, 31, 33, 39, 54, 55, 60, 61, 62, 63	1E-7/hr	Lognormal EF-3	The ASEP value is the NRC LER Data Summary[11] value for air operated valves.

Table 8.2-5
Valve Failure Rates (Continued)

Component Failure Mode	Range from Other Sources	Data Sources	ASEP Mean Value	Distribution	Comments
Unavailability Due to Test and Maintenance	6E-5/D to 6E-3/D	18, 31, 33, 39, 54, 55, 60, 61, 62, 63	8E-4/D	Lognormal EF=10	A detailed multiple regression analysis was done using the plant test and maintenance motor operated valve responses to questions asked in NUREG-0737.[64]
<u>Hydraulic Operated Valves</u>					
Failure to Operate	3E-4/D to 2E-2/D	11, 18, 31, 33, 39, 54, 55, 60, 61, 62, 63	2E-3/D	Lognormal EF=3	The ASEP value is the NRC LER Data Summary[11] value for air operated valves. There are two types of failures included in the failure rate: 1E-3 valve hardware faults, 1E-3 valve control circuit command faults.
Failure Due to Plugging	2E-5/D to 1E-4/D, 1E-7/yr	18, 31, 33, 39, 54, 55, 60, 61, 62, 63	1E-7/hr	Lognormal EF=3	The ASEP value is the NRC LER Data Summary[11] value for air operated valves.
Unavailability Due to Test and Maintenance	6E-5/D to 6E-3/D	18, 31, 33, 39, 54, 55, 60, 61, 62, 63	8E-4/D	Lognormal EF=10	A detailed multiple regression analysis was done using the plant test and maintenance motor operated valve responses to questions asked in NUREG-0737.[64]

Table 8.2-5
Valve Failure Rates (Continued)

Component Failure Mode	Range from Other Sources	Data Sources	ASEP Mean Value	Distribution	Comments
<u>Explosive Operated Valves</u>					
Failure to Operate	1E-3/D to 9E-3/D	11, 18, 31, 33, 39, 54, 55, 60, 61, 62, 63	3E-3/D	Lognormal EF=3	The ASEP value is from the Station Blackout Study[27] for motor operated valves. There are two types of failures included in the failure rate: 5E-4 valve hardware faults 2.5E-3 valve control circuit command faults.
Failure Due to Plugging	2E-5/D to 1E-4/D	18, 31, 33, 39, 54, 55, 60, 61, 62, 63	1E-7/hr	Lognormal EF=3	The ASEP value is the NRC LER Data Summary[11] value for motor operated valves.
Unavailability Due to Test and Maintenance	6E-5/D to 6E-3/D	18, 31, 33, 39, 54, 55, 60, 61, 62, 63	8E-4/D	Lognormal EF=10	A detailed multiple regression analysis was done using the plant test and maintenance motor operated valve responses to questions asked in NUREG-0737.[64]

Table 8.2-5
Valve Failure Rates (Continued)

Component Failure Mode	Range from Other Sources	Data Sources	ASEP Mean Value	Distribution	Comments
Manual Valve					
Failure Due to Plugging	2E-5/D to 1E-4/D, 1E-7/yr	18, 31, 33, 39, 54, 55, 60, 61, 62, 63	1E-7/hr	Lognormal EF=3	The ASEP value is the NRC LER Data Summary[11] value.
Unavailability Due to Test and Maintenance	6E-5/D to 6E-3/D	18, 31, 33, 39, 54, 55, 60, 61, 62, 63	8E-4/D	Lognormal EF=10	A detailed multiple regression analysis was done using the plant test and maintenance motor operated valve responses to questions asked in NUREG-0737.[64]
Failure to Open	--	--	1E-4/D	Lognormal EF=3	ASEP used the IREP Procedures Guide Value.[7]
Failure to Remain Closed	--	--	1E-4/D	Lognormal EF=3	ASEP used the WASH-1400[39] value.
Check Value					
Failure to Open	6E-5/D to 1.2E-4/D	11, 39	1E-4/D	Lognormal EF=3	ASEP used the generic value from the IREP Procedures Guide.[7]
Failure to Close	--	--	1E-3/D	Lognormal EF=3	ASEP used the generic value from the IREP Procedures Guide.[7]

Table 8.2-5
Valve Failure Rates (Continued)

Component Failure Mode	Range from Other Sources	Data Sources	ASEP Mean Value	Distribution	Comments
Safety Relief Valves (SRVs) - BWR					
Failure to Open for Pressure Relief	--	--	1E-5/D	Lognormal EF=3	ASEP used the generic value from the IREP Procedures Guide.[7]
Failure to Open On Actuation	--	--	1E-2/D	Lognormal EF=3	The ASEP value is the NRC LER Data Summary[11] value. There are two types of failures included in the failure rate: 9E-3 valve hardware faults, 1E-3 valve control circuit command faults.
Failure to Reclose on Pressure Relief	--	--	1.6E-2/D	Lognormal EF=3	ASEP used the 3 stage Target Rock valve value from the Station Blackout Study.[27]
Relief Valve (Not SRV or PORV)					
Spurious Open	--	--	3.9E-6/hr	Lognormal EF=10	ASEP used the IEEE Guide[85] value.

Table 8.2-5
Valve Failure Rates (Concluded)

Component Failure Mode	Range from Other Sources	Data Sources	ASEP Mean Value	Distribution	Comments
Power Operated Reliefs Valves (PORVs) - PWR					
Failure to Open on Actuation	--	--	2E-3/D	Lognormal EF=3	The ASEP value is from the NRC LER Data Summary[11] for PWR air operated valves. There are two types of failure included in the failure rate: 1E-3 valve hardware faults, 2.8E-3 valve control circuit command faults.
Failure to Open For Pressure Relief	--	--	3E-4/D	Lognormal EF=10	ASEP used the generic value from the IREP Procedures Guide.[7]
Failure to Reclose	--	--	2E-3/D	Lognormal EF=3	The ASEP valve is from the NRC LER Data Summary[11] for air operated valves. There are two types of failures included in the failure rate: 1E-3 valve hardware faults, 1E-3 valve control circuit command faults.

Table 8.2-6
Pump Failure Rates

Component Failure Mode	Range from Other Sources	Data Sources	ASEP Mean Value	Distribution	Comments
<u>Motor Driven Pump</u>					
Failure to Start	5E-4/D to 1E-2/D	18, 31, 33, 39, 54, 55, 60, 61, 62, 63, 66	3E-3/D	Lognormal EF=10	The ASEP value is from the NRC LER Data Summary.[11] There are two types of failures included in the failure rate: 2.5E-3 pump circuit breaker command faults, 4E-4 pump hardware faults.
Failure to Run	1E-6/hr to 1E-3/hr	18, 31, 33, 39, 54, 55, 60, 61, 62, 63, 66	3E-5/hr	Lognormal EF=10	ASEP used the generic value from the IREP Procedures Guide.[7]
Unavailability Due to Test and Maintenance	1E-4/D to 1E-2/D	18, 31, 33, 39, 54, 55, 60, 61, 62, 63	2E-3/D	Lognormal EF=10	A detailed multiple regression analysis was done using the plant test and maintenance motor driven pump responses to questions asked in NUREG-0737.[64]

Table 8.2-6
Pump Failure Rates (Continued)

Component Failure Mode	Range from Other Sources	Data Sources	ASEP Mean Value	Distribution	Comments
<u>Turbine Driven Pumps</u>					
Failure to Start	5E-3/D to 9E-2/D	31, 33, 39, 55, 60	3E-2/D	Lognormal EF=10	ASEP used the generic value from the IREP Procedures Guide.[7] The BWR failure to start values from the NRC LER Data Summary[11] are essentially the same as the overall values. There are two types of failures included in the failure rate: 2E-2 pump circuit breaker command faults, 1E-2 pump hardware faults. For vender specific failure rates use the NRC LER Data Summary.
Failure to Run	8E-6/hr to 1E-3/hr	31, 33, 39, 55, 60	5E-3/hr	Lognormal EF=10	The failure rate is an updated value from the Peach Bottom analysis.[4]
Unavailability Due to Test and Maintenance	3E-3/D to 4E-2/D	31, 33, 34, 60	1E-2/D	Lognormal EF=10	A detailed multiple regression analysis was done using the plant test and maintenance turbine and diesel driven pump responses to questions asked in NUREG-0737.[64]

Table 8.2-6
Pump Failure Rates (Concluded)

Component Failure Mode	Range from Other Sources	Data Sources	ASEP Mean Value	Distribution	Comments
Diesel Driven Pump					
Failure to Start	1E-3/D to 1E-2/D	33, 39, 55, 61	3E-2/D	Lognormal EF-3	ASEP used the generic values from the NRC LER Data Summary.[11] There are two types of failures included in the failure rate: 2.7E-2 pump circuit breaker command faults, 3E-3 pump hardware faults.
Failure to Run	2E-5/hr to 1E-3/hr	11, 33, 39, 55, 61	8E-4/hr	Lognormal EF-10	The failure rate is an updated value from the Peach Bottom analysis.
Unavailability Due to Test and Maintenance	--	--	1E-2/D	Lognormal EF-10	A detailed multiple regression analysis was done using the plant test and maintenance turbine and diesel driven pump responses to questions asked in NUREG-0737.[64]

Table 8.2-7
Heat Exchanger Failure Rates

Component Failure Mode	Range from Other Sources	Data Sources	ASEP Mean Value	Distribution	Comments
Heat Exchanger					
Failure Due to Blockage	--	--	5.7E-6/hr	Lognormal EF-10	ASEP used the generic value from GE's LaSalle's PSA.[67]
Failure Due to Rupture (Leakage)	--	--	3E-6/hr	Lognormal EF-10	ASEP used the generic value from the IREP Procedures Guide.[7]
Unavailability Due to Test and Maintenance	--	--	3E-5/hr	Lognormal EF-10	ASEP used the generic value from RMIEP LaSalle PRA.[68]

Table 8.2-8
Electric Power Failure Rates

Component Failure Mode	Range from Other Sources	Data Sources	ASEP Mean Value	Distribution	Comments
AC Electric Power					
Diesel Generator (DG) Hardware Failure					
Failure to Start	8E-3/D to 1E-3/D	7, 8, 33, 39, 53, 56, 57, 69	3E-2/D	Lognormal EF=3	A thorough industry-wide analysis was performed in the Reliability of AC Power System Study (NUREG/CR-2989).[69] ASEP used the generic values from that study.
Failure to Run	2E-4/hr to 3E-3/hr	7, 8, 33, 39, 53, 56, 57, 69	2E-3/hr	Lognormal EF=10	
DG Test and Maintenance Unavailability	Neg 1. to 4E-2/D	7, 8, 33, 39, 53, 56, 57, 69	6E-3/D	Lognormal EF=10	A thorough industry-wide analysis was performed in the Reliability of AC Power System Study (NUREG/CR-2989).[69] ASEP used the generic values from that study.
Loss of Offsite Power (Other than Initiator)			2E-4	Lognormal EF=3	ASEP used the value calculated in a SNLA memo dated 6/22/87 to the NUREG-4550 Team Leaders from T. A. Wheeler.
AC Bus Hardware Failure	1E-8/hr to 4E-6/hr	7, 34	1E-7/hr	Lognormal EF=5	ASEP used the value from the NSAC Oconee Probabilistic Risk Assessment.[34]

Table 8.2-8
Electric Power Failure Rates (Continued)

Component Failure Mode	Range from Other Sources	Data Sources	ASEP Mean Value	Distribution	Comments
Circuit Breaker					
Spurious Open	--	39	1E-6/hr	Lognormal EF=3	ASEP used the values from WASH-1400[39] and IREP.[7]
Fail to Transfer	--	7	3E-3/D	Lognormal EF=10	
Time Delay Relay					
Fail to Transfer	--	7	3E-4/hr	Lognormal EF=10	ASEP used the IREP[7] value.
Transformer					
Short or Open	--	33	2E-6/hr	Lognormal EF=10	ASEP used the value from the Zion PRA.[33]

Table 8.2-8
Electric Power Failure Rates (Continued)

Component Failure Mode	Range from Other Sources	Data Sources	ASEP Mean Value	Distribution	Comments
DC Electric Power					
Hardware Failure	6E-10/hr to 1E-4/hr	7, 25, 27, 33, 34, 39, 46, 53, 56, 58, 65			
Bus			1E-7/hr	Lognormal EF-5	ASEP used the generic values from IEEE[41], IREP Procedures Guide,[7] RMIEP Screening data[75] and the NSAC Oconee Probabilistic Risk Assessment.[34] The ASEP value was typical for a range of values found in past studies.
Battery			1E-6/hr	Lognormal EF-3	
Charger			1E-6/hr	Lognormal EF-3	
Inverter			1E-4/hr	Lognormal EF-3	
Test and Maintenance Unavailability					
Battery	--	8, 53	1E-3/D	Lognormal EF-10	The ASEP value was based on an 8 hr/yr down time for maintenance from the DC Power Study (NUREG-0666)[25] which was divided by 8760 hr/yr for the per demand unavailability.

Table 8.2-8
Electric Power Failure Rates (Concluded)

Component Failure Mode	Range from Other Sources	Data Sources	ASEP Mean Value	Distribution	Comments
Bus	--	7, 53	8E-6/hr	Lognormal EF=10	ASEP used the failure rate from the Calvert Cliffs IREP[53] which included the contributions of bus and circuit breaker maintenance unavailability.
Charger	--	46	3E-4/D	Lognormal EF=10	ASEP used the generic value from the RMIEP screening data.[46]
Inverter	--	46	1E-3/D	Lognormal EF=10	ASEP used the generic value from the RMIEP screening Data.[46]

Table 8.2-9
Miscellaneous Failure Rates

Component Failure Mode	Range from Other Sources	Data Sources	ASEP Mean Value	Distribution	Comments
<u>Orifice</u>					
Failure Due to Plugging	--	--	3E-4/D	Lognormal EF=3	The ASEP value is from the IREP Procedures Guide.[7]
<u>Strainer</u>					
Failure Due to Plugging	--	--	3E-5/hr	Lognormal EF=10	The ASEP value is from the IREP Procedures Guide.[7]
<u>Sump</u>					
Failure Due to Plugging	--	--	5E-5/D	Lognormal EF=100	ASEP used the Zion PRA[33] value.
<u>Cooling Coil</u>					
Failure to Operate	--	--	1E-6/hr	Lognormal EF=3	ASEP used the IEEE Guide[65] value.
<u>Transmitter</u>					
Failure to Operate	--	--	1E-6/hr	Lognormal EF=3	ASEP used the IEEE Guide[65] value.

Table 8.2-9
Miscellaneous Failure Rates (Continued)

Component Failure Mode	Range from Other Sources	Data Sources	ASEP Mean Value	Distribution	Comments
<u>Fan (HVAC)</u>					
Failure to Start	--	--	3E-4/D	Lognormal EF=3	ASEP used the motor operated fan value from WASH-1400.[39]
Failure to Run	--	--	1E-5/hr	Lognormal EF=3	ASEP used the motor operated fan value from WASH-1400.[39]
Unavailability Due to Test and Maintenance	--	--	2E-3/D	Lognormal EF-10	A detailed multiple regression analysis was done using the plant test and maintenance motor driven pump responses to questions asked in NUREG-0737.[64]
<u>Instrumentation</u> (Includes Sensor, Transmitter and Process Switch)					
Failure to Operate	--	--	3E-6/hr	Lognormal EF-10	ASEP used the generic value from WASH-1400.[39]
<u>Temperature Switch</u>					
Failure to Transfer	--	--	1E-4/D	Lognormal EF=3	ASEP used the WASH-1400[39] pressure switch value.
<u>Transfer Switch</u>					
Failure to Transfer	--	--	1E-3/D	Lognormal EF=3	ASEP used the WASH-1400[39] circuit breaker value.

Table 8.2-9
Miscellaneous Failure Rates (Continued)

Component Failure Mode	Range from Other Sources	Data Sources	ASEP Mean Value	Distribution	Comments
Instrument Air Compressor					
Failure to Start	--	--	8E-2/D	Lognormal EF=3	ASEP used the generic value from the IEEE Guide.[65]
Failure to Run	--	--	2E-4/hr	Lognormal EF=10	ASEP used the IEEE Guide[65] value.
Unavailability Due to Test and Maintenance	--	--	2E-3/D	Lognormal EF=10	A detailed multiple regression analysis was done using the plant test and maintenance motor driven pump responses to questions asked in NUREG-0737.[64]
Flow Controller					
Failure to Operate	--	--	1E-4/D	Lognormal EF=3	ASEP used the pressure switch value from WASH-1400.[39]

Table 8.2-9
Miscellaneous Failure Rates (Concluded)

Component Failure Mode	Range from Other Sources	Data Sources	ASEP Mean Value	Distribution	Comments
<u>Cooling Tower Fan</u>					
Failure to Start	--	--	4E-3/D	Lognormal EF-3	ASEP used the IEEE Guide[65] value.
Failure to Run	--	--	7E-6/hr	Lognormal EF-10	The ASEP value is from the IEEE Guide.[65]
Unavailability Due to Test and Maintenance	--	--	2E-3/D	Lognormal EF-10	A detailed multiple regression analysis was done using the plant test and maintenance motor driven pump responses to questions asked in NUREG-0737.[64]
<u>Damper</u>					
Failure to Open	--	--	3E-3/D	Lognormal EF-10	ASEP used to IREP Procedures Guide[7] value.

Table 8.2-10
Operator Action Failure Rates

Non-Recovery of Component Failure	ASEP Mean Value	Distribution	Distribution Range	Comments
DG Hardware				
5-10 min.	1.0	--	--	The ASEP values are from the Station Blackout Study.[27]
10-20 min.	1.0	--	--	
20-30 min.	1.0	--	--	
30-40 min.	1.0	--	--	
40-60 min.	0.9	Maximum Entropy	.09-1.0	
60-70 min.	0.9	Maximum Entropy	.09-1.0	
70-120 min.	0.9	Maximum Entropy	.09-1.0	
2-4 hrs.	0.8	Maximum Entropy	.08-1.0	
4-6 hrs.	0.7	Maximum Entropy	.07-1.0	
6-8 hrs.	0.6	Maximum Entropy	.06-1.0	
8-12 hrs.	0.5	Maximum Entropy	.05-1.0	
24 hrs.	0.2	Maximum Entropy	.02-1.0	
DG Test and Maintenance				
5-10 min.	1.0	--	--	The ASEP values are from the Station Blackout Study.[27]
10-20 min.	1.0	--	--	
20-30 min.	1.0	--	--	
30-40 min.	1.0	--	--	
40-60 min.	0.9	Maximum Entropy	.09-1.0	
60-70 min.	0.9	Maximum Entropy	.09-1.0	
70-120 min.	0.9	Maximum Entropy	.09-1.0	
2-4 hrs.	0.8	Maximum Entropy	.08-1.0	
4-6 hrs.	0.7	Maximum Entropy	.07-1.0	
6-8 hrs.	0.7	Maximum Entropy	.07-1.0	
8-12 hrs.	0.5	Maximum Entropy	.05-1.0	
24 hrs.	0.1	Maximum Entropy	.01-1.0	

Table 8.2-10
Operator Action Failure Rates (Continued)

Non-Recovery of Component Failure	ASEP Mean Value	Distribution	Distribution Range	Comments
DG Actuation				
5-10 min.	--	--	--	The ASEP values are from engineering judgment.
10-20 min.	--	--	--	
20-30 min.	--	--	--	
30-40 min.	0.04	Maximum Entropy	.004-.4	
40-60 min.	0.04	Maximum Entropy	.004-.4	
60-70 min.	0.04	Maximum Entropy	.004-.4	
70-120 min.	0.03	Maximum Entropy	.003-.3	
2-4 hrs.	0.03	Maximum Entropy	.003-.3	
4-6 hrs.	0.03	Maximum Entropy	.003-.3	
6-8 hrs.	0.03	Maximum Entropy	.003-.3	
8-12 hrs.	0.03	Maximum Entropy	.003-.3	
24 hrs.	0.001	Maximum Entropy	.0001-.01	
DG Common Mode				
5-10 min.	1.0	--	--	The ASEP values are from the Station Blackout Study.[27]
10-20 min.	1.0	--	--	
20-30 min.	1.0	--	--	
30-40 min.	1.0	--	--	
40-60 min.	0.9	Maximum Entropy	.09-1.0	
60-70 min.	0.9	Maximum Entropy	.09-1.0	
70-120 min.	0.8	Maximum Entropy	.08-1.0	
2-4 hrs.	0.7	Maximum Entropy	.07-1.0	
4-6 hrs.	0.6	Maximum Entropy	.06-1.0	
6-8 hrs.	0.5	Maximum Entropy	.05-1.0	
8-12 hrs.	0.3	Maximum Entropy	.03-1.0	
24 hrs.	0.1	Maximum Entropy	.01-1.0	

Table 8.2-10
Operator Action Failure Rates (Continued)

Non-Recovery of Component Failure	ASEP Mean Value	Distribution	Distribution Range	Comments
DC Hardware				
5-10 min.	0.9	Maximum Entropy	.09-1.0	The ASEP values are from the Station Blackout Study.[27]
10-20 min.	0.9	Maximum Entropy	.09-1.0	
20-30 min.	0.8	Maximum Entropy	.08-1.0	
30-40 min.	0.7	Maximum Entropy	.07-1.0	
40-60 min.	0.6	Maximum Entropy	.06-1.0	
60-70 min.	0.6	Maximum Entropy	.06-1.0	
70-120 min.	0.4	Maximum Entropy	.04-1.0	
2-4 hrs.	0.1	Maximum Entropy	.01-1.0	
4-6 hrs.	0.05	Maximum Entropy	.005-.5	
6-8 hrs.	0.01	Maximum Entropy	.001-.1	
8-12 hrs.	0.002	Maximum Entropy	.0002-.02	
24 hrs.	0.001	Maximum Entropy	.0001-.01	
DC Common Mode				
5-10 min.	1.0	--	--	The ASEP values are from the Station Blackout Study.[27]
10-20 min.	1.0	--	--	
20-30 min.	1.0	--	--	
30-40 min.	1.0	--	--	
40-60 min.	1.0	--	--	
60-70 min.	0.9	Maximum Entropy	.09-1.0	
70-120 min.	0.9	Maximum Entropy	.09-1.0	
2-4 hrs.	0.8	Maximum Entropy	.08-1.0	
4-6 hrs.	0.7	Maximum Entropy	.07-1.0	
6-8 hrs.	0.6	Maximum Entropy	.06-1.0	
8-12 hrs.	0.5	Maximum Entropy	.05-1.0	
24 hrs.	0.2	Maximum Entropy	.02-1.0	

Table 8.2-10
Operator Action Failure Rates (Concluded)

Non-Recovery of Component Failure	ASEP Mean Value	Distribution	Distribution Range	Comments
Loss of Offsite Power (LOSP)				
5 min - 24 hrs.	--	--		The ASEP values are from the site specific data curve, see Figure 7.2-4 for example.
Power Conversion System (PCS)				
5-10 min.	1.0	--	--	The ASEP values are a cubic spline fit on the data for the power conversion system non-recovery values in NUREG-0666.[25]
10-20 min.	1.0	--	--	
20-30 min.	1.0	--	--	
30-40 min.	0.9	Maximum Entropy	.09-1.0	
40-60 min.	0.6	Maximum Entropy	.06-1.0	
60-70 min.	0.4	Maximum Entropy	.04-1.0	
70-120 min.	0.06	Maximum Entropy	.006-.6	
2-4 hrs.	0.06	Maximum Entropy	.006-.6	
24 hrs.	0.0007	Maximum Entropy	.00007-.007	

9. EXPERT JUDGMENT ANALYSIS

The use of expert judgment elicitation is an integral part of the methodology used in the Probabilistic Risk Assessments (PRAs) supporting NUREG-1150. Expert judgment is used where applicable experimental data or complete analyses are unavailable. Situations such as this are common in the analysis of unusual and rare events. The expert judgment process can address highly formalized quantitative issues such as the probability distributions of specific events, or it may be used to resolve more general judgments commonly made in PRA, such as how operator recovery should be included in the accident sequence models.

Expert judgments are expressions of opinion, based on knowledge and experience, that experts make in responding to technical problems. Specifically, the judgments represent the experts' state of knowledge at the time of response to the technical question. Expert judgment is not restricted to the experts' answer, but also includes the experts' thought processes (definitions, assumptions, and algorithms) for arriving at answers.

Expert judgment is frequently needed in risk assessment, especially when the following circumstances exist:

- No other data for answering the technical problem or issue are available;
- High variability characterizes the data;
- Experts question the applicability of the data;
- Existing data needs to be supplemented, interpreted, or incorporated with model or code calculations; or
- Analysts need to establish the state of knowledge about what is currently known, what is not known, and what is worth learning.

Expert judgment is of necessity used in all technical fields. Because these judgments are often implicit, they are sometimes not acknowledged as being expert judgments. For example, expert judgment is frequently used implicitly, even unconsciously, when analysts make decisions about defining problems, establishing boundary conditions, or screening data. By contrast, expert judgment is also obtained explicitly through formal processes.

Expert judgment in risk assessment needs to be explicit rather than implicit. To this end, a formal expert judgment elicitation process ensures that the expert judgment is properly documented. Although the explicit approach requires more effort, it offers several advantages. First, the explicit approach can provide the expert with aids to process the magnitude of information associated with complex technical questions. For example, issues can be broken into logical parts that can be more easily considered. Second, the explicit process is more likely than its implicit counterpart to use the body of research on human cognition and communication. This practice usually enhances the quality of the expressed judgments. Third, the procedures of the explicit approach provide a record of the experts' judgments, and of their reasoning in arriving at these judgments. This documented record allows the judgments obtained by the explicit process to be more easily updated as new information becomes available. Fourth, people other than those immediately involved can scrutinize the explicit process and its results. With the implicit approach, there is little to review and, indeed, reviews are not often done. Thus, the explicit approach is more likely to advance through the process of reviews.

9.1 Expert Judgment Assumptions and Limitations

The expert judgment process requires considerable commitment in time, human resources, and funding. Even then, the process cannot necessarily address all issues which are candidates for expert judgment. The required time and cost of putting every issue to a formal expert judgment process would most likely be prohibitive.

The NUREG/CR-4550 expert judgment process initially considered a set of approximately fifty issues. A set of ten issues were selected for the formal process. The screening criterion was to select for the expert judgment process those issues deemed potentially most significant to risk. The expert panel reviewed the issues which were selected for the process and those screened from the process. The panel was permitted to recommend that issues screened from the process be included for expert judgment. In this manner, the panel had input to the selection process.

The remaining issues not selected for the formal expert judgment process were subjected to another screening for consideration in a less formal expert judgment process. This less formal process was conducted by the NUREG/CR-4550 staff, using the staff as the expert panel which analyzed these issues. Nine issues, which had been screened from the formal process, were investigated by the staff in the less formal process. Even though the less formal process did not allow for as broad a range of expertise and experience in the analysis of these nine issues, the process was still an explicit experience in expert judgment and, as such, yields the advantages of an explicit process discussed above.

Those issues not selected for either the formal or less formal expert judgment process were either deemed sufficiently insignificant to risk to warrant implicit expert judgment or had been resolved by new analyses or information.

9.2 Expert Judgment Development

The development and implementation of an expert judgment process is a significant undertaking, the detailed description of which far exceeds the scope of this document. The methodology, the issues reviewed, and the resulting resolutions of those issues in the NUREG/CR-4550 analysis are documented in detail in NUREG/CR-4550, Volume 2 [70]. The reader should refer to that document for an in-depth discussion on the steps of an expert judgment process. The process is outlined briefly below and illustrated in Figure 9.2-1.

Step 9.1. Select Issues

The initial selection of issues for inclusion in the expert judgment process is made by the plant leaders for the front-end analyses in cooperation with the project management staff. The expert panel participates as well by reviewing the initial list of issues selected for elicitation and issues screened from elicitation. The panel is allowed to recommend changes to the list of issues selected for elicitation.

Step 9.2. Select Experts

Experts are chosen to ensure a balance of viewpoints. To this end, experts from industry groups, engineering and consulting firms, the Federal Government, and the national laboratories can be included in the panel.

Step 9.3. Train for Elicitation

Training in probability assessment is the first scheduled activity for the expert panel. The purpose of this training is to help the experts become better able to encode their knowledge and beliefs into a form that can be incorporated into PRA models. Training includes informing the experts about the methods that will be used to process and propagate their subjective beliefs, introduction to the assessment tools and practice with these tools, calibration training using almanac questions, and an introduction to the psychological aspects of probability elicitation.

Step 9.4. Present and Review Issues

The second major activity of the expert panel involves presentations of the issues made by the plant analysts to the expert panel. The purposes of the presentations are to ensure that there exists a common understanding of the issues being addressed, ensure that all of the experts are responding to the same elicitation question; permit the exclusion of issues thought to be unimportant and the addition of issues thought to be important; allow modification of the issues or decomposition of the issues; and provide a forum for the discussion of alternative data sources, models, and forms of analysis.

Step 9.5. Discuss Analyses

The actual time needed to prepare for the elicitations depends on the work load of the project staff, the panel members and the success of Step 9.4. Certain issue decompositions may need to be altered because of comments in Step 9.4. These issues need to be prepared and sent out to the panel members before the elicitation meeting. It is suggested that the elicitation meetings not be held too soon after Step 9.4.

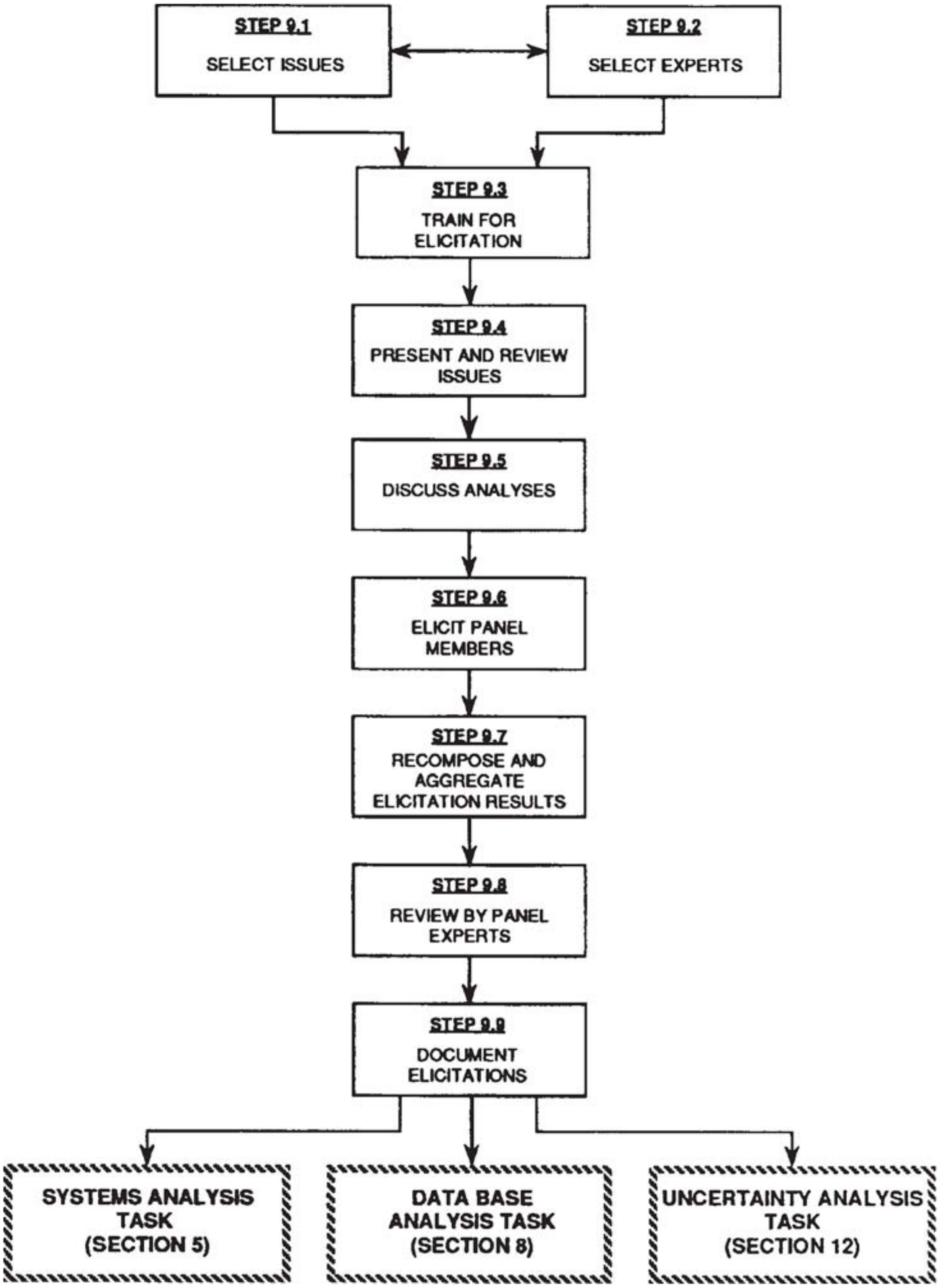


Figure 9.2-1. Step Relationship for Expert Judgment Elicitation

Some experts may choose to alter the proposed decompositions or create new decompositions and make preliminary decompositions of the issues. The elicitation meeting provides a forum for discussion of alternative views of the issue. Presentations from both the panel members and invited observers to the meetings are encouraged. These sessions can generate a substantial amount of discussion and interchange of information which often lead the experts to make revisions of their prepared analyses. In some instances in the NUREG/CR-4550 process, panel members prepared documentation that amounted to brief reports. It became apparent in the elicitation sessions that this interchange was an important source of information for the experts.

Step 9.6. Elicit Panel Members

The discussion of each issue is followed by elicitation meetings between each expert and a team composed of one normative analyst and one substantive analyst. A normative analyst is one who is expert in the field of probability assessment and decision analysis. A substantive expert is one who is knowledgeable of the problem area. The experts' assumptions and reasoning are produced during the elicitation meetings.

Step 9.7. Recompose and Aggregate Elicitation Results

Recomposition of the subjective probability distributions for each expert may be accomplished by the normative and substantive analysts using decision analysis methods implemented through computer programs. While the experts may have employed different decompositions, the end result for the aggregated issue resolutions incorporated each experts' beliefs with equal weight.

Step 9.8. Review by Panel Experts

Following the recomposition of the assessments, the written analyses of each issue are returned to each panel expert, normative expert, and substantive expert associated with the issue for review. This review process ensures that potential misunderstandings are identified and resolved and that the documentation correctly reflects the judgment of the experts involved.

Step 9.9. Document Elicitations

Clear, comprehensive documentation is crucial for ensuring that the expert judgment process is accepted as credible. There must be no question as to the openness and impartiality of the process. Users and reviewers of the results must be able to trace the development of aggregated assessments from the information presented to the experts, to the rationale which motivates each expert to generate his particular assessments, and through the process of aggregating the individual assessments into a final result, including any manipulation of the assessments needed for aggregation.

10. ACCIDENT SEQUENCE QUANTIFICATION ANALYSIS

This section describes the process of quantifying the point estimate of the core damage frequency and determining the minimal cut sets.

10.1 Accident Sequence Quantification Assumptions and Limitations

The Set Equation Transformation System[71] (SETS) computer program which achieves the symbolic manipulation of Boolean equations was used to perform the accident sequence quantification for the NUREG/CR-4550 analysis. The SETS code accepts input in the form of fault trees, Boolean equations, and point values. Fault tree models were developed for the various plant front-line and support systems and probability estimates obtained for each primary event associated with these system fault trees. These fault trees were combined, converted into Boolean equation representations, and the equations solved and quantified to obtain minimal cut sets for each of the front-line systems. The minimal cut sets for the front-line systems were then appropriately combined to determine the minimal cut sets for the accident sequences. Truncation based on probability was performed in obtaining the minimal cut sets for the systems and accident sequences. This is usually done during Probabilistic Risk Assessments (PRAs) to reduce the number of cut sets to a manageable level. In general, sequence cut sets whose probabilities (without the initiator frequency or recovery) are less than the truncation value are screened during formation of the initial partial sequence expressions. Since all initiator frequencies are less than 1.0 per year except for a few categories of transients, and since recovery actions are yet to be considered, it is likely that all sequence frequencies greater than the truncation value are identified. Therefore, the major portion of the cut sets contributing to core damage frequency can be be retained if the truncation level is selected properly.

Contrasting with the above assurances that the truncation step does not lose important cut sets, is the fact that the number of cut sets less then 1E-8 is not known. For example, if thousands of 1E-9 value cut sets are screened out, the potential for a missed 1E-6 sequence frequency exists. While this is a limitation of the analysis process, it should be noted that many of the recovery actions applicable to cut sets above 1E-8 are likely to be applicable to cut sets below that value as well. This fact provides reasonable assurance that the discarded cut sets would not add significantly to the final results and that major sequences are not missed.

In the development of the system fault tree, a system or component being unavailable on demand because it is out for test or maintenance was modeled. However, it is assumed in this methodology that the operators do not violate the technical specifications (or the "Limiting Conditions of Operation") in testing or maintaining a system or component. Therefore, "double test and maintenance" failures were not allowed to occur. These types of failures do not appear until the quantification task. Cut sets with these types of failures were deleted.

10.2 Accident Sequence Quantification Development

Each of the accident frequencies are defined by a sum of minimal cut sets. A minimal cut set is the combination of faults representing the minimum number of basic faults necessary for the sequence to occur. In performing the quantification, the analyst (1) links the appropriate fault trees identified by the top events of the accident sequences, (2) applies the appropriate recovery actions for each cut set, and (3) then quantifies the complete sequence. This process is performed in several steps as illustrated in Figure 10.2-1 and described below.

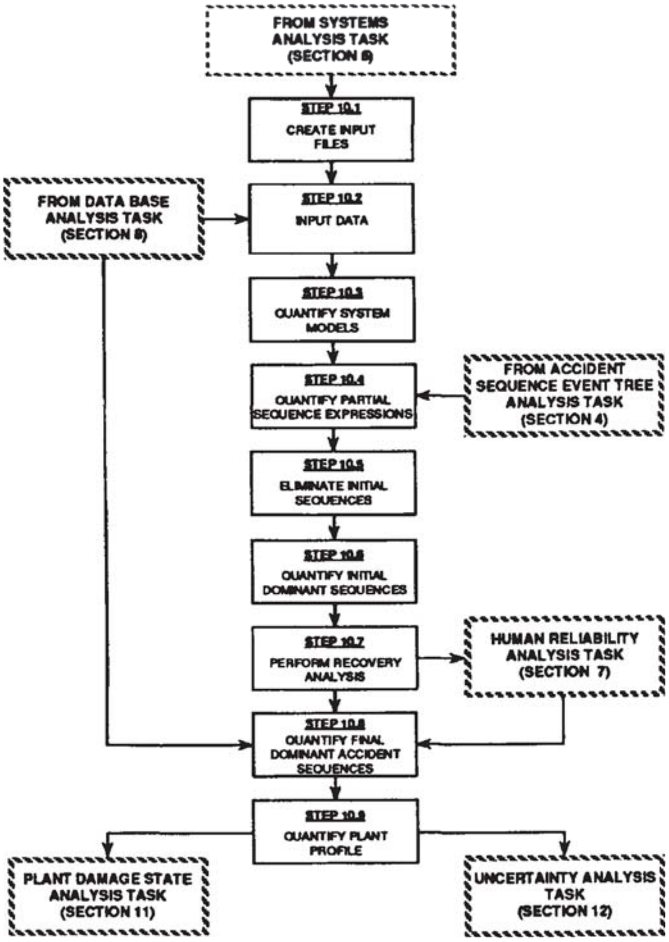

FROM SYSTEMS ANALYSIS TASK (SECTION 6)
STEP 10.1
CREATE INPUT FILES
FROM DATA BASE ANALYSIS TASK (SECTION 8)
STEP 10.2
INPUT DATA
STEP 10.3
QUANTIFY SYSTEM MODELS
STEP 10.4
QUANTIFY PARTIAL SEQUENCE EXPRESSIONS
FROM ACCIDENT SEQUENCE EVENT TREE ANALYSIS TASK (SECTION 4)
STEP 10.5
ELIMINATE INITIAL SEQUENCES
STEP 10.6
QUANTIFY INITIAL DOMINANT SEQUENCES
STEP 10.7
PERFORM RECOVERY ANALYSIS
HUMAN RELIABILITY ANALYSIS TASK (SECTION 7)
STEP 10.8
QUANTIFY FINAL DOMINANT ACCIDENT SEQUENCES
STEP 10.9
QUANTIFY PLANT PROFILE
PLANT DAMAGE STATE ANALYSIS TASK (SECTION 11)
UNCERTAINTY ANALYSIS TASK (SECTION 12)

Figure 10.2-1. Step Relationship for Accident Sequence Quantification Analysis

Step 10.1. Create Input Files

The data must first be prepared in the appropriate format for inputting into the computer. This data consists of fault trees for all the front-line and support systems and probability point estimates for each of the primary events that appear in the fault trees. The point estimates used in the initial phase of the analysis should represent the largest value needed for any sequence evaluation. This ensures that no cut set involving that variable will be lost due to the truncation process. The data are obtained from the Dependent and Subtle Failures Analysis task (see Section 6), the Human Reliability Analysis task (see Section 7), and the Data Base Analysis task (see Section 8). Combinations of human errors are kept from being truncated during the initial phase of the analysis by use of high screening values. Additional point value data for sequence evaluation and recovery actions are prepared and entered in later stages of the analysis as required.

Step 10.2. Input Data

The fault trees and point estimate data files created in Step 10.1 are input into the computer using the SETS code. A SETS user program is constructed using the SETS command language to input the fault trees and the point value estimates associated with the primary events. This user program also combines the front-line system fault trees with their support system fault trees to define integrated front-line system fault trees.

Step 10.3. Quantity System Models

The minimal cut sets for each of the integrated front-line system models is then determined using SETS. Detailed descriptions for preparing SETS user code to perform accident sequences are found in "A SETS User's Manual for Accident Sequence Analysis."[71] The reader should refer to Reference 71 for examples and instruction on preparation of the SETS user code needed for all the steps outlined in Section 10.2. The quantified minimal cut sets for each of the systems are reviewed for accuracy and consistency as part of the quality assurance check.

Step 10.4. Quantify Partial Sequence Expressions

In this methodology the analyst quantifies an initial portion of the accident sequence. This quantification of the accident sequences is performed in a step-by-step approach until whole sequences (where necessary) are quantified.

In this step the front-line system minimal cut sets are combined to form portions of the entire accident sequence. Success states of systems (where identified by the accident sequence) are also accounted for in deriving these partial sequence Boolean expressions. For example, when a system that contains a success state is combined with a system or systems that have the same state but it is a failure, the failure state must be eliminated. Mean data values are applied to the basic events in these Boolean expressions. The accident sequences are initially quantified only to the point where (1) core damage occurs because of early loss of cooling, or (2) containment heat removal fails resulting in a core vulnerable situation. At this point in the quantification process, initiator frequencies and recovery actions are not yet included. The cut sets are truncated at a lower level than the accident sequences.

Step 10.5. Eliminate Initial Sequences

In this step the analyst eliminates the first set of non-dominant accident sequences. If the frequency of the partial sequence is below the chosen screening value (e.g, 1E-8), the sequence is eliminated from further quantification. In effect if any of the additional system failures required for core damage occur with a probability of 1.0, and the initiator frequency is included, a sequence core damage frequency of less than the screening value will result. The partial sequences with a frequency of greater than or equal to the screening value are retained for further evaluation.

Step 10.6. Quantify Initial Dominant Sequences

In this step the analyst quantifies the entire expression of the accident sequences retained in Step 10.5. This process is actually performed in several steps. First, the initiator event is included in the accident sequence expression. The human errors are examined and set to their nominal values where appropriate, accounting for dependencies. Next, the full sequence expression is quantified. Third, the cut sets are reviewed and any illogical cut sets are deleted. For example, double test and maintenance is assumed not to occur. Any cut set with this type of failure is deleted. Last, if the frequency of any of the accident sequences is below the screening value, the sequence is eliminated. The sequences retained are the initial dominant sequences.

Step 10.7. Perform Recovery Analysis

In this step the analyst incorporates recovery to the initial dominant sequences. The cut sets of each sequence retained in Step 10.6 are reviewed for potential recovery actions. This process is performed as part of the Human Reliability Analysis task. The reader should refer to Steps 7.10 through 7.28 in Section 7. Once the appropriate recovery actions have been identified for each cut set, an appropriate non-recovery term is added to the cut set.

Step 10.8. Quantify Final Dominant Accident Sequences

In this step the analyst requantifies the accident sequences with the recovery included. These sequences with frequencies below the screening value are eliminated from further evaluation. The sequences with frequencies equal to or greater than the screening value are the final dominant sequences. These are the sequences which form the plant profile. In addition, these sequences form the plant damage states (see Section 11) and will be quantified in the Uncertainty Analysis (see Section 12).

Step 10.9. Quantify Plant Profile

In this step the analyst quantifies the core damage frequency for the plant. The cut sets of the dominant accident sequences are combined into one Boolean expression and quantified. This expression represents the core damage profile for the entire plant.

10.3 Accident Sequence Quantification Recommended Reporting

The reporting of the quantification of the accident sequences is perhaps one of the most important sections of the analysis. In a PRA, there are generally hundreds of potential accident sequences. But typically, only a dozen or so contribute significantly to the core damage frequency. The rationale for eliminating sequences is discussed in in this section. The following information should be reported:

- Assumptions. Any assumption used in the quantification process are discussed.

- Initial Sequence Quantification. Each accident sequence is discussed and the following information is provided: (1) the sequence core damage frequency, (2) the amount of the expression quantified, (3) whether the sequence was eliminated and the rationale, and (4) any then appropriate comments.

- Application of Recovery. The recovery actions applied to each initial dominant accident sequence are listed.

- Final Sequence Quantification. Each initial dominant accident sequence is discussed giving the following information: (1) the frequency before recovery, (2) the frequency after recovery (i.e., identifying the initial dominant sequences which also result in the final dominant sequences), (3) whether the sequence was eliminated and the rationale, and (4) any other appropriate comments.

11. PLANT DAMAGE STATE ANALYSIS

In the Level 1 portion of a Probabilistic Risk Assessment (PRA), the accident sequences, total core damage frequency, and insights derived from the results complete the analysis. When a Level 2 or Level 3 analysis is to be performed, the interface between the system analysis results and the necessary input to the accident progression event tree must be defined. This interface is described by plant damage states.

The methods and example described in this section are related directly to the Peach Bottom front-end to back-end interface. There were significant interface differences between the four plants analyzed in NUREG-1150, in particular between the PWRs and BWRs. A major difference was that there were more "feedback loops" between the back-end and front-end analysis in Peach Bottom due to potential safety system vulnerabilities to the reactor building environment. Also, the interface for Peach Bottom was handled more rigorously than for the other three plants.

A plant damage state (PDS) is a grouping of accident sequence cut sets that have similar characteristics such as vessel pressure, timing, and system availability. Thus, the same containment response and radiological consequences are expected from all of the cut sets in a given plant damage state. The PDSs are needed by the back-end analyst to determine the accident progression, containment response, and subsequent risk to the public.

While the delineation of the PDSs is not a long or complex task, it is essential to the interface between the front-end and back-end analyses. It is also the most significant interaction between the analysts of these two portions of a PRA. This task should begin long before the front-end results are completed to optimize the plant damage state definitions; however, it can be done after the fact if necessary. There is a degree of flexibility based upon the amount of system analysis that the Level 2 analyst is willing to incorporate into the accident progression event tree. If the interface is established early in the front-end analysis, the systems included in the sequence event trees can be modified and the structure adjusted to accommodate many of the questions that will have to be addressed to establish the plant damage states.

11.1 Plant Damage State Assumptions and Limitations

There are some constraints associated with the development of the plant damage states. First, it is possible for the back-end analyst to ask for information on plant conditions that are not provided explicitly by the front-end analysis. When this occurs, the analyst should pose a question (or questions) that will elicit the desired information and which can be directly answered. If this cannot be done, then the analysts jointly define the appropriate assumptions for the remaining analysis. Second, the back-end analyst may ask questions which could be answered by the front-end analysis but, because of the number of questions and the very large number of individual cut sets involved, it is impractical to do so for every cut set. In this case, the front-end analyst groups similar cut sets for which the effect upon the subsequent accident progression analysis is comparable. In performing a plant damage state analysis, the analysts must ensure that the effects of any limitations are clearly delineated and understood.

11.2 Plant Damage State Analysis Development

In this task, the plant damage states (PDSs) are defined, accident sequences are assigned to PDSs (as are individual cut sets when it is necessary to subdivide sequences), and the PDSs are quantified. This definition and quantification process involves several steps that are illustrated in Figure 11.2-1 and described below.

Step 11.1. Identify Accident Progression Questions

Questions about system and physical parameters at the onset of core damage are developed by the back-end analysts to provide the systems and phenomenological boundary conditions that influence the accident progression. These questions provide the interface between the front-end and accident progression analyses. Because these questions (approximately 10 to 30) make up the initial portion of the accident progression event tree (APET), they must be generated by the back-end analyst. The answers to these APET questions are provided by the resolution of the PDS questions. These PDS questions can be answered by system conditions, such as whether or not a system fails, and the physical parameters that can be determined by the state of all the safety and non-safety systems at specified times in the accident sequence. The plant damage state questions can be ordered according to timing and dependencies. For example, a question regarding station blackout would follow a question about loss of offsite power. Likewise, the availability of low pressure systems would come after establishing whether or not the reactor coolant system is depressurized. Also, the need for additional system models can be evaluated. This is primarily a back-end task, but the front-end analyst must be involved to ensure that the questions being posed can, in fact, be answered by the analysis results. In some instances it is necessary and appropriate to proportion a PDS among the various contributing subsets of conditions. This is done by the use of split fractions. These split fractions are the probability of answers to particular questions in the accident progression event trees. The calculation of split fractions is discussed further in Step 11.7.

Step 11.2. Determine Potential Answers

The front-end analyst determines the potential answers to the questions identified in Step 11.1 working closely with the back-end analyst. The way a question is answered may result in a different PDS. The back-end analyst might require more than a yes/no resolution. For example, one question might be 'Is the reactor at high pressure?' It would appear that the only possible answers are either yes or no. However, the real question may be: 'Is the reactor at high pressure, and if so, can the reactor be depressurized?'

The answers to each question relate to the accident sequences and the associated cut sets. A single answer to a question for an entire

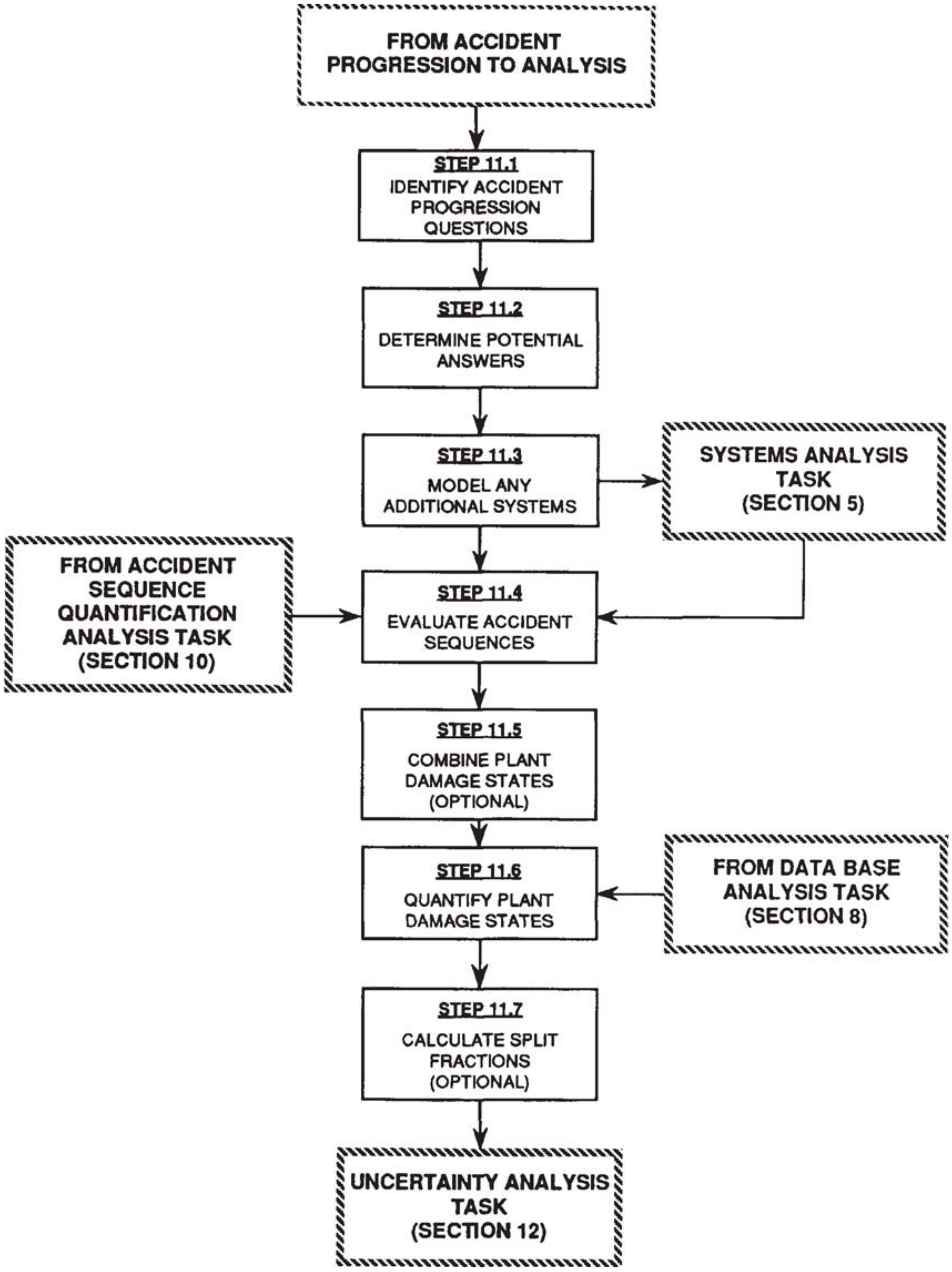

FROM ACCIDENT PROGRESSION TO ANALYSIS
STEP 11.1
IDENTIFY ACCIDENT PROGRESSION QUESTIONS
STEP 11.2
DETERMINE POTENTIAL ANSWERS
STEP 11.3
MODEL ANY ADDITIONAL SYSTEMS
SYSTEMS ANALYSIS TASK (SECTION 5)
FROM ACCIDENT SEQUENCE QUANTIFICATION ANALYSIS TASK (SECTION 10)
STEP 11.4
EVALUATE ACCIDENT SEQUENCES
STEP 11.5
COMBINE PLANT DAMAGE STATES (OPTIONAL)
STEP 11.6
QUANTIFY PLANT DAMAGE STATES
FROM DATA BASE ANALYSIS TASK (SECTION 8)
STEP 11.7
CALCULATE SPLIT FRACTIONS (OPTIONAL)
UNCERTAINTY ANALYSIS TASK (SECTION 12)

Figure 11.2-1. Step Relationship for Plant Damage State Analysis

sequence may not be possible because of the differences delineated by its cut sets. In view of the earlier real question, one possible answer for a particular case could be 'It is at low pressure,' because that accident sequence is one where depressurization was accomplished. In addition to the sequence definition, the cut sets can determine the answer. Using the same question again, the sequence definition in another instance does not address the issue of depressurization. However, the cut set failures are such that depressurization is impossible under any circumstances. One possible answer is, 'The reactor is at high pressure'. Therefore, in determining the possible answers, the sequences and the cut sets must be evaluated.

Step 11.3. Model Any Additional Systems

The analyst identifies and models any additional systems that have to be analyzed. The answers to questions identified earlier might involve systems that had no effect on the front-end analysis and therefore were not modeled initially. These systems now require some type of evaluation. This evaluation may require a detailed model or a very simplistic model. The complexity of the model should be adequate to answer the back-end questions.

Step 11.4. Evaluate Accident Sequences

Theoretically, the set of questions that define a plant damage state must be answered for every cut set of every accident sequence resulting from the front-end analysis. In actual practice, the answers are often identical for all the cut sets in a particular accident sequence. However, sometimes one or more cut sets from an accident sequence are sufficiently different from the others that they fall into a different plant damage state. When scanning the cut sets from an accident sequence analysis, patterns of failures often emerge. This can allow an analyst to recognize that large groups of cut sets will all go into the same plant damage state without having to methodically apply the questions to each cut set individually. The end result of this step in the analyses is a table of accident sequences (and the applicable cut sets if an accident sequence is split between plant damage states) tabulated against the appropriate plant damage state.

Step 11.5. Combine Plant Damage States (Optional)

In general, a separate accident progression event tree calculation is required for each PDS. Because these calculations are time-consuming and complex, it is often desirable to reduce the total number of PDSs by grouping them. The number of possible plant damage states can be very large but, in practice, the actual number usually is on the order of a few dozen. For efficiency in the back-end calculations, the number of plant damage states should be reduced to between 5 and 15. Given the list of accident sequence cut sets with their corresponding plant damage states from Step 11.4, it is a straightforward matter to sort the cut sets by plant damage state. Each PDS will include one or more cut sets from one or more accident sequences. Interim PDSs can be combined whenever a particular question can be incorporated directly into the accident progression event tree as opposed to being part of the PDS definition. For example, one question may concern the success or failure of the Automatic Depressurization System (ADS) in a BWR. If that is the only difference between two PDSs, then they can be combined and a new PDS formed. When the task is completed one would expect to have approximately ten or less plant damage states. NOTE: For convenience in reporting, the initially regrouped list may be referred to as "interim PDSs" (or PDSs) and the last list as the "final PDSs" (or PDS groups). Section 11.3 discusses an approach to nomenclature for handling these collections of PDSs.

Step 11.6. Quantify Plant Damage States

In this step the analyst quantifies the plant damage states. In order to do this, the failures (i.e., cut sets) comprising each PDS are grouped together into one Boolean equation which is the sum of all the cut sets in that PDS. This Boolean equation is then quantified using event frequencies from the data base and the cut set files generated earlier. The frequency of each PDS is calculated just as it was for the accident sequences. In the NUREG/CR-4550 analyses, the TEMAC code[73] was used to perform the quantification. Therefore, the output of the quantification process is a set of statistics and core damage risk measures identical to that obtained on each accident sequence.

Step 11.7. Calculate Split Fractions (Optional)

In Step 11.1 the front-end and back-end analysts jointly identified the questions to be included in the PDS definitions. At that time the decision may be made to incorporate some of the potential questions into the accident progression event tree instead of being part of the PDS definition. These decisions are sometimes made for computational convenience in the overall Level 3 PRA process. Also, the accident progression event tree is usually still evolving during this time, and the questions may arise after the PDS analysis is largely complete. Therefore, it is sometimes easier to incorporate a new question into the accident progression event tree than to redo a significant portion of the PDS analysis.

While PDS-type questions may be incorporated into the accident progression event tree, it remains the responsibility of the front-end analysts to provide the quantification of these questions. Generally, this quantification is provided in the form of split fractions that are assigned to the possible outcomes of the questions. For example, suppose that a particular plant damage state includes some cut sets with ADS success and others with ADS failure and that the accident progression analysis requires that these two groups of cut sets be treated separately in the accident progression event tree. The analyst will sort the cut sets and determine the fraction of the time that ADS has failed in that plant damage state. These split fractions are provided to the back-end analyst along with the PDS frequency for input to the accident progression event tree. In many cases split fractions are needed for questions with more than two possible outcomes.

When performing the uncertainty analysis discussed in Section 12 in support of the integrated Level 3 uncertainty analysis, a Monte Carlo sample for each split fraction is generated (i.e., if 100 observations are used in the uncertainty analysis, 100 values will be generated for each split fraction). This is necessary because the split fractions are determined by the relative cut set frequencies which change for each sample member. This is very important and should not be overlooked by the analysis team.

11.3 Plant Damage State Nomenclature

Plant damage states can be numbered for referencing, but it is useful to have an abbreviated damage state identifier assigned to each cut set in order to summarize and communicate the information efficiently.

One approach is to number the questions (branches in the accident progression event tree) and the answers to each question. If this approach is used it is helpful to let the same number represent the same (or similar) outcome in each set of answers (e.g., 1 for failure, 2 for available if power restored, 3 for success). It is also useful to group the responses by function or system. Using such a pattern, each sequence (or cut set) then has associated with it a numerical identifier which uniquely describes the resolution of the questions for that sequence.

In the Peach Bottom analysis there were 16 questions (see Table 11.5-1) which were placed in seven groups. The seven groups are: initiating event (1 question), electric power (3 questions), stuck open relief valve (1 question), high pressure systems (2 questions), ADS-RCS depressurization (1 question), low pressure and DHR systems (5 questions), and venting and containment isolation (3 questions). An example of an identifier for a Peach Bottom plant damage state would be 4-211-2-12-1-22222-122. The initiating event group is the first character of the identifier. The 4 indicates that the initiating event is a transient; see Table 11.5-1, question 1, answer 4. The next three characters are the electric power group. This group consists of questions 2, 3, and 4 in Table 11.5-1. The 211 identifier indicates that there is a loss of offsite power and subsequent station blackout with no DC power available. The remaining characters follow the same logic. This is discussed in more detail in Section 11.5.

Other analysts may find it more convenient or appropriate to use letter identifiers or combinations of letters and numbers creating an alphanumeric identifier. The important point is that the identifier be unique and that it communicate the necessary information between the front-end and back-end analysts. A few letters were used in the Peach Bottom analysis for special reasons as defined later in this section.

11.4 Plant Damage State Analysis Recommended Reporting

The reporting of the Plant Damage State Analysis is another important aspect of the effort. The way the sequences (and their failures -- cut sets) were reorganized into PDSs and their frequencies are reported. The following should be included:

- Assumptions. All assumptions used in the Plant Damage State Analysis process.

- Plant Damage State Characteristics. The accident progression event tree questions and answers used to define the plant damage states.

- Plant Damage States. The accident sequences and the corresponding cut sets that comprise each plant damage state should be tabulated.

11.5 Example of Plant Damage State Analysis

The plant damage states are the interface between the systems analysis leading to core damage accident sequences (front-end analysis), and the accident progression analysis (back-end analysis). To provide this interface the cut sets for the accident sequences contributing to core damage must be sorted into groups with common attributes relative to the accident progression event tree. This can be accomplished by answering selected questions that specify the state of the systems or phenomena when core damage occurs for each cut set of the sequence. Although not done for the Peach Bottom analysis, these questions could be depicted in the form of a "bridge tree" between the sequence event trees and the accident progression event tree.

Step 11.1. Identify Accident Progression Questions

In the Peach bottom analysis 16 questions were established by the back-end analyst to examine coolant injection and system success that could affect the radionuclide releases from the core and retention in the containment. This set of questions describes the state of the safety systems and the related accident phenomena. Each unique set of answers to these 16 questions defines a plant damage state (PDS). Each PDS potentially results in a different challenge to the containment and ultimately a different source term for release to the environment. Table 11.5-1 lists the 16 questions. The total number of possible PDSs is the product of the number of answers for each question; potentially a very large and unmanageable number. However, a number of the combinations are not logical, while other combinations are not significant for any given analysis. Thus, the expectation was for a limited number of PDSs, which was the actual outcome of the analysis.

Step 11.2. Determine Possible Answers

Table 11.5-1 uses many of the common symbols, initialisms and acronyms defined elsewhere, but some additional explanation is helpful. In examining each cut set, certain information was useful in determining the answers and providing guidelines to simplify the task. Questions 1 (initiating event group) and 5 (stuck-open relief valve group) from Table 11.5-1 can be answered by inspection of the accident sequence itself. In contrast, the answer to Question 6 (high pressure systems group), success or failure of High Pressure Core Injection (HPCI) and Reactor Core Isolation Cooling (RCIC), may or may not be obvious from the accident

Table 11.5-1
Peach Bottom Accident Progression Event Tree Questions
for Plant Damage States

In order to define the plant damage states for Peach Bottom, the following information is needed for each cut set of each accident sequence such that each question is uniquely answered.

1. What is the Initiating Event (IE)?

    1) A-Large LOCA
    2) S1-Medium LOCA
    3) S2/3-Small/small-small LOCA
    4) T-Transient (all other transients)
    5) TC-Transient without scram (ATWS)
    6) IORV-Inadvertent open relief valve

2. Is there a Loss of Offsite Power (LOSP)?

    1) Seismically induced LOSP
    2) LOSP IE or random LOSP
    3) No LOSP

3. Is there a station blackout (Event B)?

    1) Yes - LOSP IE or random LOSP and loss of all Diesel Generators (DGs)
    2) No - At least one DG working

4. Is DC power available given a station blackout?

    1) No - All DC is failed
    2) Yes - At least one train of DC is working

5. Does a safety relief valve (SRV) stick open early?

    1) Yes - At least one SRV sticks open (P1, P2, or P3)
    2) No - No stuck open SRV

6. Are the High Pressure Injection system (HPCI) and Reactor Core Isolation Cooling system (RCIC) initially working (Events U1 and U2)?

    1) No - Both HPCI and RCIC have initially failed
    2) Yes - Either HPCI or RCIC is initially working

7. Is the Control Rod Drive system (CRD) initially operating (Events U3 and U4)?

    1) fCRD - CRD is definitely failed.
    2) rCRD - CRD is not operating but has not failed either (i.e., depends on LOSP or T1 restored).
    3) Yes - CRD is operating.

Table 11.5-1
Peach Bottom Accident Progression Event Tree Questions
for Plant Damage States (Continued)

(This assumes that if it can work, then it's normally on; therefore, no availability question is asked).

8. What is the initial vessel pressure (Events X1 and X2)?

1) fADS - ADS has failed; therefore, the vessel pressure can not be reduced to low pressure.
2) High - Auto ADS has failed but it is possible to achieve low pressure in the vessel but the operator has not depressurized.
3) Low - Auto ADS or Manual depressurization has worked or any LOCA or transient and stuck open SRV has occurred except for ATWS.

9. What is the initial status of low pressure ECCS (Events V2 and V3)?

1) fLPC - Both LPCI and LPCS have failed and can not be recovered.
2) Recoverable - Both are not currently available but can be recovered given recovery of offsite power or the diesel generators.
3) Available - One pump is running but no injection due to high vessel pressure.
4) Yes - Either LPCS or LPCI is working

10. What is the initial status of Residual Heat Removal (RHR) systems (SCS, SPC, CSS) i.e., the top events W1, W2, and W3?

1) fRHR - All RHR modes are failed
2) Recoverable - All RHR modes are currently unavailable but can be recovered after LOSP and B or T1 and B restored.
3) Yes - One RHR mode is available and working.

(no available question since, if on, it will work).

11. What is the initial status of Condensate System (Event V1)?

1) fCOND - condensate system is failed.
2) rCOND - condensate system is recoverable (after LOSP or T1 restored).
3) aCOND - condensate system is available but not injecting.
4) Yes - condensate system is working (although this answer is not possible given core damage).

Table 11.5-1
Peach Bottom Accident Progression Event Tree Questions
for Plant Damage States (Concluded)

12. What is the initial status of High Pressure Service Water system, HPSW (Event V4)?

    1) fHPSW - HPSW is failed.
    2) rHPSW - HPSW is recoverable (given recovery of offsite power or the diesel generators.
    3) aHPSW - HPSW is available. Manual lineup and actuation required.
    4) Yes - HPSW is working (not possible given core damage).

13. What is the initial status of the Containment Spray System (CSS) (Event W3)?

    1) fCCS - CSS is failed.
    2) rCSS - CSS is recoverable (given recovery of offsite power or the diesel generators).
    3) aCSS - CSS is available, but manual actuation is required.
    4) Yes - CSS is working.

14. Is the containment vented before core damage (Event Y)?

    1) No - Containment is not vented.
    2) DW - Drywell vent.
    3) uDW - Drywell is vented in ATWS, but pressure still high.
    4) uWW - Wetwell is vented in ATWS, but pressure is still high.
    5) WW - Wetwell vent

15. What is the level and timing of containment leakage?

    1) No leakage in excess of tech spec.
    2) Level 2 leakage occurs after core damage (leak).
    3) Level 3 leakage occurs after core damage (rupture).
    4) Level 2 leakage occurs before core damage or isolation failure (leak).
    5) Level 3 leakage occurs before core damage or isolation failure (rupture).

    (A leak vs. rupture depends on the sequence. In non-ATWS sequences, a leak would be an 8-inch line break or less. For ATWS sequences, a leak would be less than two 18-inch line breaks.)

16. What is the location of leakage?

    1) Containment intact
    2) Drywell
    3) Drywell Head
    4) Wetwell

sequence. If the initiator is a large or medium LOCA, the steam supply to HPIC and RCIC will be lost early so that, effectively, both fail. The word "initially" used in these questions refers to the time period prior to core damage.

Answers to several questions include a case where the system has not failed due to hardware failures, but due to a loss of power. Thus, if power were restored, the system could operate. The purpose of these, and similar questions is to determine if water could be injected into the core later, during core melt progression. Injection could mitigate the core melt or it could cause detrimental effects. The resolution of that concern is a back-end issue, but the answers to these front-end systems questions provide the necessary input to the back-end analysis.

Similarly, several questions have answers indicating that the system is available. That is, the system may be operating, but the vessel pressure is too high for injection, or the number of pumps may be insufficient for success in preventing core damage, although it could affect the back-end situation. Also, the system could be available if the operator should choose to use it.

One answer to Question 14, 'Is the containment vented before core damage?', is '1) No - Containment is not vented.' In this case, something failed that prevents venting. Alphabetic characters are used for an answer when there are further alternative answers that are not delineated in the PDS given here. For example, another possible answer to question 14 is X. This symbol was developed by the back-end analysts after the original answers to the question. The symbol X represents the answer, 'Venting is possible, but not done or conditions do not permit venting.' There were no dominant accident sequences in the Peach Bottom analysis where venting was involved in the system event trees.

Some containment failure states are determined from the containment isolation system fault tree. If isolation failure occurs with a conditional probability of 1, the failure would be a leak after core damage and in the drywell. This is incorporated into the PDS identifier as answer 2 for Question 15 and answer 2 for Question 16. In addition, there are two other answers possible for Questions 15 and 16. If random failures of valves cause the leakage, the identifier is Y2 given LOSP and X2 otherwise. It was determined that containment isolation failure does not result in a significant leak at Peach Bottom. A simplified isolation fault tree was constructed and two paths had a potential for being unisolated; the Reactor Building Cooling Water (RBCW) Reactor Coolant Pump (RCP) seal cooling lines, and the drywell (DW) drain lines. From the back-end perspective, neither of these paths was important. The RBCW lines are not connected to the primary system and leakage into the RBCW system is unlikely. The DW sump lines require a double random valve failure which has a probability low enough so as to be neglected.

Step 11.3 Model Any Additional Systems

In the Peach Bottom analysis it was not necessary to fully model any additional systems in order to respond to the 16 questions posed by the back-end analyst. The original event trees and system fault trees had included all the systems and components of interest with the exception of certain containment isolation paths. This system was examined without the development of a complete fault tree.

Step 11.4 Evaluate Accident Sequences

For the Peach Bottom analysis it was convenient to aggregate the 16 questions into 7 groups of questions. These groupings were:

- Question 1 - What is the initiating event?
- Questions 2, 3, and 4 - What electric power is available?
- Question 5 - Do any relief valves stick open?
- Questions 6 and 7 - What is status of high pressure systems?
- Question 8 - What is the status of RCS depressurization?
- Questions 9 to 13 - What is the status of low pressure and decay heat removal systems?
- Questions 14 to 16 - Is the containment vented or does isolation fail?

These questions were addressed first for a complete accident sequence, and then for the individual cut sets where necessary. As noted below, there are a limited number of answers to each of these groups of questions, and only a few combinations of these actually show up as dominant in the analysis.

Step 11.5 Combine Plant Damage States

The 18 dominant accident sequences in the Peach Bottom analysis are presented in Table 11.5-2. The sequences are divided by cut set into the plant damage states shown. As shown in the table, the cut sets from sequences 2, 8, 13, 14 and 15 were expanded into three groups. There are three possible core damage scenarios. One is failure of the ADS with the high pressure systems working (ADS). Another is success of the ADS and of containment venting, but equipment failure occurs due to the harsh environment (/ADS*/VENT). The final scenario is success of the ADS but failure of containment venting. This scenario depicts failure of the low pressure systems on containment repressurization with core damage occurring before or after containment failure depending on which systems are running (/ADS*VENT). This tripled the number of cut sets in sequences 2, 8, 13, 14, and 15.

Each PDS is represented by a 16-character vector depicting the applicable answers to each of the 16 questions which establish the PDS. Because the 16-character vector is not in itself very informative, a brief guide is given in Table 11.5-3.

Table 11.5-2
Plant Damage States by Accident Sequence Before Simplification

Accident Sequence		Cut Sets(1)	PDS 16-Character Vector
1.	T1-BNU11	1-130	4-21S-2-22-S-22222-122
2.	T3A-C-SLC	1-9*ADS	5-322-2-23-2-33333-XX2
		1-9*/ADS*/VENT	5-322-2-23-3-43333-1X2
		1-9*/ADS*VENT	5-322-2-23-3-43333-4X2
3.	T3A-CU11X	1-14	5-322-2-23-2-33333-XX2
4.	S1-V2V3V4NU11	1-3	1-322-2-13-3-13113-XX2
5.	T1-BU11U21	1	4-211-2-12-1-22222-122
6.	T1-P1BNU11	1-57	4-21S-1-22-3-22222-122
7.	T1-BU11NU21	1-79	4-21S-2-22-S-22222-122
8.	T3C-C-SLC	1-6*ADS	5-322-1-23-2-33333-XX2
		1-6*/ADS*VENT	5-322-1-23-3-43333-1X2
		1-6*/ADS*/VENT	5-322-1-23-3-43333-4X2
9.	T1-P2V234NU11B	2,3	4-222-1-13-3-11131-XY2
		1,4,5	4-222-1-13-3-13113-XY2
10.	T2-P2V234NU11	1	4-322-1-13-3-13113-XX2
11.	T3B-P2V234NU11	1	4-322-1-13-3-13113-XX2
		2	4-322-1-13-3-11131-XX2
12.	A-V2V3	1-3	1-322-2-13-3-13113-XX2
13.	T1-C-SLC	1-4*ADS	5-222-2-23-2-33233-XY2
		1-4*/ADS*VENT	5-222-2-23-3-43233-1Y2
		1-4*/ADS*/VENT	5-222-2-23-3-43233-4X2
14.	T3B-C-SLC	1-4*ADS	5-322-2-23-2-33333-XX2
		1-4*/ADS*VENT	5-322-2-23-3-43333-1X2
		1-4*/ADS*/VENT	5-222-2-23-3-43233-4X2
15.	T2-C-SLC	1-4*ADS	5-322-2-23-2-33333-XX2
		1-4*/ADS*VENT	5-322-2-23-3-43333-1X2
		1-4*/ADS*/VENT	5-322-2-23-3-43333-4X2
16.	T3A-P2V234NU11	1	4-322-1-13-3-13113-XX2
17.	T3C-CU11X	1-5	5-322-1-23-2-33333-XX2
18.	T1-P1BU11U21	1	4-211-1-12-3-22222-122

(1) See Appendix E, Reference 4 for more details.

Table 11.5-3
Plant Damage State Vector Groups

Question	1	2,3,4	5	6,7	8	9,10,11,12,13	14,15,16
Description	Initiating Event	Electric Power	Stuck Open SRVs	High Press. Systems	ADS-RCS Depress.	Low Press & DHR Systems	Venting & Containment Isolation
Answers	1 A, S1 4 T 5 ATWS	212 SBO 211 SBO&DC Failure 21S SBO&Special Battery Depletion Considerations 222 LOSP Only 322 No LOSP	1 Yes 2 No	23 HPCI or RCIC Success,CRD Success 22 HPCI or RCIC Success,CRD Recoverable 13 HPCI&RCIC Fail, But CRD OK 12 HPCI&RCIC Fail, CRD Recoverable 11 HPCI,RCIC& CRD Fail	1 ADS Fail 2 ADS Available 3 ADS Success S ADS Special Battery Depletion Considerations 43333 Low Press. Systems Working or Available 43233 Low Press. Systems Working or Available, Condensate Recoverable	33333 Low Press. Systems Available 33233 Low Press. Systems Available Condensate Recoverable 22222 Low Press. Systems Recoverable 22122 Low Press. Systems Recoverable Except Condensate Fails 11131 Low Press. Sys. Fail Except HPSW 33113 Low Press. Systems Available Except Condensate & HPSW Fail 13113 Low Press. Systems Fail Except RHR & CSS	122 No Venting & Isolation Fails 1X2 No Venting, Random Isolation Failures 4X2 Wetwell Vented in ATWS, Random Isolation Failures 1Y2 No Venting, Mostly Random Failures -Some Sequence Dependence XX2 Random Failures XY2 Mostly Random Failures -Some Sequence Dependence

The cut sets in Table 11.5-2 that have the same plant damage state identifiers are grouped together. Another technique used to group the plant damage states was simplification. One simplification that was done in the Peach Bottom analysis was to combine the large and medium LOCAs into one group. This was accomplished by answering Question 1 with the large LOCA answer (number 1) when the original answers are number 1 (large LOCA) or number 2 (medium LOCA). Table 11.5-4 lists the 20 interim plant damage states obtained along with the accident sequence number and the cut set numbers for that sequence. The 20 interim plant damage states were regrouped into 9 final plant damage states (listed in Table 11.5-5) by using simplifications. More detail on the simplifications is provided on the tables.

A brief description of two final plant damage states (Table 11.5-5) is provided below. Narrative descriptions of all of the PDSs are provided in Section 4 of Reference 4.

PDS-5 4-212-6-22-3-22222-111

This PDS is composed of three accident sequences: T1-P1BNU11, T1-BNU11, and T1-BU11NU21. These sequences involve a station blackout with or without one stuck open safety relief valve and initially successful operation of HPCI or RCIC. Battery depletion may or may not occur before core damage. The vessel remains at low pressure if a safety relief valve is stuck open, otherwise, it repressurizes on loss of DC. AC systems are available on recovery of AC power. Venting is not possible until AC is restored.

PDS-8 5-322-2-23-6-33333-611

This PDS is composed of three sequences: T3A-C-SLC, T3B-C-SLC, and T2-C-SLC. This is a loss of AC bus or PCS with failure to scram, and standby liquid control (SLC) also fails. HPCI fails on high suppression pool temperature, and the reactor is a) not manually depressurized, or b) is manually depressurized to use the low pressure systems. If a, then early containment damage (CD) results and venting will not occur before CD. If b, then the containment will pressurize until either venting, containment failure, or SRV reclosure on high containment pressure. In all b cases, the low pressure injection systems will fail due to low NPSH or harsh environments and CD will result. Venting will be tried before CD. The control rod drive system is working in all cases.

All of the plant damage states may be described in a similar manner.

Step 11.6 Quantify Plant Damage States

There was a variation in the PDS interface process for the Peach Bottom analysis. Events representing battery depletion uncertainty were applied to three long-term station blackout sequences (numbers 1, 6, and 7; see Table 11.5-2). The paragraph following this one briefly discusses the process used to accomplish this; for further information, go to Reference 4, Section 4.12. The result was an expansion of the number of cut sets

Table 11.5-4
Interim Peach Bottom Plant Damage States

PDS#	PDS Vector	Contributing Accident Sequence Cut Sets(1)
1.	1-322-2-13-3-13113-XX2	4(1-3)+12(1-3)
2.	4-322-1-13-3-13113-XX2	11(1)+10(1)+16(1)
3.	4-322-1-13-3-11131-XX2	11(2)
4.	4-222-1-13-3-11131-XY2	9(2,3)
5.	4-222-1-13-3-13113-XY2	9(1,4,5)
6.	4-211-1-12-3-22222-122	18(1)
7.	4-211-2-12-1-22222-122	5(1)
8.	4-21S-1-22-3-22222-122	6(1-57)
9.	4-21S-2-22-S-22222-122	1(1-130)+7(1-79)
10.	5-322-1-23-2-33333-XX2	17(1-5)
11.	5-322-1-23-2-33333-XX2	8(1-6)*ADS)
12.	5-322-1-23-3-43333-1X2	8(1-6*/ADS*VENT)
13.	5-322-1-23-3-43333-4X2	8(1-6*/ADS*/VENT)
14.	5-322-2-23-2-33333-XX2	2(1-9*ADS)+14(1-4*ADS)+ 15(1-4*ADS)
15.	5-322-2-23-3-43333-1X2	2(1-9*/ADS*VENT)+14(1-4*/ADS*VENT) +15(1-4*/ADS*VENT)
16.	5-322-2-23-3-43333-4X2	2(1-9*/ADS*/VENT)+14(1-4*/ADS*/VENT)+ 15(1-4*/ADS*/VENT)
17.	5-322-2-23-2-33333-XX2	3(1-14)
18.	5-222-2-23-2-33233-XY2	13(1-4*ADS)
19.	5-222-2-23-3-43233-1Y2	13(1-4*/ADS*VENT)
20.	5-222-2-23-3-43233-4X2	13(1-4*/ADS*/VENT)

(1) See Appendix E, Reference 4 for more details. This column gives the cut sets for the accident sequences that go into that PDS, e.g., 7(2) means cut set #2 from accident sequence #7. Also, 13(1-4*ADS) means cut sets 1 through 4 of accident sequence 13 are all multiplied by the split fraction designated as ADS.

(2) X in question 14 means the vent set point is not reached by the time of core damage, therefore, random or operator failure is possible later in the sequence (handled in the APET). The 1 for question 14 in PDSs 6-9 implies station blackout, so that without AC venting can not occur until AC is recovered (also handled in the APET). The 1 for question 14 as it applies to PDSs 12, 15, and 19 and the 4 applied to PDSs 13, 16, and 20 implies the venting set point is reached before core damage and random or operator failure may or may not occur.

Table 11.5-5
Final Peach Bottom Plant Damage States

PDS#	Final PDS Vector	Interim PDS Numbers	Accident Sequences (Cut Sets) Included
1.	1-322-2-13-3-13113-111	1	4(1-3)+12(1-3)
2.	4-622-1-13-3-13113-111	2,5	9(1,4,5)+11(1)+10(1)+16(1)
3.	4-622-1-13-3-11131-111	3,4	9(2,3)+11(2)
4.	4-211-6-12-1-22222-111	6,7	5(1)+18(1)
5.	4-212-6-22-3-22222-111	8,9	1(1-130)+6(1-57)+7(1-79)
6.	5-322-6-23-2-33333-111	10,17	3(1-14)+17(1-5)
7.	5-322-1-23-6-33333-611	11,12,13	8(1-6)
8.	5-322-2-23-6-33333-611	14,15,16	2(1-9)+14(1-4)+15(1-4)
9.	5-222-2-23-6-33233-611	18,19,20	13(1-4)

Notes:

1) Venting may be required before core damage for PDSs 7, 8, and 9. Venting is not possible until AC power is restored for PDSs 4 and 5. For all other PDSs venting may fail due to operator or random failure, but is not required until after core damage occurs, so it is handled in the APET.

2) Containment isolation failures were either unlikely or not possible in the defined PDSs.

3) The digit 6 was used for several questions in the sixteen character PDS vector, since it had not been used previously, to depict several conditions depending on the questions as explained below:

Question 2 - If LOSP has occurred, all systems respond the same. The APET will handle any differences using TEMAC 4 to split the cut sets.

Question 5 - Differences caused by a stuck open SRV are handled in the APET using split fractions.

Questions 8 and 14 - The difference is manual ADS, which can be handled in the APET using split fractions. The low pressure response is also handled by the APET, depending on primary system pressure results. The venting response depends on whether or not there is a quasi-stable state with low pressure injection working.

for these three sequences by a factor of 5. Theoretically, this expansion of cut sets should not change the core damage frequency. However, since this substitution also provided a more accurate evaluation of recovery, depending upon when battery depletion might occur, and 1 of the 3 sequences was a very high contributor to core damage, the core damage frequency did change by a small amount. Table 11.5-6 summarizes the point estimate core damage frequencies before and after this change. This resulted in a 12% increase in the core damage frequency. This variation effected PDS-5 (Table 11.5-5), which is a grouping of sequences 1, 6, and 7.

A cumulative probability distribution was developed to model the failure probability of the station batteries versus time for station blackout sequences. Because the batteries could fail over a range of times, the uncertainty of battery failure time was incorporated into the accident sequence model by discretizing the battery failure distribution into four areas, with each area centered at equal increments of time, or time parameters. The curve was discretized only out to 10 hours. After 10 hours, core damage will result due to other failures regardless of the state of the batteries. The total probability of each area was calculated and assigned to the mean time of the area. The four time parameters were incorporated into the accident sequence models by being linked together with fault tree "OR" logic, and replacing a single "Battery-Fails" event in the fault trees with the set of four mutually exclusive linked time parameters. The probability associated with each time parameter was used in the point estimate calculations, but for the uncertainty analysis the time parameters were used as switches, always taking on the value of either 0.0 or 1.0. The number of times each time parameter was sampled at 1.0 was proportional to its probability. Furthermore, the sampling of the time parameters was correlated so that, for each sample of the accident sequence model, only one of the time parameters would be valued at 1.0, with the others at 0.0. This correlation was imposed on the sampling because, although battery failure may occur over a range of time, it can only occur once during an accident. The implementation of the battery depletion issue involved expanding each cut set in sequences 1, 6, and 7 to five cut sets by multiplying each cut set by the following individual terms:

INJ-FAILS	Injection Fails
BAT-DEP-3HR	Battery Depletion Occurs Within 3 Hours
BAT-DEP-5HR	Battery Depletion Occurs Within 5 Hours
BAT-DEP-7HR	Battery Depletion Occurs Within 7 Hours
BAT-DEP-9HR	Battery Depletion Occurs Within 9 Hours

This expanded PDS-5 from 266 cut sets to 1330 cut sets.

The final plant damage states are input to the uncertainty analysis and to the back-end analysis.

The accident sequences need to be grouped for input to the accident progression event tree for the back-end analysis. A comprehensive mapping of the accident sequences to the plant damage states is given in Table 11.5-7. The 9 final plant damage states are listed with their original accident sequence number and code name (see Table 11.5-2) along

Table 11.5-6
Core Damage Frequency by Plant Damage States

PDS#	PDS Vector	Number of Cut Sets and Frequency Before Battery Depletion Added		Number of Cut Sets and Frequency After Battery Depletion Added	
1.	1-322-2-13-3-13113-111	6	2.13E-7	No Change, Except	
2.	4-622-1-13-3-13113-111	6	2.27E-7	as Noted Below	
3.	4-322-1-16-3-11131-111	3	5.83E-9		
4.	4-211-6-12-1-22222-111	2	1.95E-7		
5.	4-212-6-22-3-22222-111	266	6.95E-7	1330	1.07E-6
6.	5-322-6-23-2-33333-111	19	2.82E-7		
7.	5-322-1-23-6-33333-611	6	1.07E-7		
8.	5-322-2-23-6-33333-611	17	1.47E-6		
9.	5-222-2-23-6-33233-611	4	4.43E-8		
	Total Point Estimates	329	3.24E-6	1393	3.62E-6

Note: In accounting for battery depletion in more detail, the total number of cut sets was expanded from 329 to 1393 and the total core damage frequency increased from 3.24E-6 to 3.62E-6.

Table 11.5-7
Peach Bottom Accident Sequences Included in Each Plant Damage State

PDS	Accident Sequences and Cut Sets*	Number of Cut Sets
1	4(S1-V2V3V4NU11)(CS1-3) + 12(A-V2V3)(CS1-3)	6
2	9(T1-P2V234NU11B)(CS1,4,5) + 11(T3B-P2V234NU11)(CS1) + 10(T2-P2V234NU11)(CS1) + 16(T3A-P2V234NU11)(CS1)	6
3	9(T1-P2V234NU11B)(CS2,3) + 11(T3B-P2V234NU11)(CS2)	3
4	5(T1-BU11U21)(CS1) + 18(T1-P1BU11U21)(CS1)	2
5	1(T1-BNU11)(CS1-650) + 6(T1-P1BU11)(CS1-285) + 7(T1-BU11NU21)(CS1-395	1330
6	3(T3A-CU11X)(CS1-14) + 17(T3C-CU11X(CS1-5)	19
7	8(T3-C-SLC)(CS1-6)	6
8	2(T3A-C-SLC)(CS1-9) + 14(T3B-C-SLC(CS1-4) + 15(T2-C-SLC)(CS1-4)	17
9	13(T1-C-SLC)(CS1-4)	4
	Total Cut Sets	1393

*Accident Sequence Number (accident sequence code name)(cut sets included) with the associated cut sets from that sequence. By use of Table 11.5-7, the primary contributors to each plant damage state can be inferred from the corresponding accident sequences. The core damage frequency statistics for each final plant damage state are given in Table 11.5-8 along with an abbreviated description of the PDS. Plant damage states 5 and 8 (described in Step 11.5) contribute 42.0% and 32.5%, respectively. These two examples are discussed further in the following paragraphs.

Plant Damage State 5 1330 Cut Sets

Mean CDF 1.90E-6/reactor year 42.0% of Total CDF

The cut sets in PDS-5 are characterized by diesel generator failure given a loss of offsite power and failure to recover offsite power. This may be due to hardware failures and subsequent failure to repair the diesel generators or cooling failures which, in turn, cause diesel generator failure. In all cases, the injection failure is the end result. Either injection fails early with HPCI and RCIC failing or later due to battery depletion and loss of safety system control. PDS-5 cut sets involve all of the combinations of these failures leading to a large number of cut sets with a more uniform distribution of contribution per individual cut set. Key events are the operator failure to initiate the emergency heat sink, diesel generator failure to run, HPCI and RCIC failure due to the steam environment, battery depletion, failure to recover diesel generator hardware failures, and failure to recover offsite power.

Plant Damage State 8 17 Cut Sets

Mean CDF 1.46E-6/reactor year 32.5% of Total CDF

All the cut sets in this plant damage state are characterized by a transient initiating event followed by RPSM failure, a standby liquid control (SLC) operator or hardware failure and no feasible recovery (NR). Key events are RPSM, NR, IE-T3A, and operator failure to restore the SLC after testing.

All of the plant damage states are similarly described in Section 5.3 of Reference 4.

Step 11.7. Calculate Split Fractions

When the accident sequences were initially categorized by plant damage state, there were 20 unique states. These PDSs were labeled interim plant damage states since they were combined to form the final PDSs. However, the back-end analysts need to know the proportion of each of the final nine PDSs that come from the interim PDSs. These proportions were calculated and called split fractions. For example, PDS-7 has three subsets of conditions such as ADS failure, ADS success with venting failure (VENT), and ADS success with venting success. The cut sets can be resorted, usually by hand, into these three categories. The outcome might be 20% ADS failures and 60% venting failures resulting in split fractions of 0.20 for ADS, 0.48 for /ADS*VENT, and 0.32 for /ADS*/VENT, where /ADS is automatic depressurization success and /VENT is venting

Table 11.5-8
Peach Bottom Plant Damage State Core Damage Frequencies

	Plant Damage State Code	Simplified Description	5%	Medium	Mean	95%	% of Total
1.	1-322-2-13-3-13113-111	LOCA-HPIFAILS-LPIFAILS	2.5E-9	4.4E-8	2.6E-7	7.8E-7	5.7
2.	4-622-1-13-3-13113-111	TRANS-SORV-LPIFAILS	1.1E-9	3.0E-8	2.2E-7	8.1E-7	4.9
3.	4-622-1-13-3-11131-111	TRANS-SORV-LPIFAILS	5.9E-11	1.2E-9	6.1E-9	2.7E-8	0.1
4.	4-211-6-12-1-22222-111	TRANS-SBO-NODC-HPIFAILS-NOADS	3.5E-9	5.0E-8	2.1E-7	7.1E-7	4.6
5.	4-212-6-22-3-22222-111	TRANS-SBO-BATDEP	3.5E-8	4.0E-7	1.9E-6	4.8E-6	42.0
6.	5-322-6-23-2-33333-111	ATWS-HPIFAILS-LPIAVAIL	3.2E-9	5.9E-8	3.0E-7	1.1E-6	6.7
7.	5-322-1-23-6-33333-611	ATWS-IORV-SLCFAILS	1.2E-9	2.3E-8	1.1E-7	3.8E-7	2.5
8.	5-322-2-23-6-33333-611	ATWS-SLC-FAILS	1.8E-8	2.9E-7	1.5E-6	5.6E-6	32.5
9.	5-222-2-23-6-33233-611	ATWS-LOSP-LPIAVAIL	4.3E-10	1.0E-8	4.4E-8	1.6E-7	1.0
		Total Core Damage Frequency	3.5E-7	1.9E-6	4.5E-6	1.3E-5	100.0

success. Table 11.5-9 contains the mean split fraction values for the Peach Bottom plant damage states. A Monte Carlo sample for each split fraction is generated.

Another grouping of the accident sequences or plant damage states by initiating event is often useful to the back-end analysts. This categorization, labeled super plant damage states, is illustrated in Table 11.5-10 considering in order of precedence ATWS, LOSP, other transients, and LOCAs. The precedence is that a LOSP, which becomes an ATWS, is grouped with ATWS and transient-induced LOCAs, e.g., stuck open SRVs, are grouped with the transients, not the LOCAs.

Another alternative category is station blackout. Short-term station blackout results from two accident sequences, T1-BU11U211 and T1-P1BU11U21, and accounts for 4.6% of the total CDF. These two sequences constitute the entire PDS-4. Station blackout due to battery depletion results from three accident sequences, T1-BNU11, T1-P1BNU11, and T1-BU11NU21, and accounts for 42.0% of the total CDF. These three sequences constitute the entire PDS-5. Thus, in this categorization, PDS-4 and PDS-5 together represent station blackout and constitute 46.6% of the total CDF.

These outputs represent the last of the information generated in the front-end analysis and provided to the back-end analysis.

Table 11.5-9
Peach Bottom Plant Damage States/Split Fractions

Final PDS	Interim PDS	Variable	Split Fraction
1	1		None Required
2	2	/LOSP	0.630
	5	LOSP	0.370
3	3	/LOSP	0.052
	4	LOSP	0.948
4	6	SRV	0.082
	7	/SRV	0.098
5	8	SRV	0.069
	9	/SRV	0.931
6	10	SRV	0.073
	17	/SRV	0.927
7	11	ADS	0.200
	12	/ADS*VENT	0.002
	13	/ADS*/VENT	0.798
8	14	ADS	0.200
	15	/ADS*VENT	0.002
	16	/ADS*/VENT	0.798
9	18	ADS	0.200
	19	/ADS*VENT	0.002
	20	/ADS*/VENT	0.798

Table 11.5-10
Peach Bottom Super Plant Damage States

Super Plant Damage State	Contributing Accident Sequences		5%	Median	Mean	95%	% of Total
ATWS (PDS-6,	2	T3A-C-SLC	3.1E-8	4.4E-7	1.9E-6	6.6E-6	42.2
7,8 and 9)	3	T3A-CU11X					
	8	T3C-C-SLC					
	13	T1-C-SLC					
	14	T3B-C-SLC					
	15	T2-C-SLC					
	17	T3C-C-CU11X					
LOSP (PDS-4,	1	T1-BNU11	8.3E-8	6.2E-7	2.2E-6	6.0E-6	48.9
5 and parts	5	T1-BU11U21					
of 2 and 3)	6	T1-P1BNU11					
	7	T1-BU11NU21					
	9	T1-P2V234NU11B					
	18	T1-P1BU11U21					
Transient	10	T2-P2V234NU11	6.1E-10	1.9E-8	1.4E-7	4.7E-7	3.1
(Parts of	11	T3B-P2V234NU11					
PDS-2 and 3)	16	T3A-P2V234NU11					
LOCA (PDS-1)	4	S1-V2V3V4NU11	2.5E-9	4.4E-8	2.6E-7	7.8E-7	5.8
	12	A-V2V3					
Total Core Damage Frequency			3.5E-7	1.9E-6	4.5E-6	1.3E-5	100.0

12. UNCERTAINTY ANALYSIS

This section discusses the sources and treatment of uncertainty in a Probabilistic Risk Assessment (PRA). Uncertainty in the analysis comes from every step of the process. It can be both qualitative and quantitative in nature, and arises from the data base used to determine parameter values, modeling assumptions, and completeness of the analysis.

A detailed uncertainty analysis is an important analytical tool. Decisionmakers need to understand the margins of safety at existing facilities and to determine the best allocation of resources to enhance safety. Many early PRAs did not include uncertainty analysis in the quantification of risk, or were less sophisticated than the methods applied in the NUREG/CR-4550 analyses. The methods used for NUREG/CR-4550 provide measures of the dominant risk contributors and dominant contributors to the uncertainty of risk. Furthermore, the methods are compatible with the uncertainty methods used in the containment performance and consequence analyses. This enhances the propagation of uncertainty through the entire risk analysis process, so that final risk calculations reflect the uncertainty of all aspects of the PRA.

12.1 Uncertainty Analysis Assumptions and Limitations

It is important to distinguish between the concepts of uncertainty and variability. The nature of the events considered in a PRA (such as initiating events, component failures, operator actions) is such that they are treated as being random processes, and modeled through the use of probabilistic models. It is this use of probability which gives the PRA its name. Sources of random variability are incorporated directly in the PRA models.

However, because of a lack of data or a lack of detailed understanding of the physical phenomena being modeled, the relationships that are used to describe the variability are not precisely known. This can be reflected in a lack of precision in the value of a component failure rate, or in the provision of alternative mathematical formalisms. This lack of knowledge is the uncertainty that is of interest here, and which leads to the lack of precision in the predictions of the PRA. An increased level of knowledge will not change the fact that a PRA is a probabilistic model, but it will give greater confidence in the predictions of that model.

12.2 Uncertainty Quantification

Two basic types of uncertainty were addressed in NUREG/CR-4550: parameter value uncertainty and modeling uncertainty. Sources of parameter uncertainty include lack of data on component failure modes, interpretation of data and component performance records, and the use of industry-wide data for the plant specific analyses. Modeling uncertainty reflects limitations of knowledge regarding phenomenological progression through the plant systems, and human response to abnormal conditions.

The parameters of interest are those of the probability models for the accident sequence logic. They include failure rates, component unavailabilities, initiating event frequencies, and human error probabilities. Modeling uncertainties include issues such as success criteria, failure logic in fault trees, and phenomenological processes and their impact on system performance. The essential difference between the parameter value uncertainty and modeling uncertainty is the following. Parameter estimates can take on any of a continuous range of values, and the fact that there is uncertainty as to which value is correct does not change the structure of the logic model. With regard to modeling uncertainties, different modeling hypotheses can be proposed which may well lead to different logical representations of the systems and processes incorporated into the accident models.

Modeling uncertainties are treated similarly by defining discrete or continuous probability distributions over the different modeling hypotheses. Previous studies have incorporated modeling uncertainties into their analyses by performing sensitivity analyses to identify which modeling hypotheses are most significant. However, the uncertainty associated with the various hypotheses was not incorporated into an integrated estimate of risk. The method for the NUREG/CR-4550 analysis was to use expert judgment (Section 9) to elicit from a panel of experts various hypotheses for important modeling uncertainties or issues. These hypotheses were incorporated into an aggregated model. Then the aggregated model uncertainty was propagated through the accident sequence quantification so as to include the various hypotheses in the final overall core damage and risk estimates. Each issue was resolved by deriving parameter estimates and associated probability distributions relevant to the issue which incorporated with equal weight the hypotheses of each expert.

The application of the results of an uncertainty analysis requires a method which calculates measures of uncertainty for the accident frequency estimate (e.g., core damage frequency, plant damage state frequency) and which calculates the contribution of the various basic events in the accident models to the frequency estimates. The basic event probability models contribute both to the point estimate of the frequency and to the uncertainty of the frequency estimate. Thus, the method chosen for uncertainty analysis should be sufficiently comprehensive to satisfy the needs of decisionmakers.

There are several methods available for propagating uncertainty through models. A summary of methods is available in NUREG/CR-4836.[38] Some methods are unwieldy when applied to large system models and do not permit calculation of useful risk measures. The method selected for NUREG/CR-4550 is a restricted Latin Hypercube Sampling (LHS)[70] for generating the samples of the basic event distributions, which are input to the Top Event Matrix Analysis Code (TEMAC).[73] TEMAC uses the samples generated in the LHS to calculate various statistics of the top events (e.g., plant damage state or accident sequence frequency) of the accident models.

LHS is a constrained Monte Carlo technique which forces the sampling of the basic event probability distributions to include samples from the tails of the distributions. The LHS code is flexible in that it can sample a variety of random variable distributions (e.g., lognormal, normal, beta, empirical distributions). TEMAC uses the LHS parameter samples and the accident sequence equations (cut sets) as input to quantify the core damage estimates. TEMAC generates a sample of the accident sequence frequency, a point estimate of the frequency, and various importance measures and ranking for the basic events. Reference 38 describes the code calculations and output in detail. A brief description of the calculations generated by TEMAC is given below. It is recommended that sampling of basic event probabilities and frequencies which are modeled from the same parameter estimate be statistically correlated. The need for this is discussed in NUREG/CR-4836[38] and by Apostolakis and Kaplan.[74] When component failures are grouped into generic categories, it is assumed that all components in a particular group have the same failure rate or probability. The sample of the component failure rates should be the same for each component in a particular group.

For example, suppose for the generic component failure "Motor-Operated Valve (MOV) fails to remain open," a lognormal distribution with a mean value of 1.0E-4/h and error factor of 3 is established in the data base analysis to model the uncertainty in the estimate of this component failure rate. Suppose, as well, that fifteen MOVs (normally open) have been incorporated into the systems analysis (Section 5) of the plant. These MOVs are all tested on a monthly schedule (720 h). Thus, the probability distribution for the failures of an MOV to remain open for 720 h is modeled as:

- lognormal,
- mean = 1.0E-4/h x 720 h,
  = 0.07,
- error factor = 3.

The distribution for the fifteen basic events, "MOV-XX fails to remain open for 720 h" has been derived by shifting the relevant parameter distribution by the time scalar. The above distribution is incorporated into the LHS input file. All fifteen events will be quantified in the accident sequence uncertainty analysis by using the same sample of this distribution generated by the LHS.

Now suppose that another set of ten MOVs, normally open, have been incorporated into the systems analysis. Suppose that these values are tested on a quarterly basis (2160 h). The distribution for the ten basic events, "MOV-YY fails to remain open for 2160 h" is based on the same parameter estimate as the monthly tested MOVs. However, the parameter distribution is now scaled by the time scalar of 2160 h:

- lognormal,
- mean = 1.0E-4/h x 2160 h,
  = 0.22,
- error factor = 3.

It is important to realize that even though both groups of MOVs have distributions based on the same failure rate estimate, the difference in time scaling for the two groups necessitates that each group be modeled from a unique distribution in the LHS. This is because the LHS code cannot sample a time dependent parameter and then match the parameter sample to various time factors.

The LHS users guide[72] explains how the LHS code can correlate the samples of two such similar distributions. Thus, the monthly and quarterly tested MOV distributions can be sampled with a high degree of correlation between the samples (up to about 0.99). It is recommended that the sampling of similarly based LHS distributions be so correlated.

The following descriptive statistics are generated by TEMAC for the frequency.

- The nominal estimate of the accident frequency (quantified with all basic events and initiating events set equal to a user-specified nominal value).

- Mean of the frequency sample.

- Standard deviation of the frequency sample.

- 0.5, 0.25, 0.50, 0.75, and 0.95 quantiles of the frequency sample.

The entire sample of the accident frequency generated by TEMAC is directed to an output file so that the cumulative probability distribution and probability density functions of the frequency can be tabulated. TEMAC does not contain any plotting routines, but the data can be plotted using graphic software packages.

In addition to the accident frequency sample and relevant statistics, TEMAC calculates several importance measures. These measures provide an understanding of those events in the model which are significant to the estimate of the accident frequency. Different measures are calculated to develop an understanding of risk contributors based on different importance criteria. These are explained below.

Risk Reduction

Risk reduction is a measure of the change in the accident frequency from a proportional change in the basic event probability. This measure yields a ranking of the basic events by importance, or contribution, to the accident frequency. The risk reduction figure of merit is analogous to the potential reduction in the accident frequency if a base event probability is set to zero, or made perfectly reliable. This measure is useful in identifying which components, human actions, maintenance practices, and initiating events should be the focus of effort to improve reliability and reduce risk. Uncertainty intervals for risk reduction are also calculated. These are the 0.05 and 0.95 quantiles of the risk reduction calculations generated by performing 'n' such calculations over the LHS matrix of base and initiating events samples ('n' being the size of the LHS). The risk reduction uncertainty intervals show the uncertainty in a basic event's contribution to risk from the uncertainty of the accident frequency. Initiating events are ranked separately from basic events.

Risk Increase

Risk increase (sometimes called risk achievement) can be thought of as the increase in risk that results should a particular base event probability be set to 1.0. This measure is meaningful only for probabilities and is not used in conjunction with initiating event frequencies. This measure is useful to assess which elements of the risk model are the most crucial for maintaining risk at current levels. Uncertainty intervals for risk increase are calculated as with risk reduction.

Uncertainty Importance

The uncertainty importance measure focuses on the contribution to the variance of the accident frequency attributable to each of the base and initiating events that jointly constitute the accident equation. In particular, if F is a composite of these events, where F represents the frequency of the top event, it is reasonable to expect a reduction in the Var(F) if the value of an event, X_j, is known with certainty. If X_j is known with certainty, then the variance of F is conditional on the specific value of X_j and is denoted by $\mathrm{Var}(F|X_j)$. Moreover, the conditional reduction in the variance of F attributable to ascertaining the true value of the event X_j is expressed as

$$\mathrm{Var}(F) - \mathrm{Var}(F|X_j).$$

The conditional variance of F, Var(F), can be expressed in terms of the expected value of the conditional variance, $E_{Xj}[\mathrm{Var}(F|X_j)]$, and the variance of the conditional expectation, $\mathrm{Var}_{Xj}[E(F|X_j)]$, as follows:

$$\mathrm{Var}(F) = E_{Xj}[\mathrm{Var}(F|X_j)] + \mathrm{Var}X_j[E(F|X_j)]$$

or

$$\mathrm{Var}_{Xj}[E(F|X_j)] = \mathrm{Var}(F) - E_{Xj}[\mathrm{Var}(F|X_j)].$$

The square root of the right-hand side of the above equation is the measure referred to as an uncertainty importance for event X_j.

The uncertainty importance measure requires calculating the variance of a conditional expectation of a random variable, $\mathrm{Var}_{Xj}[E(F|X_j)]$. If the random variable has a long-tailed distribution, such as occurs when lognormal distributions are used with large error factors, then its variance is extremely difficult to estimate. This estimation problem is directly attributable to the scale of the numbers involved. The scaling problem can be overcome by performing uncertainty importance calculations based on a logarithmic scale for the top event frequencies. The log scale produces a reliable ordering of the events and expresses the results in terms of log-based risk.

However. the log-based uncertainty importance calculations do not readily translate back to a linear scale; thus, the uncertainty importance calculations in TEMAC are given only in terms of log-based risk. TEMAC does, however, provide the analyst with information that aids in the interpretation of the results of the log-based uncertainty importance calculation. This is accomplished by computing the ratio, $R_{.05}$, of the 0.05 quantile of the distribution of the top event frequency when X_j is held constant at its mean value, to the 0.05 quantile of the top event frequency when X_j is not held constant. A similar ratio, $R_{.95}$, is calculated by TEMAC for the 0.95 quantiles.

If $R_{.05}$ and $R_{.95}$ are both greater than 1.0, then the distribution of the frequency of the top event with X_j held constant at its mean value has shifted to the right, or shows an overall higher level of risk. On the other hand, if $R_{.05}$ and $R_{.95}$ are both less than 1.0, then the distribution of the frequency of the top event with X_j held constant at its mean value has shifted to the left, or shows an overall lower level of risk. If $R_{.05}$ is greater than 1.0 and $R_{.95}$ is less than 1.0, then the overall uncertainty in the distribution of the top event frequency has decreased. Likewise, if $R_{.05}$ is less, 1.0 and $R_{.95}$ is greater than 1.0, then the overall uncertainty in the distribution of the top event frequency has increased.

The uncertainties of the parameter values defined in the Data Base Analysis (Section 8) and the modeling uncertainties, established and quantified in the Expert Judgment Analysis (Section 9), are propagated through the accident sequence models. The quantification of the accident frequency and risk measures incorporate these uncertainties. The series of steps for this process are described below and illustrated in Figure 12.2-1.

Step 12.1. Obtain Information

In this step the analyst gathers the information from the other tasks which is necessary for the uncertainty analysis. The information needed is:

- Basic Event Point Estimates and Probability Models (Section 8),
- Expert Judgment Point Estimates and Probability Models (Section 9),
- Accident Sequence Equations (Section 10), and
- Plant Damage States Equations (Section 11).

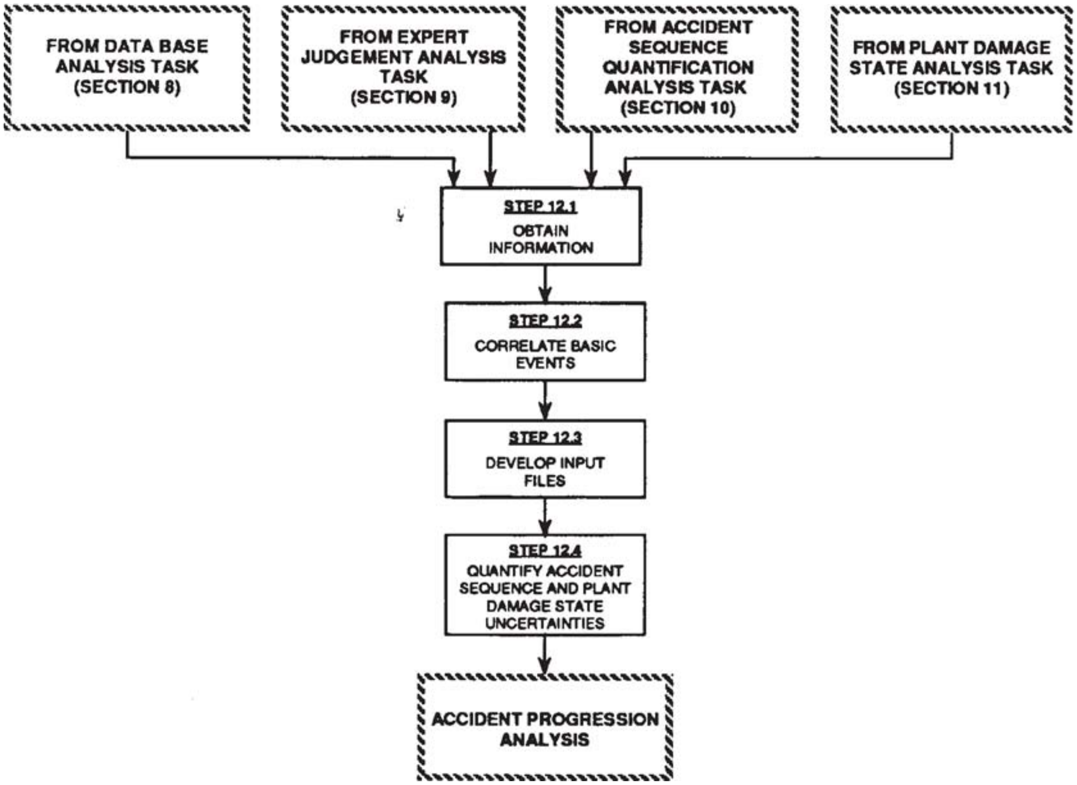

FROM DATA BASE ANALYSIS TASK (SECTION 8)
FROM EXPERT JUDGEMENT ANALYSIS TASK (SECTION 9)
FROM ACCIDENT SEQUENCE QUANTIFICATION ANALYSIS TASK (SECTION 10)
FROM PLANT DAMAGE STATE ANALYSIS TASK (SECTION 11)
STEP 12.1
OBTAIN INFORMATION
STEP 12.2
CORRELATE BASIC EVENTS
STEP 12.3
DEVELOP INPUT FILES
STEP 12.4
QUANTIFY ACCIDENT SEQUENCE AND PLANT DAMAGE STATE UNCERTAINTIES
ACCIDENT PROGRESSION ANALYSIS

Figure 12.2-1. Step Relationship for Uncertainty Analysis

Step 12.2. Correlate Basic Events

In this step the analyst identifies the basic event probability models that are statistically correlated. All of the basic events and initiators defined in the Systems Analysis task need to be grouped into sets defined by the same component failure mode and probability distribution. A probability distribution for each set of basic events is put into the LHS input file. TEMAC, which uses the samples generated by the LHS code to quantify the accident modes frequency, requires an input file which links each basic event in the accident equation to its sample in the LHS output, thus ensuring that all events of the same set are modeled by the appropriate sample.

It is suggested that the analyst group all of the basic events quantified in the Data Analysis (Section 8) using the following hierarchy:

- Group all basic events by component type (e.g., MOV, AOV, MDP),
- Within each component group, organize events into subgroups by failure mode (e.g., fail-to-start, fail-to-run),
- For time related basic events, group all events from each component failure mode group into sets according to the time parameter value used to quantify the event probability (e.g., 6 h, 720 h), and
- For demand related failures, no further grouping is necessary beyond the component failure model level.

It is important to note that, if different parameter estimates are developed for components within the same component group (e.g., Service Water Motor-Drive Pump, Residual Heat Removal Motor-Driven Pump), then these should be treated as separate component groups.

Step 12.3. Develop Input Files

In this step the analyst develops the input files for the TEMAC and LHS input structure. The TEMAC and LHS user manuals[73,72] describe the structure of these files.

Step 12.4. Quantify Accident Sequence and Plant Damage State Uncertainties

In this step the analyst generates the samples of all of the random variables defined in Step 12.2, and propagates the uncertainties through the calculation of accident frequency. The random variable samples are generated by running the LHS code. This produces a matrix of 'n' vectors. Each vector contains one sampled value for each random variable. The LHS matrix is one of the input files for TEMAC. TEMAC is run to generate the accident frequency sample, and to calculate the frequency statistics and importance measures.

13. REFERENCES

[1] Reactor Risk Reference Document, NUREG-1150, U. S. Regulatory Commission, Washington, DC, February 1987.

[2] Bertucio, R. C., et al., Analysis of Core Damage Frequency: Surry Unit 1, Internal Events, NUREG/CR-4550, Vol. 3, Rev. 1, SAND86-2084, Sandia National Laboratories, Albuquerque, NM, (draft copy available in NRC public documents room).

[3] Bertucio, R. C., et al., Analysis of Core Damage Frequency; Sequoyah Unit 1, Internal Events, NUREG/CR-4550, Vol. 5, Rev. 1, SAND86-2084, Sandia National Laboratories, Albuquerque, NM, (draft copy available in NRC public documents room).

[4] Kolaczkowski, A. M., et al., Analysis of Core Damage Frequency; Peach Bottom Unit 2, Internal Events, NUREG/CR-4550, Vol. 4, Rev. 1, SAND86-2084, Sandia National Laboratories, Albuquerque, NM, August 1989.

[5] Drouin, M. T., et al., Analysis of Core Damage Frequency: Grand Gulf Unit 1, Internal Events, NUREG/CR-4550, Vol. 6, Rev. 1, SAND86-2084, Sandia National Laboratories, Albuquerque, NM, September 1989.

[6] Bohn, M. P. and J. A. Lambright, Recommended Procedures for Simplified External Event Risk Analysis, NUREG/CR-4840, SAND88-3102, Sandia National Laboratories, Albuquerque, NM (draft copy available in NRC public documents room).

[7] Carlson, D. D., et al., Interim Reliability Evaluation Program Procedures Guide, NUREG/CR-2728, SAND82-1100, Sandia National Laboratories, January 1983.

[8] Kolb, G. J., et al., Interim Reliability Evaluation Program: Analysis of the ANO Unit 1 Nuclear Power Plant, NUREG/CR-2787, SAND82-0978, Sandia National Laboratories, Albuquerque, NM, June 1982.

[9] Categorization of Reactor Safety Issues from a Risk Perspective, NUREG-1115, U. S. Nuclear Regulatory Commission, Washington, DC, March 1985.

[10] Gorham-Bergeron, E., et al., Evaluation of Severe Accident Risks: Methodology for the Accident Progression, Source Term, Consequence, and Risk Integration and Uncertainty Analysis, NUREG/CR-4551, Vol.1, SAND86-1309, Sandia National Laboratories, Albuquerque, NM, (draft copy available in NRC public documents room).

[11] Hubble, W. H. and C. Miller, Data Summaries of Licensee Event Reports of Valves at U. S. Commercial Nuclear Power Plants, NUREG/CR-1363, Vol 1., Appendices O-Y, EGG-EA-5125, EG&G Idaho, Inc., Idaho Falls, ID, June 1980.

[12] Hubble, W. H. and C. Miller, Data Summaries of Licensee Event Reports of Pumps at U. S. Commercial Nuclear Power Plants, NUREG/CR-1205, EGG-EA-5524, EG&G, Idaho, Inc., Idaho Falls, ID, January 1982.

[13] ATWS: A Reappraisal, Part 3: Frequency of Anticipated Transients, EPRI-2230, Interim Report, Electric Power Research Institute, Palo Alto, CA, January 1982.

[14] ATWS: A Reappraisal, Part 3: Frequency of Anticipated Transients, EPRI-801, Electric Power Research Institute, Palo Alto, CA, July 1978.

[15] Mackowiak, D. P., et al., Development of Transient Initiating Event Frequencies for Use in Probabilistic Risk Assessments, NUREG/CR-3862, EG&G-2323, Idaho National Engineering Laboratories, Idaho Falls, ID, May 1985.

[16] Additional Information Required for NRC Staff Generic Report on Boiling Water Reactors, NEDO-24708A, Class 1, Rev. 1, General Electric Co., San Jose, CA, December 1980.

[17] Generic Evaluation of Feedwater Transients and Small Break Loss of Coolant Accidents in Westinghouse Designed Operating Plants, NUREG-0611, U. S. Nuclear Regulatory Commission, Washington, DC, January 1980.

[18] Generic Evaluation of Feedwater Transients and Small Break Loss of Coolant Accidents in Combustion Engineering Designed Operating Plants, NUREG-0635, U. S. Nuclear Regulatory Commission, Washington, DC, January 1980.

[19] Generic Evaluation of Small Break Loss of Coolant Behavior in Babcock and Wilcox Designed 177-FA Operating Plants, NUREG-0565, U. S. Nuclear Regulatory Commission, Washington, DC, January 1980.

[20] Iman, R. L. and S. C. Hora, Modelling Time to Recovery and Initiating Event Frequency for Loss of Offsite Power Incidents at Nuclear Power Plants, NUREG/CR-5032, SAND87-2428, Sandia National Laboratories, Albuquerque, NM, January 1988.

[21] Fleming, K. N., et al., Classification and Analysis of Reactor Operating Experience Involving Dependent Events, EPRI-NP-3967, Electric Power Research Institute, Palo Alto, CA, June 1985.

[22] Atwood, C. L., Common Cause Fault Rates for Pumps, NUREG/CR-2098, EGG-EA-5189, EG&G Idaho, Inc., Idaho Falls, ID, February 1983.

[23] Steverson, J. A. and C. L. Atwood, Common Cause Fault Rates for Valves, NUREG/CR-2770, EGG-EA-5485, EG&G Idaho, Inc., Idaho Falls, ID, February 1983.

[24] Atwood, C. L. and J. A. Steverson, Common Cause Fault Rates for Diesel Generators: Estimates Based on Licensee Event Reports at U. S. Nuclear Power Plants 1976-1978, NUREG/CR-2099, EGG-EA-5359, EG&G Idaho, Inc., Idaho Falls, ID, June 1982.

[25] Baranowsky, P. W., et al., A Probabilistic Safety Analysis of DC Power Supply Requirements for Nuclear Power Plants, NUREG-0666, U. S. Nuclear Regulatory Commission, Washington, DC, April 1981.

[26] Ornstein, H., Air Systems Problems at U. S. Light Water Reactors, AEOD/C701, U. S. Nuclear Regulatory Commission, Washington, DC, March 1987.

[27] Kolaczkowski, A. M. and A. C. Payne, Station Blackout Accident Analysis, NUREG/CR-3226, SAND82-2450, Sandia National Laboratories, Albuquerque, NM, May 1983.

[28] Baranowsky, P. W., Evaluation of Station Blackout Accidents at Nuclear Power Plants, NUREG-1032, U. S. Nuclear Regulatory Commission, Washington, DC, May 1985.

[29] Mays, S. E., et al., Interim Reliability Evaluation Program: Analysis of the Browns Ferry, Unit 1, Nuclear Power Plant, NUREG/CR-2802, EGG-2199, EG&G Idaho,Inc., Idaho Falls, ID, July 1982.

[30] Amico, P. J., et al., Interim Reliability Evaluation Program: Analysis of Millstone Point, Unit 1 Nuclear Power Plant, NUREG/CR-3085, SAND82-7212, Sandia National Laboratories, Albuquerque, NM, February 1983.

[31] Garcia, A. A., et al., Crystal River-3 Safety Study, Volume 1 -- Main Report, NUREG/CR-2515, SAND81-7229/I, Sandia National Laboratories, Albuquerque, NM, December 1981.

[32] Steambinding of Auxiliary Feedwater Pumps, AEOD/C404, U. S. Nuclear Regulatory Commission, Washington, DC, July 1984.

[33] Zion Probabilistic Safety Study, Commonwealth Edison Company, Chicago, IL, 1981.

[34] Oconee PRA, A Probabilistic Risk Assessment of Oconee Unit 3, NSAC-60, Electric Research Power Institute, Palo Alto, CA, June 1984.

[35] Swain, A. D., Accident Sequence Evaluation Program Human Reliability Analysis Procedure, NUREG/CR-4772, SAND86-1996, Sandia National Laboratories, Albuquerque, NM, February 1987.

[36] Swain, A. D. and H. E. Guttman, Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications, NUREG/CR-1278, SAND80-0200, Sandia National Laboratories, Albuquerque, NM, August 1983.

[37] PRA Procedures Guide, NUREG-2300, U. S. Nuclear Regulatory Commission, Washington, DC, January 1983.

[38] Bohn, M. P., et al., Approaches to Uncertainty Analysis in Probabilistic Risk Assessment, NUREG/CR-4836, SAND87-0871, Sandia National Laboratories, Albuquerque, NM, January 1988.

[39] Reactor Safety Study -- An Assessment of Accident Risks in U. S. Commercial Nuclear Power Plants, WASH-1400, NUREG-75/014, U. S. Nuclear Regulatory Commission, Washington, DC, October 1975.

[40] Poloski, J. P. and W. H. Sullivan, Data Summaries of Licensee Event Reports of Diesel Generators at U. S. Commercial Nuclear Power Plants January 1, 1976 through December 31, 1978, NUREG/CR-1362, EG&G Idaho, Inc., Idaho Falls, ID, January 1985.

[41] Brown, S. R., Data Summaries of Licensee Event Reports of Protective Relays and Circuit Breakers at U. S. Commercial Nuclear Power Plants January 1, 1976 to December 31, 1986, NUREG/CR-4212, EGG-2370, EG&G Idaho, Inc., Idaho Falls, ID, January 1985.

[42] Miller, C. F., et al., Data Summaries of Licensee Event Reports of Selected Instrumentation and Control Components At U. S. Commercial Nuclear Power Plants January 1, 1976 to December 31, 1978, NUREG/CR-1740, EGG-EA-5388, EG&G Idaho, Inc., Idaho Falls, ID, May 1981.

[43] Hubble, W. H. and C. F. Miller, Data Summaries of Licensee Event Reports of Control Rods and Drive Mechanisms at U. S. Commercial Nuclear Power Plants January 1, 1972 to April 30, 1978, NUREG/CR-1331, EG&G Idaho, Inc., Idaho Falls, ID, February 1980.

[44] Drago, J. P., et al., The In-plant Reliability Data Base for Nuclear Plant Components: Interim Data Report - The Pump Component, NUREG/CR-2886, ORNL/TM-8465, Oak Ridge National Laboratory, Oak Ridge, TN, December 1982.

[45] Borkowski, R. J., et al., The In-plant Reliability Data Base for Nuclear Plant Components: Interim Report - The Valve Component, NUREG/CR-3154, ORNL/TM-8647, Oak Ridge National Laboratory, Oak Ridge, TN, December 1983.

[46] Kahl, W. K. and R. J. Borkowski, The In-plant Reliability Data Base for Nuclear Plant Components: Interim Report - Diesel Generators, Batteries, Chargers, and Inverters, NUREG/CR-3831, ORNL/TM-9126, Oak Ridge National Laboratory, Oak Ridge, TN, January 1985.

[47] McClymont, A. S. and B. W. Poehlman, Loss of Offsite Power at Nuclear Power Plants: Data and Analysis, EPRI NP-2301, Electric Power Research Institute, Palo Alto, CA, March 1982.

[48] Wyckoff, H., Losses of Offsite Power at U. S. Nuclear Power Plants All Years Through 1985, NSAC-103, Electric Power Research Institute, Palo Alto, CA, May 1986.

[49] Diesel Generator Reliability at Nuclear Power Plants: Data and Preliminary Analysis, (Interim Report), ERPI NP-2433, Electric Power Research Institute, Palo Alto, CA, June 1982.

[50] PORV Failure Reduction Methods - Final Report, CEN-145, CE Power Systems, Windsor, CT, December 1980.

[51] Bento, J. P., Reliability Data Book for Components in Swedish Nuclear Power Plants, RSK 85-25, Nuclear Safety Board of the Swedish Utilities for Swedish Nuclear Power Directorate, Sweden.

[52] Martz, H. F. and D. E. Whiteman, A Statistical Analysis of Nuclear Power Plant Pump Failure Rate Variability - Some Preliminary Results, NUREG/CR-3650, LA-10014-MS, Los Alamos National Laboratory, Los Alamos, NM, February 1984.

[53] Payne, A. C., et al., Interim Reliability Evaluation Program: Analysis of the Calvert Cliffs Unit 1 Nuclear Power Plant, NUREG/CR-3511, SAND82-2086, Sandia National Laboratories, Albuquerque, NM, August 1984.

[54] Kolb, G. J., et al., Reactor Safety Study Methodology Applications Program: Oconee #3 PWR Power Plant, NUREG/CR-1659/2, SAND80-1879/2, Sandia National Laboratories, Albuquerque, NM, May 1981.

[55] Carlson, D. D., et al., Reactor Safety Study Methodology Applications Program: Sequoyah #1 PWR Power Plant, NUREG/CR-1659/1, SAND80-1897/1, Sandia National Laboratories, Albuquerque, NM, February 1981.

[56] Hatch, S. W., et al., Reactor Safety Study Methodology Applications Program: Calvert Cliffs #2 PWR Power Plant, NUREG/CR-1659/3, SAND80-1879/3, Sandia National Laboratories, Albuquerque, NM, May 1982.

[57] Indian Point Probabilistic Safety Study, Power Authority of the State of New York and Consolidated Edison Company, New York, NY, 1982.

[58] Seabrook Station Probabilistic Safety Assessment, PLG-0300, Pickard, Lowe and Garrick, Irvine, CA, December 1983.

[59] "Reactor Coolant Pump Seal Failure," U. S. Nuclear Regulatory Commission Memorandum (Draft), T. E. Murley to D. G. Eisenhut, 1981, and references.

[60] Hatch, S. W., et al., Reactor Safety Study Methodology Applications Program: Grand Gulf #1 BWR Power Plant, NUREG/CR-1659/4, SAND80-1879/4, Sandia National Laboratories, Albuquerque, NM, October 1981.

[61] Big Rock Point Nuclear Power Plant Probabilistic Risk Assessment, Consumers Power Company, Jackson, MI, 1981.

[62] Feedwater Transients in Pressurized Water Reactors Designed by the Babcock and Wilcox Company, NUREG-0560, U. S. Nuclear Regulatory Commission, Washington, DC, May 1979.

[63] Generic Evaluation of Feedwater Transients and Small Break Loss of Coolant Accidents in GE-Designed Operating Plants and Near-Term Operating License Applications, NUREG-0626, U. S. Nuclear Regulatory Commission, Washington, DC, January 1980.

[64] Clarification of TMI Action Plan Requirements, NUREG-0737, U. S. Nuclear Regulatory Commission, Washington, DC, November 1980.

[65] IEEE Guide to the Collection and Presentation of Electrical, Electronic, Sensing Component, and Mechanical Equipment Reliability Data for Nuclear Power Generating Stations, IEEE-Std 500-1984, IEEE, New York, NY, 1983.

[66] Probabilistic Risk Assessment: Limerick Generating Station, Revision 4, Philadelphia Electric Company, Philadelphia, PA, June 1982.

[67] Call, A. J., et al., La Salle County Station Probabilistic Safety Analysis, NEDO-31085, Class I, General Electric Company, San Jose, CA, November 1985.

[68] Payne, A., C., et al., Analysis of La Salle Unit 2 Nuclear Power Plant: Risk Methods Integration and Evaluation Program, Volume 5, Parameter Estimate Analysis and Screening Human Reliability Analysis, NUREG/CR-4832, SAND87-7157, Sandia National Laboratories, Albuquerque, NM. (Copy of draft available in NRC Public Document Room.)

[69] Battle, R. E. and D. J. Campbell, Reliability of Emergency AC Power Systems at Nuclear Power Plants, NUREG/CR-2989, ONRL/TM-8545, Oak Ridge National Laboratory, Oak Ridge, TN, July 1983.

[70] Wheeler, T. A., et al., Analysis of Core Damage Frequency: Expert Judgment Elicitation on Internal Event Issues; Part 1 - Expert Panel Results and Part 2 - Project Staff Results, NUREG/CR-4550, Vol.2, SAND86-2084, Sandia National Laboratories, Albuquerque, NM, December 1988.

[71] Stack, D. W. A SETS User's Manual for Accident Sequence Analysis, NUREG/CR-3547, SAND83-2238, Sandia National Laboratories, Albuquerque, NM, January 1984.

[72] Iman, R. L. and M. J. Shortencarier, Fortran 77 Program and User's Guide for the Generation of Latin Hypercube and Random Samples for Use with Computer Models, NUREG/CR-3624, SAND83-2365, Sandia National Laboratories, Albuquerque, NM, March 1984

[73] Iman, R. L. and M. J . Shortencarier, A User's Guide for the Top Event Matrix Analysis Code (TEMAC), NUREG/CR-4598, SAND86-0960, Sandia National Laboratories, Albuquerque, NM, August 1986.

[74] Apostolakis, G. and S. Kaplan, "Pitfalls in Risk Calculations," Reliability Engineering, 2, pp. 135-145, 1981.

[75] Mosleh, A., et al, Procedures for Treating Common Cause Failures in Safety and Reliability Studies, NUREG/CR-4780, EPRI NP-5613, Electric Power Research Institute, Palo Alto, CA, February 1988.

[76] Welker, E. L. and M. Lipon, "Estimating the Exponential Failure Rate from Data with No Failure Events," Proceedings 1974 Annual Reliability and Maintainability Symposium, Los Angeles, CA, January 29-31, 1974.

[77] Whitehead, D. W., Recovery Actions in PRA for the Risk Methods Integration and Evaluation Program (RMIEP), NUREG/CR-4834/2 of 2, Sandia National Laboratories, December 1974.

[78] Martz, H. F., Waller, R. A., Bayesian Reliability Analysis, John Wiley and Sons, New York, New York, 1982.

APPENDIX A

SPECIAL ISSUE AND SEQUENCE ANALYSES

APPENDIX A

SPECIAL ISSUE AND SEQUENCE ANALYSES

During the course of the analyses and the development of the overall methodology, several issues were treated rather uniquely. Such issues may or may not arise in other similar probabilistic risk assessments (PRAs), however the treatment in this instance was sufficiently unique that they are presented here for future reference. The issues so treated included:

Anticipated Transient Without Scram (ATWS) for BWRs
Seal LOCA for PWRs
Steam Generator Tube Rupture (SGTR) for PWRs
PORV and ADV Block Valves for PWRs.

1.1 BWR ATWS Analysis

This section describes the Anticipated Transient Without Scram (ATWS) analysis for the BWR including the development of the ATWS Event Tree. This event tree becomes a transfer tree for all the LOCA and transient initiators with a subsequent failure of the Reactor Protection System (RES). The response of a BWR to a postulated failure to insert the control rods following an anticipated transient involves the following events. There is an initial pressure increase in the Reactor Coolant System caused by the power imbalance when the turbine is tripped. This initial pressure increase does not present an immediate danger to the integrity of the reactor for two reasons: (1) voiding is increased when the recirculation pumps are tripped and Safety Relief Valves (SRVs) begin discharging (increased voiding decreases moderator effectiveness); and (2) the SRVs can adequately control this initial pressure increase by discharging steam to the suppression pool. The power level will stabilize at some fraction of full power with or without operator action. Nevertheless, systems are initiated or actions are taken by the operators to reduce core reactivity, to achieve subcriticality, and to maintain coolant inventory.

The ATWS analysis proceeded in the following manner.

Step 1. BWR ATWS Sequence Progression

The analysts conducted a detailed study of the accident sequence progression to define the ATWS sequences. The interaction of primary system and containment system responses with the mitigating system response and operator actions were examined. This included consideration of reactor power level, pressure, and water level response versus suppression pool temperature and containment pressure when, and if, mitigating events (such as high pressure injection and standby liquid control activation) occur. This was important to identifying the critical points when systems must operate or when operator actions are required. Existing thermal-hydaulic calculations were used initially to delineate the accident progression, and any additional plant-specific calculations required were defined.

Step 2. Definition of ATWS Success Criteria

The ATWS scenarios developed by Oak Ridge National Laboratory, Idaho National Engineering Laboratory and General Electric Company[1,2,3] were reviewed to establish timing of the ATWS sequences and the operator responses and therefore the ATWS success criteria. Where appropriate and necessary, this information was supplemented with additional calculations performed using the LTAS code.[4]

These thermal-hydraulic calculations generally supplied the following information:

- effects on reactor power and suppression pool of operation with or without Standby Liquid Control (SLC),
- effects on reactor power, suppression pool, and containment with reactor water level maintained at the top of the active fuel, or at whatever level is achievable with the injection system (e.g., High Pressure Core Spray (HPCS) can maintain a level at approximately two-thirds of the core height at Grand Gulf),
- effects of reactor depressurization on reactor power, suppression pool, and containment,
- effects on suppression pool and containment if Main Steam Isolation Valves (MSIV) close, and
- effects of low pressure injection on primary system integrity if SLC fails,
- effects of containment pressurization and Residual Heat Removal (RHR) and/or venting on Automatic Depressurization System (ADS) and low pressure injection.

Step 3. ATWS Event Tree Development

Based upon the information gathered in Steps 1 and 2, the critical ATWS events were identified. Some examples of these top events are shown below. These event names may be, and are, altered to reflect plant-specific events where appropriate. Some specific examples of this are cited later. This particular set was used in the Peach Bottom analysis.[5]

T	Transient initiating event requiring reactor trip.
RPSM/E	Success or failure of the Reactor Protection System mechanical portions or electrical portions.
ARI	Success or failure of the Alternate Rod Insertion system.

RPT Success or failure of a trip of the recirculation pumps either automatically or manually.

ROD Success or failure of manual rod insertion.

M Success or failure of overpressure protection by the safety relief valves.

SLC Success or failure of the Standby Liquid Control system in achieving timely subcriticality.

I Success or failure to inhibit the Automatic Depressurization System (ADS).

U1 Success or failure of the High Pressure Coolant Injection (HPCI) system.

X1 Success or failure of reactor depressurization.

V Success or failure of low pressure systems to cool the core.

W Success or failure of the Residual Heat Removal (RHR) system in the suppression pool cooling or containment spray modes.

As noted earlier, it is often advantageous to alter the nomenclature to reflect plant-specific issues or concerns. For example, in the Grand Gulf analysis[6] the SLC event is divided into four events. These deal with success or failure of the operator to initiate SLC early in the accident (C'), or late in the accident (C'') and success or failure to inject 86 gpm of borated water (C3) or 43 gpm of borated water (C4).

Obviously, some of these top events involve operator actions. There are certain operator actions, in fact, that are critical to the mitigation of an ATWS initiating event that are more than the simple "initiation" of a system. These types of actions become top events and generally require detailed analysis.

Once the top events are defined and the success criteria established, the ATWS event tree can be developed. The actual development follows the steps outlined in Section 4,* namely:

Obtain Information
Identify Event Tree
Identify and Order Events
Identify Dependencies
Construct Initial Systemic Event Tree
Simplify Event Tree
Identify Event Tree Transfers
Resolve Core Vulnerable Sequences

*Section references are to the main body of this report.

It should be noted that, in this particular instance, the resolution of core vulnerable sequences was actually accomplished as part of the back-end analysis, although this would normally be part of the front-end analysis.

An example event tree (Peach Bottom Unit 2) is shown in Figure 1.1. Because the ATWS event tree is complex, two sequences are discussed here to illustrate the development of the event tree. For this purpose consider Sequences 6 and 11:

(6) T * RPSM * /RPT * /M * /SLC * /I * /U1 * /W

In Sequence 6 a transient occurs that requires the reactor to scram (T). The mechanical RPS fails (RPSM) which eliminates any possibility of scramming the reactor or manually inserting the control rods. The recirculation pumps are tripped (/RPT) and the SRVs properly cycle to control reactor pressure (/M). SLC is successfully initiated to inject borated water into the reactor to reduce reactivity (/SLC). The ADS valves are inhibited (/I) to maintain sufficient reactor pressure to initiate HPCI for coolant makeup (/U1). The RHR system is initiated in the SPC or CSS mode (/W) to cool the containment. The result is a safe core and containment. [Note: The slash preceding the system designator indicates success.]

(11) T * RPSM * /RPT * /M * /SLC * /I * U1 * X1

Sequence 11 is the same as Sequence 6 until HPCI (U1) fails. The reactor depressurization fails (X1) and core cooling is lost. This results in core damage in a vulnerable containment.

Step 4. BWR ATWS Human Reliability Analysis

Once the accident sequences were defined, the operator actions were also identified. Human reliability analysts then performed an extensive Human Reliability Analysis (HRA) of the operations staff for the postulated ATWS accident sequences. This analysis involved several substeps.

Step 4.1. ATWS HRA Information Requirements

Visits were made to the plant and the training simulators for the purpose of acquiring plant-specific information on training, procedures (normal and abnormal operations), human engineering aspects of the control room, and experience and education levels of the staff. Discussions were held with training instructors and reactor operators. Where possible, the HRA analysts observed the operators executing the ATWS scenarios on the plant simulator. Training manuals and emergency and off-normal operating procedures were reviewed.

If necessary, thermal-hydraulic runs (using the LTAS code[4]) were performed for various scenarios to determine sequence timing.

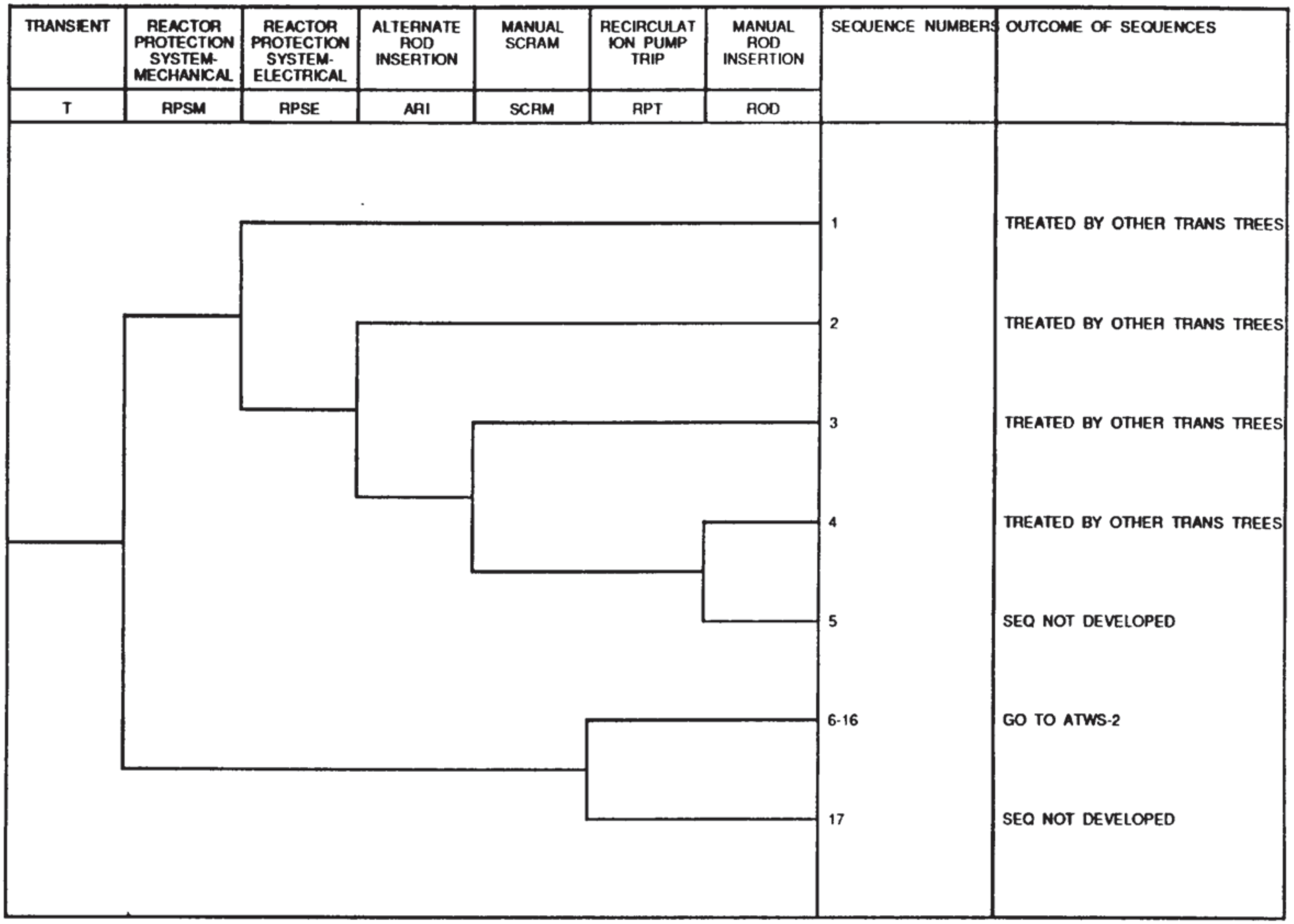


Figure 1.1-1. Anticipated Transient Without Scram Event Tree
(Page 1 of 2)

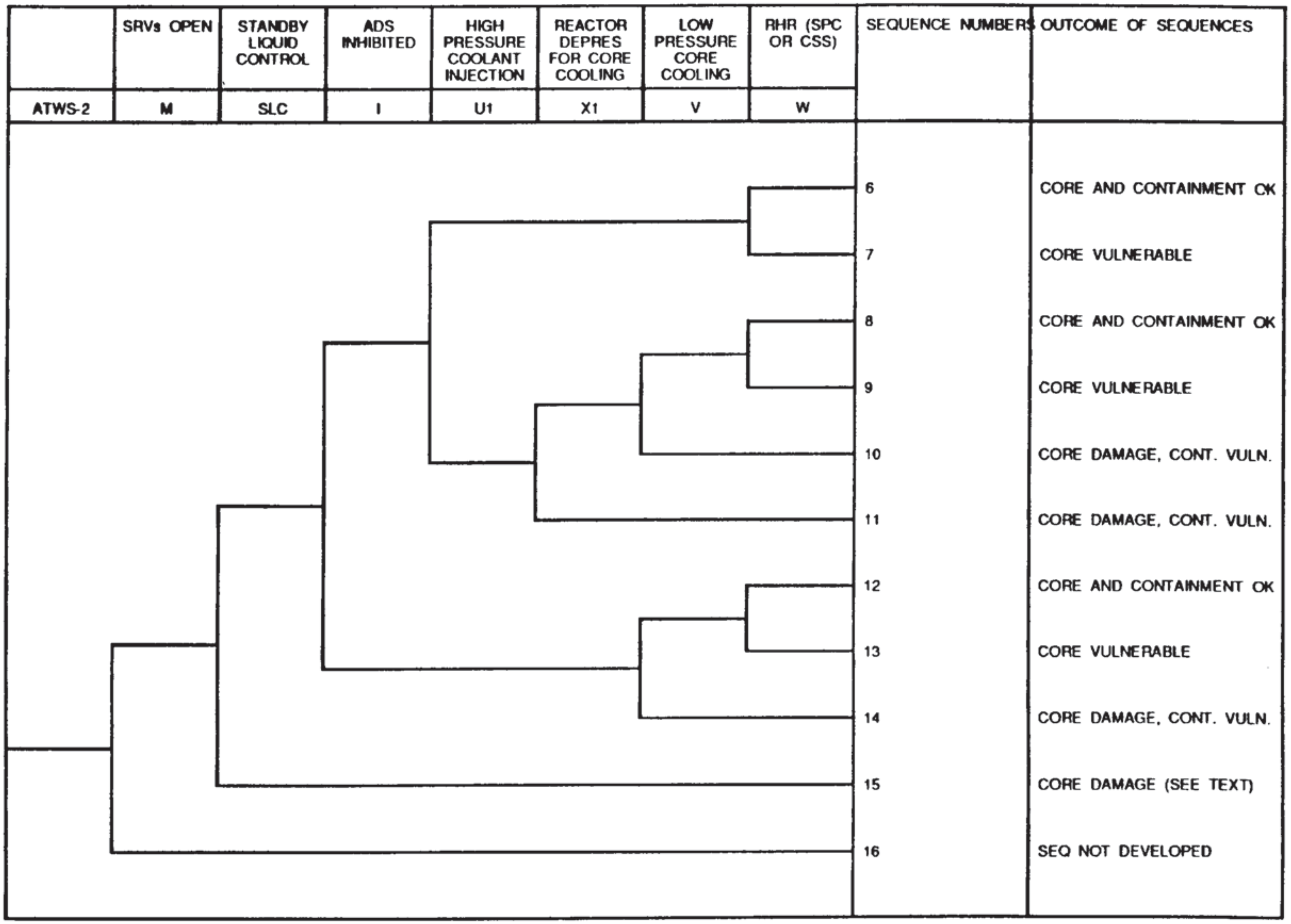

ATWS-2
SRVs OPEN
M
STANDBY LIQUID CONTROL
SLC
ADS INHIBITED
I
HIGH PRESSURE COOLANT INJECTION
U1
REACTOR DEPRES FOR CORE COOLING
X1
LOW PRESSURE CORE COOLING
V
RHR (SPC OR CSS)
W
SEQUENCE NUMBERS
OUTCOME OF SEQUENCES
6 CORE AND CONTAINMENT OK
7 CORE VULNERABLE
8 CORE AND CONTAINMENT OK
9 CORE VULNERABLE
10 CORE DAMAGE, CONT. VULN.
11 CORE DAMAGE, CONT. VULN.
12 CORE AND CONTAINMENT OK
13 CORE VULNERABLE
14 CORE DAMAGE, CONT. VULN.
15 CORE DAMAGE (SEE TEXT)
16 SEQ NOT DEVELOPED

Figure 1.1-1. Anticipated Transient Without Scram Event Tree
(Page 2 of 2)

Step 4.2. Analysis of Operator Tasks for ATWS

The major operator tasks (from Step 3) for which human error probabilities were needed were identified by the HRA analysts. A detailed task analysis was performed based upon staffing, team interactions, and control room layout. Preconditions for each task could differ as a result of the success or failure of previous tasks or safety systems. Each set of preconditions and relevant performance shaping factors were considered when the human error probabilities were assigned to each operator task. A number of references were available to assist in the quantification process for each plant. The principal ones being the Accident Sequence Evaluation Program Human Reliability Analysis Procedures,[7] Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications,[8] and A Human Reliabiltiy Analysis for the ATWS Sequence with MSIV Closure at the Peach Bottom Atomic Power Station.[9]

Step 5. BWR ATWS Quantification

The ATWS quantification differs from the other sequence quantification discussed in Section 10 of this report. The ATWS quantification was accomplished in two steps as discussed below.

Step 5.1. Identification of Dominant ATWS Sequences

Initially, the Boolean expressions for the top event systems were combined with the sum of the potential transient initiating event frequencies using the SETS code.[10] Based upon these results, those ATWS sequences which were below the selected truncation value (typically 1E-8/yr) even with all the initiating events combined were deleted. Next, the analyst reviewed the cut sets in the retained sequences and segregated them by initiator. That is, the analyst decided which systems were required to respond to a particular initiator. These cut sets were then combined with the individual initiator frequency to obtain a sequence frequency for each initiating event. Again, the results were reviewed and those sequences with frequencies below the truncation value deleted. The remaining cut sets were evaluated for possible recovery actions and requantified.

The dominant sequences were then identified. The value used to determine dominance can differ between plants, that is, the truncation value may have to change to avoid discarding significant sequences prematurely. As noted above, truncation values were typically on the order of 1E-8/yr.

Step 5.2. Identification of ATWS Sequence Cut Sets

The next step in the ATWS quantification was to establish the cut sets for the dominant sequences. For each dominant sequence defined in Step 5.1, the dominant cut sets (i.e., the cut sets comprising at least ~90% of the system unavailability) were identified. The dominant cut sets for each system of the sequence were combined with the operator events to form the sequence cut sets. For example, using Sequence 11 identified in Step 3, the system top events were as follows:

RPSM	Failure of mechanical aspects of the RPS
/RPT	Success of recirculating pump trip
/M	Success of overpressure protection
/SLC	Success of standby liquid injection
/I	Success of ADS inhibit
U1	Failure of high pressure injection
X1	Failure of reactor depressurization

A system model was only developed for event U1, the other events were represented by "black boxes" (See Section 5) or operator actions. The dominant cut sets for U1 were:

HCI-TDP-FS-20S37	Turbine driven pump (TDP) fails to start
HCI-TDP-MA-20S37	TDP out for maintenance
HCI-TDP-FO-20S37	TDP fails to run for 1 hour
HCI-MOV-CC-MV14	Motor operated valve (MOV) 14 fails to open
HCI-MOV-CC-MV19	MOV 19 fails to open
HCI-MOV-MA-PCV50	Pressure control valve 50 out for maintenance
HCI-MOV-MA-MV14	MOV 14 out for maintenance
HCI-MOV-MA-MV17	MOV 17 out for maintenance
HCI-MOV-MA-MV57	MOV 57 out for maintenance
HCI-MOV-MA-MV20	MOV 20 out for maintenance
HCI-ICC-HW-FC108	Flow controller fails
HCI-CKV-HW-CV65	Check valve (CV) 65 fails to open
HCI CKV-HW-CV32	CV 32 fails to open
HCI-CKV-HW-TCV18	Test check valve 18 fails to open

The operator action top event for this sequence was:

ESF-XHE-FO-DATWS	Operator fails to depressurize.

Therefore, the most dominant cut sets (top five) for this sequence, with the initiator a transient with PCS available and successes approximated as 1.0, became:

IE-T3A*NR*RPSM*/RPT*/M*/SLC*/I*ESF-XHE-FO-DATWS*HCI-TDP-FS-20S37

IE-T3A*NR*RPSM*/RPT*/M*/SLC*/I*ESF-XHE-FO-DATWS*HCI-TDP-MA-20S37

IE-T3A*NR*RPSM*/RPT*/M*/SLC*/I*ESF-XHE-FO-DATWS*HCI-TDP-FO-20S37

E-T3A*NR*RPSM*/RPT*/M*/SLC*/I*ESF-XHE-FO-DATWS*HCI-MOV-CC-MV14

IE-T3A*NR*RPSM*/RPT*/M*/SLC*/I*ESF-XHE-FO-DATWS*HCI-MOV-CC-MV19

Step 5.3. ATWS Plant Damage States

Once the dominant ATWS sequences (and the associated cut sets) were obtained, the "front-end" and "back-end" analysts jointly examined the cut sets to determine the ATWS plant damage states. The cut sets were re-grouped appropriately into the various damage states (see Section 11 for a discussion of plant damage states) which were then quantified. These damage states were fully quantified using the mean values and the TEMAC code[11] to obtain the mean estimate for core damage. Later in the analysis, uncertainty estimates and sensitivity analyses were also quantified using the TEMAC code (see Section 12).

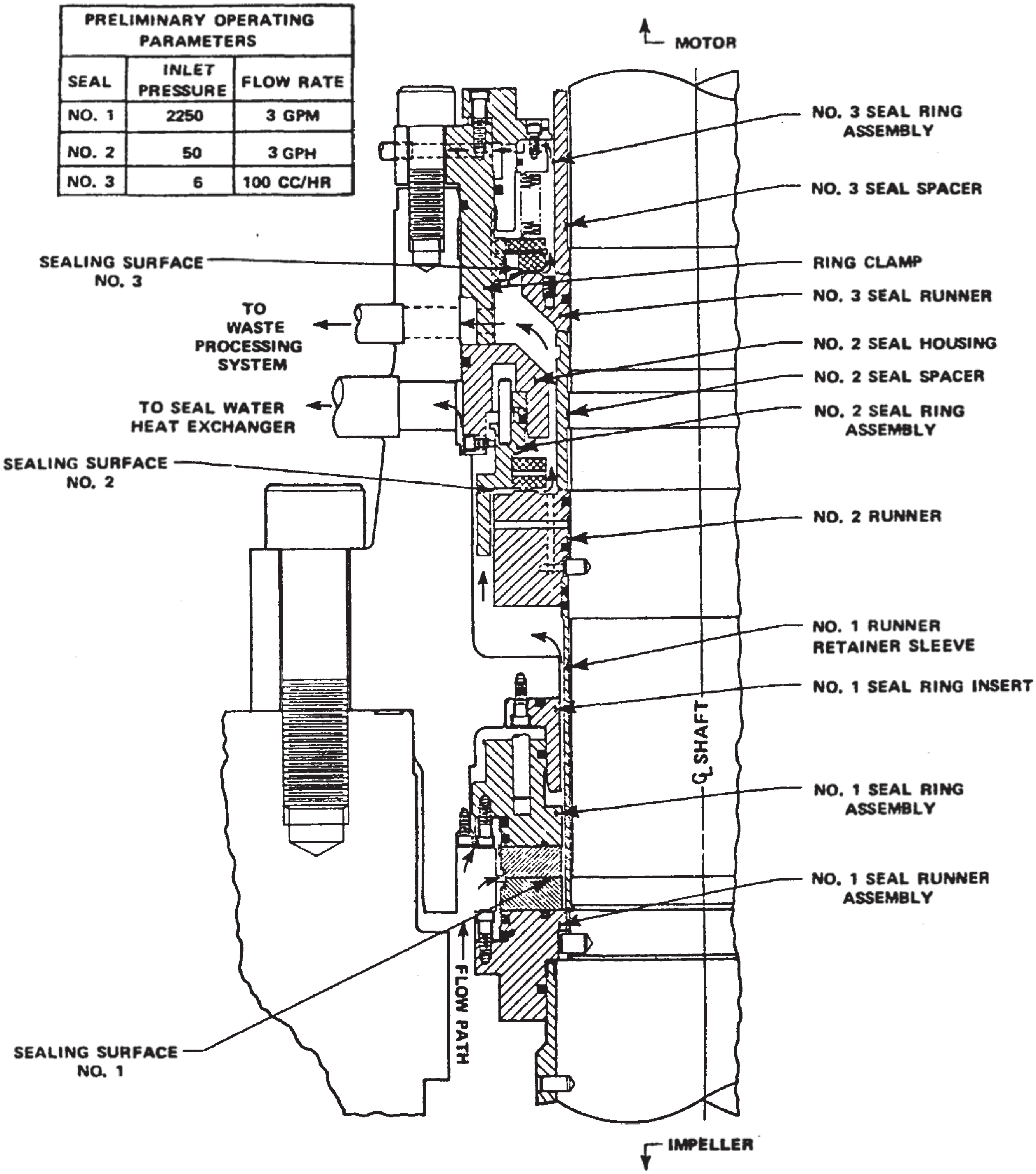
1.2 PWR Seal LOCA Analysis

This section describes the PWR seal LOCA analysis including the elicitation of expert judgment on LOCA probabilities. The performance of reactor coolant pump (RCP) seals during off-normal conditions such as a loss of seal cooling is a concern for PWRs. Because only Westinghouse PWRs are being analyzed in NUREG-1150, this discussion is limited to that RCP design.

1.2.1 Discussion of Seal Performance and Failure

The Westinghouse RCP shaft seal is a three-stage seal assembly, as shown in Figure 1.2-1. The number one seal is a film-riding controlled leakage seal, whereas the number two and three stages are rubbing-face type seals. The normal operational leakage (approximately 3 gpm) across the number one seal cools the seal assembly. This high pressure subcooled leakage is supplied by an injection system upstream of the seal. Part of the injection water flows through the seal assembly and the remainder flows into the reactor coolant system as makeup water. Backup cooling is provided by a water-to-water heat exchanger parallel to the labyrinth seal (Seals 1 and 2).

During a prolonged station blackout, both injection and cooling water would be lost. High pressure reactor coolant water would then flow up the shaft into the seal system. The shaft and the seal assembly would experience abnormal temperature distributions. This condition will



PRELIMINARY OPERATING PARAMETERS		
SEAL	INLET PRESSURE	FLOW RATE
NO. 1	2250	3 GPM
NO. 2	50	3 GPH
NO. 3	6	100 CC/HR

RCP Typical Shaft Seal Arrangement

Figure 1.2-1. Westinghouse RCP Seal Assembly

affect the angle between the face plates of the RCP seals and the gap between the faceplates of the number one film-riding seal. This is expected to increase the leakage to approximately 21 gpm, a flow rate considered to be acceptable in terms of coolant loss. However, there is concern that without adequate cooling, the shaft seals could fail to restrict the flow to 21 gpm, and that leakage up to a maximum of 480 gpm per pump could result. The basis for this concern is discussed below.

The gap between the number one seal faceplates is established by a force balance, which can be affected by flow rate, the angle between the faceplates of the seal ring and runner, enthalpy, and inlet pressure. The fluid pressure profile between the seal faceplates determines the opening forces on the seal. The closing force on the seal is proportional to the differential pressure across the seal and acts on the upper surface of the seal ring. If these forces are unbalanced, the gap will increase or decrease as necessary, until the forces are balanced. The number two seal stage is designed to withstand full system pressure without loss of integrity in the event that the number one seal stage fails. But, in the event both number one and number two seals fail, the number three seal stage is not expected to limit leakage.

1.2.2 Question for Elicitation

The question or issue addressed in the elicitation process involved the failure probability of the Westinghouse RCP shaft seals and the resultant leak rates under station blackout conditions. Thus, the panel dealt with the leak rate, in gallons per minute as a function of time, resulting from seal failure caused by the loss of cooling to the pump shaft. This situation is expected under prolonged station blackout conditions. The hypothesized failure modes involved loss of the seal ring geometry, and degradation of the elastomer material of the o-rings. The size of the resultant leak is dependent upon the combination of seal ring failure and o-ring failures in the various seal stages.

The issue was put before a panel of experts especially familiar with the design of these pump seals and knowledgeable about operating and experimental experience regarding the seals.[12] The first step was the generation of a single RCP logic tree which, by consensus of the panel, describes the possible failure combinations of seal rings and o-rings and the resultant leak rates. This logic tree is shown in Figure 1.2-2.

The experts then provided estimates of the failure probabilities for the four events of the tree. Estimates were provided for two different elastomers because the older material (used at Surry and Sequoyah) has exhibited significant degradation in some experiments. A new elastomer has exhibited much less degradation under similar conditions. In addition to two seal materials, the issue was also addressed for two scenarios on primary system status; with and without cooldown (depressurization) within four hours after the onset of the loss of RCP cooling. Successful depressurization means the seals will be subject to cooler, less harsh conditions.

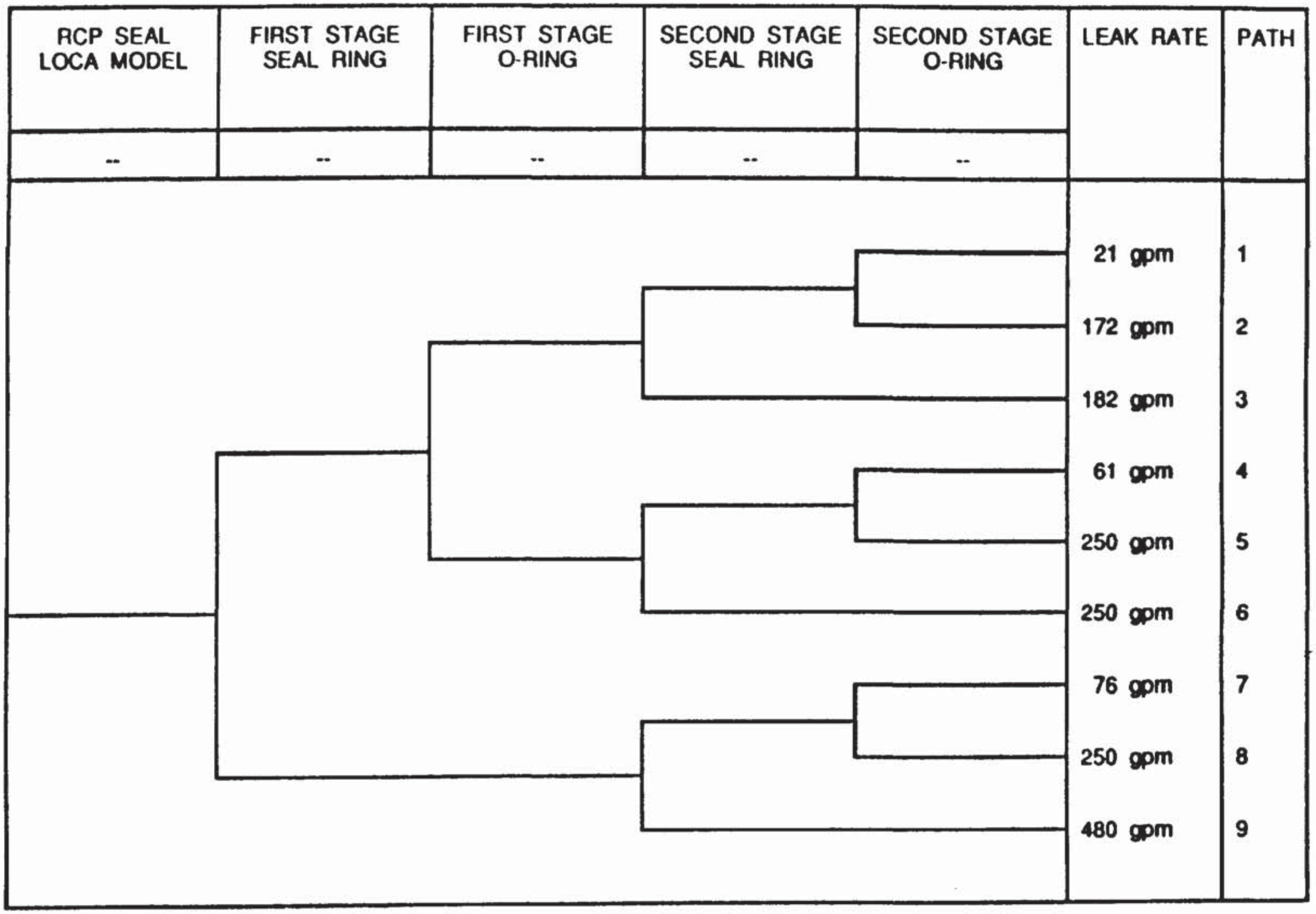


Figure 1.2-2. Decision Tree for RCP Seal Issues (One Assembly)

Once the failure of a single RCP seal assembly had been addressed and failure rates for the various components established, the relationship of seal component failures between pumps was evaluated. Because Westinghouse PWRs may have up to four steam generator loops with an RCP for each, the probability of a combined leak rate from all of the pump seals is the resolution of the issue. The question considered was:

> If one RCP seal assembly fails by a specific combination of faults of the seal rings and o-rings, will any or all of the other RCP seal assemblies experience a similar failure?

Thus, this issue addressed whether or not the heat and pressure stresses induce a common cause failure of the seal rings and o-rings. Although the experts developed very different assessments for correlating failures between components there was one consensus reached; if two similar components in two pumps failed (e.g., first stage seal rings in two pumps) then the same component could be assumed to fail in all other pumps. This reduced the estimation of the total probabilities to determining the failure combination for a two pump model.

The logic tree (Figure 1.2-2) was expanded for each expert to model the failure relationships between two pumps. Each expert's tree was quantified using his proposed failure rates and correlation of components between pumps. The trees were quantified for various points in time after loss of cooling because the experts believed that o-ring failure probability would increase with time. The individual results were averaged to calculate aggregated leak rates and their probabilities. Three specific cases were considered:

1. Old o-ring material - with primary cooldown
2. Old o-ring material - without primary cooldown
3. New o-ring material - without primary cooldown.

The seal LOCA models were not quantified for the case with the new o-ring material without primary cooldown because the models are only weakly dependent on whether cooldown occurs, although some differences do show up long after battery depletion would have become a more serious problem. With the new o-ring material, face seal stability dominates the models. Three-loop plant results are shown on Table 1.2-1, the results for a four-loop plant may be found in Reference 12.

1.2.3 Integration of Seal LOCA Model into Station Blackout Sequences

The prediction of RCP seal behavior under loss of all seal cooling conditions is an integral part of station blackout model development in the front-end analysis. The starting point for the seal LOCA model development is Table 1.2-1 (using Surry[13] as the example). The leak rates reported represent total leakage from all three pumps. Different leak sizes were used to represent different combinations of stage failures in the three pumps. The changing probabilities with time indicate increasing leak rates.

Table 1.2-1. Aggregated RCP Seal LOCA Probabilities - Three Pumps (Adapted from Reference 12)

Leak Rate	Old O-Rings Time (Hrs.)					New O-Rings Time (Hrs.)				
(gpm)	1.5	2.5	3.5	4.5	5.5	1.5	2.5	3.5	4.5	5.5
63	.306	.290	.274	.274(.2580)*	.274(.241)	.817	.816	.814	.812	.811
103	-	-	-	-	-	7.7E-3	7.7E-3	7.7E-3	7.7E-3	7.7E-3
183/224	.148	.0370	.0502	.0478(.0640)	.0466(.0790)	.0136	.0142	.0157	.0173	.019
294	-	-	-	-	-	1.9E-3	1.9E-3	1.9E-3	1.9E-3	1.9E-3
372	8.5E-3	5.0E-3	4.5E-3	3.7E-3	3.3E-3	4.5E-4	5.0E-3	5.3E-3	5.7E-3	6.0E-3
425	-	-	-	-	-	1.9E-3	1.9E-3	1.9E-3	1.9E-3	1.9E-3
516/526/546	3.5E-4	3.4E-4	3.2E-4	3.2E-4	3.2E-4	.145	.145	.145	.145	.145
602/614	.001	0	0	0	0	4.7E-4	4.7E-4	4.7E-4	4.7E-4	4.7E-4
750	.530	.660	.660	.660	.660	7.7E-3	7.7E-3	7.7E-3	7.7E-3	7.7E-3
1440	4.3E-3	4.3E-3	4.3E-3	4.3E-3	4.3E-3	5.0E-3	5.0E-3	5.0E-3	5.0E-3	5.0E-3

*Parentheses denote calculations which change if no depressurization is assumed.

These values are the probabilities of being at a particular leak rate at a particular time.

The key to use of this data is to be able to calculate a time of LOCA onset and subsequent core uncovery for each possible failure scenario. Therefore, it is necessary to define a series of individual scenarios or pathways which identify the time of seal failure, the variation of leak rate, and the probability of these pathways. Initially a total of twenty pathways were identified that included the initial leak rate, the time of initial seal failure, any increases in leak rate, the time at which leak rate increases, and the probability of each pathway. These twenty pathways were consolidated into eight states in order to simplify the sampling of uncertainty. There were seven failure states and one success state. These are summarized as follows:

Leak Rate (gpm)	Time to Leak Rate Increase (hrs)	Probability
750 C	1 1/2	0.5302
183 - 750	2 1/2	0.1270
183 C	2 1/2	0.0161
183 C	3 1/2	0.0161
1440 C	1 1/2	0.0043
183 C	1 1/2	0.0140
372 - 750	2 1/2	0.0040

C - Constant leak rate

The seal LOCA model was then integrated into the station blackout event trees. Two constraining criteria were imposed: 1) consideration of non-recovery of AC power would be separate from that for seal LOCA, and 2) a minimum number of events would be used.

Seal LOCAs (SLOCAs) are caused by loss of all seal cooling. At 90 minutes after loss of all cooling, it is believed that the seal temperatures have increased enough for the seal to be at risk of failure. Prior to 90 minutes there is no risk of seal failure. After 90 minutes, with no cooling, the seal may fail or may remain intact. It may develop a small leak which increases with time, or it may have a constant leak rate. If a seal LOCA occurs, core uncovery can be averted if AC power is restored, thus enabling restoration of safety injection flow.

The mathematical development of the core damage frequency due to seal LOCA is as follows:

Probability Core Damage	=	Probability at risk for SLOCA	*	Probability SLOCA Occurs	*	Probability No recovery of AC Prior to Core Uncovery

The probability of being at risk for a SLOCA is the probability that AC power has not been restored within 90 minutes of a loss of seal cooling. The probability of SLOCA is established by expert elicitation. All scenarios are assumed to start at 90 minutes from loss of cooling. Finally, the probability of not recovering is just the probability of non-recovery of AC power prior to the characteristic core uncovery time in developing this probability, it must be conditional on non-recovery of AC in the first 90 minutes. The core damage equation can be written:

$$\text{Probability CD} = \sum_{i=1}^{8} P_{NRAC}(t) * f_{SL_i}(t) * C_{NRAC}(t + \lambda_i)$$

where: i = seal LOCA scenario index, and t, in this case, equals 90 minutes.

λ_i = core uncovery time associated with break size

$f_{SLi}(t)$ = probability of ith seal LOCA scenario at time t, from loss of all seal cooling

$P_{NRAC}(t)$ = probability of non-recovery of AC power by time t, given loss of power at $t = 0$.

$P_{NRAC}(t) = 1 - F_{NRAC}(t)$, where F is the cumulative probability of recovery of AC power.

$C_{NRAC}(t + \lambda)$ = conditional probability of non-recovery of AC power by time $t + \lambda$, given no recovery at time t.

$$C_{NRAC}(t + \lambda) = \frac{P_{NRAC}(t + \lambda)}{P_{NRAC}(t)} = \frac{1 - F_{NRAC}(t + \lambda)}{1 - F_{NRAC}(t)}$$

recognizing the form for C_{NRAC}, the equation reduces to:

$$\text{Probability CD} = \sum_{1=i}^{8} f_{SLi}(t) * P_{NRAC}(t + \lambda_i)$$

The values for f_{SLi}, λ_i, and $P_{NRAC}(t + \lambda_i)$ are shown in Table 1.2-2. Core uncovery times were calculated for Surry with and without secondary depressurization. The complete tabulation is reported in Appendix D of Reference 13.

It is recommended that all analysts consult Reference 12 for more detail on the elicitation process on RCP Seal LOCA. Likewise, either Reference 13 or 14 may be considered for more detail on the incorporation of the results of the elicitation into the plant models.

Table 1.2-2 Reduced Surry RCP Seal LOCA Model Results
(Adapted from Reference 13, Appendix D)

Leak Path	Time to		Time to	Time to	Prob.	Prob.
(gpm)	Transfer	Prob.	CU (hrs)	RAC (hrs)	NRAC	CD
	(hrs)		(with secondary depressurization)			
		f_{SLi}	i		$P(t+\lambda)$	
750 C	1 1/2	0.5302	2.07	3.6	0.138	0.07317
183 - 750	2 1/2	0.1270	2.75	4.3	0.018	0.01372
183 C	2 1/2	0.0161	12.0	13.5	0.05	0.00081
183 C	3 1/2	0.0161	12.2	13.7	0.05	0.00081
1440 C	1 1/2	0.0043	0.97	2.5	0.21	0.00091
183 C	1 1/2	0.0140	10.9	12.4	0.05	0.00070
372 - 750	2 1/2	0.0040	2.6	4.1	0.115	0.00047
						0.09059

Notes to Table:

Core Damage Probability is ~ 99% of the total for 20 pathways

C - Constant leak rate
CU - Core Uncovery RAC - Recovery of AC power
NRAC -Non-recovery of AC power
CD - Core Damage

1.3 Steam Generator Tube Rupture

In the initial NUREG-1150 studies, steam generator tube rupture (SGTR) was considered as a potential initiating event but, based upon a limited screening analysis suggesting a very minimal contribution to core damage frequency, it was dropped from further consideration. Some reviewers were quite critical of that decision in light of the results of other assessments. On the other hand, there are analysts who argue that SGTR is not an issue because it is an isolatable event. Given this dichotomy of opinion, SGTR was treated explicitly in the reanalysis, and it did, in fact, contribute to the core damage frequency for the PWRs.

1.3.1 The SGTR Accident Progression

The SGTR initiator is treated as a transient, but it is a transient that is unique because it causes a breach of the primary pressure boundary into the secondary side pressure boundary. The SGTR initiator is a double-ended rupture of a single tube which results in a primary coolant outflow that requires a makeup flow of approximately 600 gpm. With such an outflow, safety injection (SI) will actuate on low pressurizer pressure, shortly after the rupture occurs. Turbine trip, main feedwater isolation and auxiliary feedwater (AFW) start will occur on the SI signal.

The operator is instructed to identify and isolate the affected steam generator. Isolation of the affected steam generator involves closure of the main steam isolation valves (MSIV), the AFW inlet valve, the steam generator blowdown line, and turbine driven pump steam admission valve. Complete isolation will not occur until the reactor coolant system (RCS) pressure is reduced below that of the steam generator. The water level in the affected steam generator will continue to rise due to the influx of water through the break. The pressure in this steam generator will also rise as the average steam generator water temperature increases.

The operator is then instructed to cool down the RCS as rapidly as possible using the good steam generators and then to depressurize the RCS using the pressurizer sprays, or by opening a power operated relief valve (PORV), to reduce the RCS pressure below that of the steam generator. This will terminate the break flow. At this point, with the pressure in the RCS less than that in the steam generator, the steam generator isolated, and AFW flow being provided to the other steam generators, the system is stable and under control. Subsequent activities to cool the affected steam generator and to put the reactor in cold shutdown are not included in this analysis.

1.3.2 SGTR Event Tree Development

Once the decision was reached to treat SGTR explicitly, the analysis followed the methodology outlined elsewhere in this report. Only selected portions of the analysis are presented here in order to highlight specific features.

An event tree for SGTR is shown in Figure 1.3-1 and the event names are defined in Table 1.3-1. The corresponding success criteria are given in Table 1.3-2. As noted above, this initiator is unique in that it involves a breach of the primary pressure boundary into the secondary pressure boundary. As a result, success criteria involved with integrity of the primary pressure boundary become enmeshed with the necessity of preserving the secondary side pressure boundary. The two systems now form a continuous pressure boundary and must therefore be maintained at pressures consistent with secondary side criteria. Normally open effluent lines to the steam generator must be isolated because they now represent open lines to the primary system.

The three functions required in response to SGTR are reactor scram, core heat removal, and operator control of RCS pressure. If all of these functions are provided, the transient is mitigated at an early stage. As described earlier, operator control of RCS pressure requires RCS cooldown using heat removal through the good steam generators, and depressurization of the primary system using the pressurizer sprays or opening a PORV.

Failure to trip the reactor (automatically or manually) causes the pressure in the RCS to increase, potentially resulting in the rupture of other steam generator (SG) tubes with a resultant increase in flow from the RCS to the secondary system. This induced pressure increase is counter productive to the RCS depressurization required to mitigate tube rupture. Because of the complexity of this particular sequence, SGTR with a failure to scram was conservatively considered to be a core damage sequence.

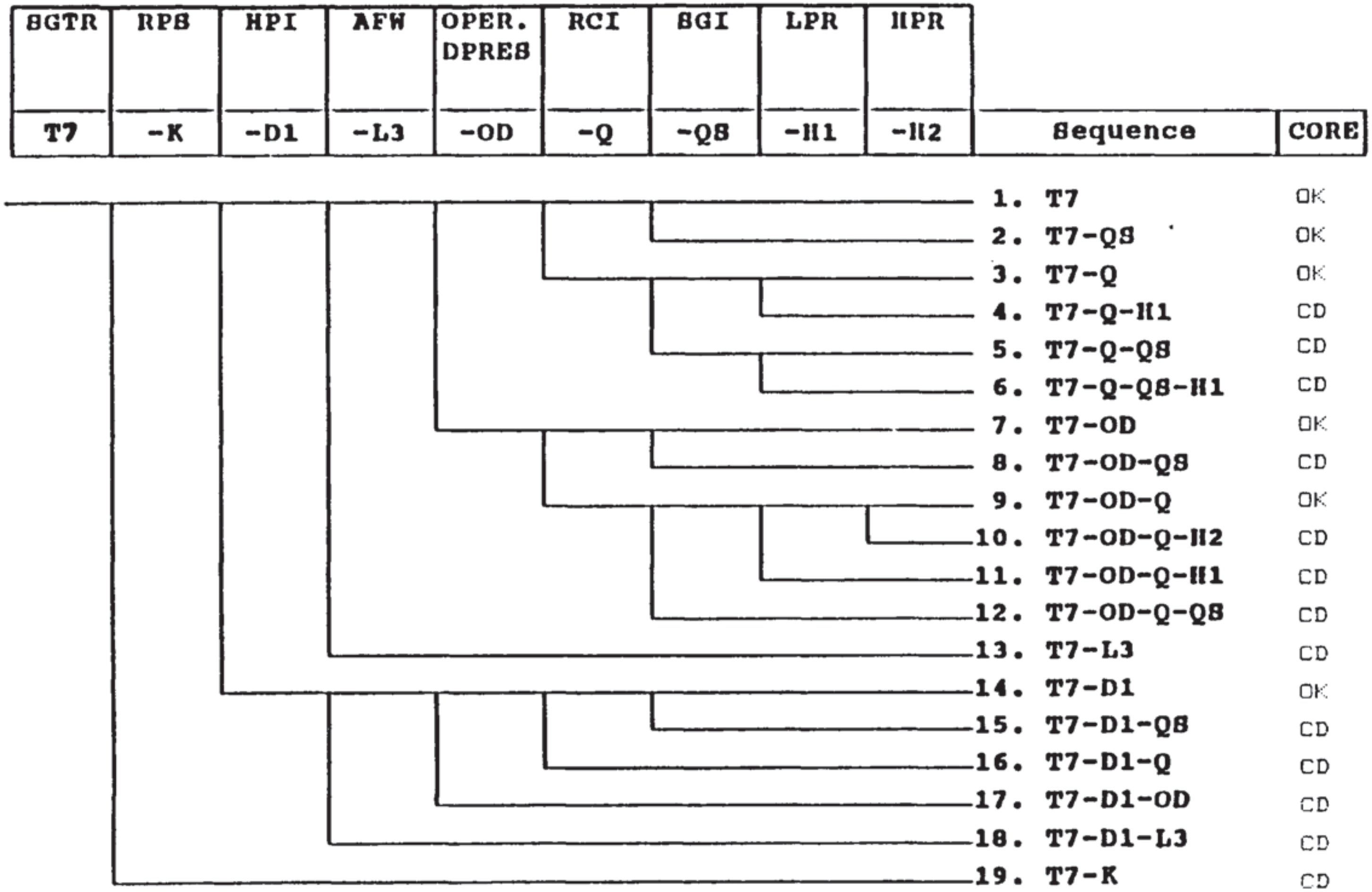
1.3.3 Discussion of the SGTR Sequences

The event tree presented in Figure 1.3-1 is based upon the Surry analysis.[13] The details of the events may vary slightly from plant to plant but this illustrates the key points. The analysis led to the definition of nineteen sequences which are discussed below.

<u>Sequence 1</u> - This sequence represents successful mitigation of the initiator. Primary and secondary side pressures have been equalized thereby mitigating the break flow. SG integrity, and concurrently RCS integrity, have been maintained and heat removal is provided by the good steam generators.

<u>Sequence 2</u> - This sequence represents a failure of the SG integrity. However, it was classified as a safe state even though it violates the success criteria because the time of the sequence extends it beyond the 24 hour mission time used in the analysis. This results from the successful depressurization of the RCS with the attendant reduction in leak rate and extension of the time before injection water sources are depleted.

<u>Sequence 3</u> - This sequence represents a loss of primary system integrity as a result of a stuck open PORV, but successful coolant recirculation from the containment sump using LPR after depletion of the refueling water storage tank (RWST) by the SI flow. Secondary side integrity is



Sequence	CORE
1. T7	OK
2. T7-QS	OK
3. T7-Q	OK
4. T7-Q-H1	CD
5. T7-Q-QS	CD
6. T7-Q-QS-H1	CD
7. T7-OD	OK
8. T7-OD-QS	CD
9. T7-OD-Q	OK
10. T7-OD-Q-H2	CD
11. T7-OD-Q-H1	CD
12. T7-OD-Q-QS	CD
13. T7-L3	CD
14. T7-D1	OK
15. T7-D1-QS	CD
16. T7-D1-Q	CD
17. T7-D1-OD	CD
18. T7-D1-L3	CD
19. T7-K	CD

Figure 1.1.1. Steam Generator Tube Rupture Event Tree
(Adapted from Reference 13)

Table 1.3-1 Definition of Terms for SGTR Event Tree (Adapted from Reference 13)

Term or Symbol	Definition
SGTR (T7)	Steam Generator Tube Rupture
RPS (K)	Reactor Protection System
HPI (D1)	High Pressure Injection
AFW (L3)	Auxiliary Feedwater
OPER DPRES (OD)	Operator Depressurizes
RCI (Q)	Reactor Coolant Integrity
SGI (QS)	Steam Generator Integrity
LPR (H1)	Low Pressure Recirculation
HPR (H2)	High Pressure Recirculation

Table 1.3-2 SGTR Transient Success Criteria Summary Information (Adapted from Reference 13)

Function	Success Criteria
REACTOR SUBCRITICALITY	Reactor Protection System (Auto/Manual)
CORE HEAT REMOVAL -EARLY	1 of 3 AFW Pumps to 1 of 2 SGs
RCS INTEGRITY	Depressurize RCS below SG Relief Valve Setpoint and isolate: MSIV, SG Blowdown line, steam line to turbine driven pump and steam line to DHR valve
CONTAINMENT PRESSURE SUPPRESSION	Not Applicable
CORE HEAT REMOVAL -LATE	AFW
CONTAINMENT ATMOSPHERE HEAT REMOVAL	Not Applicable
COMMENTS:	Definition of RCS boundary expanded to include SG; hence SG integrity must be considered also.

maintained preserving coolant inventory and allowing heat removal through the steam generators. Because the reactor has been depressurized previously in response to the tube rupture, it was assumed further depressurization would be possible thus eliminating the need for high pressure recirculation.

Sequence 4 - This sequence is similar to Sequence 3 except that failure to switch to LPR from the sump results in core damage.

Sequence 5 - This sequence represents an unmitigated loss of coolant inventory which ultimately prevents recirculation from the sump. The loss of RCS integrity early in the sequence requires recirculation from the sump, while the loss of SG integrity results in continued loss of coolant inventory to the atmosphere. The eventual depletion of the sump will result in cavitation (failure) of the LPR pumps, resulting in core uncovery. Recovery of this sequence is possible through refilling of the RWST or cross connects to the second unit RWST.

Sequence 6 - This sequence in similar to Sequence 5, but represents failure of coolant recirculation due to failures in the LPR system. Recovery is possible with continued safety injection using water sources at the second unit.

It should be noted that because the operator has depressurized in Sequences 3 through 6, break flows are low enough to provide substantial time for operator recovery actions such as providing alternate sources of coolant for injection. In contrast, in Sequences 7 through 12, the operator has failed to depressurize and the inventory loss rates are much higher.

Sequence 7 - This sequence represents a mitigated SGTR with failure to depressurize the reactor. The probability of this state is very low due to the provision of safety valves on the steam generators, all of which would have to fail closed in order to fulfill the requirements of this state.

Sequence 8 - This sequence is similar to Sequence 2 except that the break flows are higher. Failure of the operator to depressurize, combined with the loss of SG integrity, eventually leads to depletion of the RWST through the unisolated SG.

Sequence 9 - This sequence represents a safe state because retention of SG integrity permits preservation of coolant inventory and continued recirculation from the sump. The high pressure recirculation is required because of the stuck open relief valve earlier in the sequence accompanied by operator failure to depressurize.

Sequences 10 and 11 - These sequences represent failure of recirculation due to faults in the high pressure and low pressure recirculation systems.

Sequence 12 - This sequence involves a simultaneous loss of RCS integrity and SG integrity. Continued safety injection is required to maintain the RCS inventory, but the loss of SG integrity causes diversion of the inventory outside of containment. The previous failure to depressurize means the RCS remains at high pressure with the attendant large discharge rates. Recirculation is not considered because the sump inventory would be insufficient to maintain it.

Sequence 13 - This sequence is an SGTR with loss of auxiliary feedwater. The response to loss of AFW in other transients is to initiate feed and bleed cooling. But, feed and bleed cooling requires sustained pressure in the RCS, which is counter to the requirements for mitigation of SGTR. Due to limited prior evaluation of such circumstances, SGTR with loss of all feedwater was considered a core damage sequence.

Sequence 14 - This sequence represents a recoverable loss of safety injection. Safety injection fails early in response to the loss of pressurizer pressure. Restoration of RCS integrity is possible by rapid cooldown and depressurization of the primary. When the RCS and SG pressures are equal no further coolant makeup is required. If these actions are accomplished in a time frame such that core recovery is maintained and the RCS inventory is adequate to support heat removal through the SG, the system is maintained in an acceptable state.

Sequence 15 - This sequence leads to core uncovery through combined loss of SG integrity and failure of safety injection. Coolant is lost through the failed SG with no capability to makeup inventory.

Sequence 16 - This sequence is similar to Sequence 15 except that RCS inventory is lost through the pressurizer PORV.

Sequence 17 - This sequence represents failure to depressurize the RCS to limit leakage. Continued break flow through the ruptured tube leads to core uncovery.

Sequence 18 - This sequence is similar to Sequence 13 except that the feed and bleed option can not even be considered due to the failure of safety injection prior to failure of AFW. This sequence leads to core uncovery.

Sequence 19 - This sequence is an ATWS sequence as discussed above. ATWS was not considered mitigatible when combined with a tube rupture.

1.3.4 Quantification of SGTR Event Tree

The analysis of the systems required for response to SGTR proceeds as described in Sections 5 through 10 of this report. Several specific issues had to be addressed in analyzing the SGTR events. For the '4550' studies the SGTR frequency is based upon five reported SGTR events in some 500 reactor years of operation, all of which are assumed to be single tube events. This results in a SGTR initiating event frequency of 0.01/yr. Another issue of importance to the SGTR analysis is the maintenance of SG integrity. The probability of a SG safety relief valve (SRV) being demanded during SGTR with operator depressurization was estimated to be 0.3. If the operator failed to depressurize the RCS and the SG PORV is not blocked, the demand probability was assumed to be 0.15. If the operator failed to depressurize the RCS and the SG PORV is blocked, then it was estimated (conservatively) that the demand probability for the SG SRV is 1.00. If RCS depressurization has not occurred, it is assumed that and SRV remains open with a probability of 1.0. When these estimates are combined with the system availabilities, core damage frequencies on the order of 1 to 2 E-6 per reactor year result for Surry[13] and Sequoyah.[14] This represents approximately 3 to 4 percent of the mean core damage frequency reported for these plants.

1.4 Treatment of Relief Valve Block Valves

There is a history of unacceptable leakage in pressurizer PORVs and steam generator atmospheric dump valves (ADV) during PWR operations. These valves are normally installed with motor operated valves (MOV) located between the relief or dump valve and the high pressure system. This arrangement permits "blocking" of the relief/dump valves so that maintenance or repair can be performed while the system remains at pressure. In order to counteract the unacceptable leakage of the PORVs and ADVs, it has become relatively common practice to operate with the block valves closed at least for some periods of time. This situation has obvious implications for risk assessment because closed block valves effectively inhibit the automatic action of the PORVs and ADVs in response to off-normal conditions.

In order to incorporate the block valves into the systems analysis the analysts considered a number of questions:

First, what are the issues as a function of whether or not the valves were open or closed.

Second, if block valves may be open or closed, what is the fraction of time they are in either position.

If the valves were open, then the points of concern included: 1) if maintenance or surveillance was performed, were the valves returned to the proper configuration, i.e., a human reliability issue, and 2) what is the likelihood that a normally open MOV fails closed under accident conditions. If the valves were closed, then the concerns included: 1) what are the error probabilities related to the operator recognizing that depressurization is required and taking the appropriate steps to open the valves, and 2) what is the likelihood that the valve will fail to open if and when demanded.

The concerns outlined above were addressed using the techniques described in the main body of this report and the supporting references. The difficulty arose in establishing the fraction of time the block valves are open or closed. In this analysis plant operating and maintenance logs were consulted and discussions were held with the operators. It was not always possible to establish unequivocally the valve position history. Therefore, point estimates of the fractions of the time the valve was open or closed were generated and used in the analysis.

Another issue which surfaced during the ASEP analyses relates to the design of the power supplies to the block valves and the power operated relief valves (PORV or ADV). There have been instances in which electric power to the PORV was supplied from one train while power to the block valve was supplied from another. Therefore, a situation is created in which loss or failure of either power train disables the relief function.

A related concern, which did not appear explicitly in the ASEP analyses, but which has been reported, relates to the status of the block valve after it is closed. In some instances, when the PORV has been declared inoperable because of Tech Spec requirements not being met, the block valve was closed and power removed from the valve motor control center (MCC). The difficulty created is that if the PORV is demanded with block valve closed and power removed, the operator cannot open the valve from the control room. An operator would have to go to the power bus and restore power to the MCC before the valve could be operated. This could induce an unacceptable delay in recovery activities. The potential for such a condition should be considered in any analysis.

1.5 Quantification of Relief Valve Demand

A key question which arises during PRAs is the quantification of the probability that one or more relief valves, if demanded, will open and then fail to close, thus putting the system into some type of LOCA. This probability is the product of the probability of failure to close per demand and the number of demands or cycles. The first term, probability of failure to close per demand, has been pursued in various studies and a value of 0.03/demand was selected as the original ASEP generic value, a value that falls into the range suggested by Licensee Event Reports. The second term, number of cycles or demands, is much more difficult to establish. Reports from the PWR vendors[15,16,17] indicate that that primary system SRVs have never been demanded in a transient (i.e., a demand probability <1E-8). This is attributed to the fact that in those plants which have both PORVs and SRVs the set point of the latter is higher, leading to a much lower likelihood of the valve being challenged. The probability of a PORV being challenged has variously been reported in the range 0.01 to 1.0, depending upon the initiating event. Unfortunately, this does not address the question of how many times the valves may be challenged in a given scenario. A number of analyses exist which predict pressure levels and durations for a variety of conditions, but these can be very plant and event specific and have limited applicability. Therefore, a substantial effort was devoted toward establishing these values in the ASEP analyses. Several examples are provided below to indicate the type of approach used in this effort.

1.5.1 RCS PORV Failure to Reclose Event

At Surry, during an S3 LOCA the high pressure injection capacity exceeds the LOCA leak rate. Therefore, the PORV will be demanded if the operator fails to control the injection flow, with a conditional probability of 1.0. In this situation, the probability of failure to reclose then depends upon the following:

Probability operator fails to control injection = 0.1
Probability PORV is not blocked = 0.9
Probability PORV fails to reclose = 0.03
Probability Operator fails to close block valve = 2.7E-3
Probability block valve fails to close = 0.04

or

$$P_{frc} = 0.1 * 0.9 * 0.03 * (2.7E-3 + 0.04) = 1.2E-4$$

In this example, the failure of the operator to shut the block valve was assumed to be a skill-based error.

1.5.2 Relief Demand Rate During Station Blackout

During a station blackout event at Surry, the SG ADVs would be unavailable because they are not loaded on the emergency bus. Therefore, the probability of a pressurizer PORV demand was assessed as 1.0. Thus, it was necessary to calculate a per valve demand basis. The probability of having at least one PORV unblocked is:

$$P_{1ub} = 1 - P_{1b*}P_{2b} = 1 - (0.3)*(0.3) = 0.91$$

The probability of a PORV being blocked was assessed as 0.3 based on plant experience from 1982-1987.

Based upon available information, the probability that a SG PORV would be demanded during station blackout was estimated to be one SG PORV every 20 minutes on each steam generator for a duration of one hour. Thus, there would be 9 demands for SG PORV. The probability of a SG PORV being demanded and failing to reclose is, as noted for the pressurizer PORVs above, the product of the number of demands and the probability for failure to reclose. In this instance, 9 demands * 0.03 or 0.271.

1.5.3 Relief Demand Rate During SGTR

The probability of a SG safety relief valve (SRV) being demanded during SGTR with operator depressurization was estimated to be 0.3 based upon the elicitation of expert judgment. If the operator failed to depressurize the RCS and the SG PORV is <u>not</u> blocked, the demand probability was assumed to be 0.15. On the other hand, if the operator failed to depressurize the RCS and the SG PORV <u>is</u> blocked, then it was estimated (conservatively) that the demand probability for the SG SRV is 1.00. If RCS depressurization has not occurred, it is assumed that an SRV remains open with a probability of 1.0.

The point of these examples is not to provide an exhaustive set of solutions, but to alert the reader to at least some of the potential 'special issues' that may arise in the course of a PRA.

REFERENCES

1. Harrington, R. M., and S. A. Hodge, ATWS at Browns Ferry Unit One -- Accident Sequence Analysis, NUREG/CR-3470, ORNL TM-8902, Oak Ridge National Laboratory, Oak Ridge, TN, July 1984.

2. Dallman, R. J., et al., Severe Accident Sequence Analysis Program -- Anticipated Transient Without Scram Simulations for Browns Ferry Nuclear Power Plant Unit 1, Draft, NUREG/CR-4165, EG&G-2379, Idaho National Engineering Laboratory (EG&G Idaho), Idaho Falls, ID, February 1985.

3. Assessment of BWR Mitigation of ATWS, NUREG-0460, Alternate No. 3, NEDO-24222, 80NED021, Class I, General Electric, February 1981.

4. Harrington, R. M. and L. J. Fuller, BWR-LTAS: A Boiling Water Reactor Long-Term Accident Simulation Code, NUREG/CR-3764, ORNL/TM-9163, Oak Ridge National Laboratory, Oak Ridge, TN, February 1985.

5. Kolaczkowski, A. M., et al., Analysis of Core Damage Frequency from Internal Events: Peach Bottom, Unit 2, NUREG/CR-4550, Vol.4, Rev 1, SAND86-2084, Sandia National Laboratories, Albuquerque, NM, August 1989.

6. Drouin, M. T., Analysis of Core Damage Frequency from Internal Events: Grand Gulf, Unit 1, NUREG/CR-4550, Vol. 6, Rev 1, SAND86-2084, Sandia National Laboratory, Albuquerque, NM, September 1989.

7. Swain, A. D., Accident Sequence Evaluation Program Human Reliability Analysis Procedure, NUREG/CR-4772, SAND86-1996, Sandia National Laboratories, Albuquerque, NM, February 1987.

8. Swain, A. D., and H. E. Guttman, Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications, NUREG/CR-1278, SAND80-0200, Sandia National Laboratories, Albuquerque, NM, August 1983.

9. Luckas, Jr., W. J., et al., A Human Reliability Analysis for the ATWS Accident Sequence with MSIV Closure at the Peach Bottom Atomic Power Station, A-3272, Brookhaven National Laboratory, Upton, NY, May 1986.

10. Worrell, R. B., and D. W. Stack, A SETS User's Manual for the Fault Tree Analyst, SAND77-2051, Sandia National Laboratories, Albuquerque, NM, 1978.

11. Iman, R. L., and M. J. Shortencarier, A User's Guide for the Top Event Matrix Analysis Code (TEMAC), NUREG/CR-4598, SAND86-0960, Sandia National Laboratories, Albuquerque, NM, August 1986.

12. Wheeler, T. A., et al., Analysis of Core Damage Frequency: Expert Judgment Elicitation on Internal Event Issues; Part 1 - Expert Panel and Part 2 - Project Staff, NUREG/CR-4550, Volume 2, Rev. 1, SAND86-2084, Sandia National Laboratories, Albuquerque, NM, April 1989.

13. Bertucio, R. C., et al., Analysis of Core Damage Frequency from Internal Events: Surry, Unit 1, NUREG/CR-4550, Volume 3, Rev. 1, SAND86-2084, Sandia National Laboratories, Albuquerque, NM, (draft copy available in NRC public documents room).

14. Bertucio, R. C., et al., Analysis of Core Damage Frequency from Internal Events: Sequoyah, Unit 1, NUREG/CR-4550, Volume 5, Rev. 1, SAND86-2084, Sandia National Laboratories, Albuquerque, NM, (draft copy available in NRC public documents room).

15. Probabilistic Analysis and Operational Data in Response to NUREG-0737, Item II.K.3.2 for Westinghouse NSS Plants, WCAP-9804, Westinghouse Electric Company, Pittsburgh, PA, February 1981.

16. Report on Power-Operated Relief Valve Opening Probability and Justification for Present System and Setpoints, #12-1122779, Babcock and Wilcox, Lynchburg, VA, 1981.

17. PORV Failure Reduction Methods -- Final Report, CEN-145, CE Power Systems, Windsor, CT, December 1980.

NRC FORM 335
(2-89)
NRCM 1102,
3201, 3202

U.S. NUCLEAR REGULATORY COMMISSION

BIBLIOGRAPHIC DATA SHEET

(See instructions on the reverse)

1. REPORT NUMBER
(Assigned by NRC. Add Vol., Supp., Rev., and Addendum Numbers, if any.)
NUREG/CR-4550
SAND86-2084
Vol. 1, Rev. 1

2. TITLE AND SUBTITLE
Analysis of Core Damage Frequency: Internal Events Methodology

3. DATE REPORT PUBLISHED
MONTH January YEAR 1990

4. FIN OR GRANT NUMBER
A1228

5. AUTHOR(S)
D.M. Ericson, Jr., Editor*, T.A. Wheeler, T.T. Sype,
M.T. Drouin**, W.R. Cramond, A.L. Camp, K.J. Maloney,
F.T. Harper

6. TYPE OF REPORT

7. PERIOD COVERED *(Inclusive Dates)*

8. PERFORMING ORGANIZATION – NAME AND ADDRESS *(If NRC, provide Division, Office or Region, U.S. Nuclear Regulatory Commission, and mailing address; if contractor, provide name and mailing address.)*

Sandia National Laboratories
Albuquerque, NM 87185

*ERC Environmental and Energy Services Company
**Science Applications International Corporation

9. SPONSORING ORGANIZATION – NAME AND ADDRESS *(If NRC, type "Same as above"; if contractor, provide NRC Division, Office or Region, U.S. Nuclear Regulatory Commission, and mailing address.)*

Division of Systems Research
Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission
Washington, DC 20555

10. SUPPLEMENTARY NOTES

11. ABSTRACT *(200 words or less)*

NUREG-1150 examines the risk to the public from a selected group of nuclear power plants. This report describes the methodology that evolved as the internal event core damage frequencies for four plants were generated in support of NUREG-1150. The objective is to perform an analysis that closely approximates a state-of-the-art Level 1 Probabilistic Risk Assessment (PRA). Therefore, in principle, it is similar to those used in previous PRAs. However, this methodology, based upon previous studies and using analysts experienced in these techniques, allows the analysis to be focused upon selected areas. With this approach only the most important systems and failure modes are emphasized and modeled in detail, and the data and human reliability analyses are simplified. An analysis employing this methodology (exclusive of external reviews) can be completed in nine to twelve months using two or three full-time experienced systems analysts and part-time personnel in other areas, such as data analysis and human reliability analysis. This is significantly faster and less expensive than previous analyses, but even so, most of the insights that are obtained by the more expensive studies are still provided.

12. KEY WORDS/DESCRIPTORS *(List words or phrases that will assist researchers in locating the report.)*

Probabilistic Risk Assessment (PRA)
safety analysis
core damage
uncertainty
internal events methodology

13. AVAILABILITY STATEMENT
unlimited

14. SECURITY CLASSIFICATION
(This Page)
unclassified
(This Report)
unclassified

15. NUMBER OF PAGES

16. PRICE

DISTRIBUTION:

Frank Abbey
U. K. Atomic Energy Authority
Wigshaw Lane, Culcheth
Warrington, Cheshire, WA3 4NE
ENGLAND

Kiyoharu Abe
Department of Reactor Safety
Research
Nuclear Safety Research Center
ToKai Research Establishment
JAERI
Tokai-mura, Naga-gun
Ibaraki-ken,
JAPAN

Ulvi Adalioglu
Nuclear Engineering Division
Cekmece Nuclear Research and
Training Centre
P.K.1, Havaalani
Istanbul
TURKEY

Bharat Agrawal
USNRC-RES/AEB
MS: NL/N-344

Kiyoto Aizawa
Safety Research Group
Reactor Research and Development
Project
PNC
9-13m 1-Chome Akasaka
Minatu-Ku
Tokyo
JAPAN

Oguz Akalin
Ontario Hydro
700 University Avenue
Toronto, Ontario
CANADA M5G 1X6

David Aldrich
Science Applications International
Corporation
1710 Goodridge Drive
McLean, VA 22102

Agustin Alonso
University Politecnica De Madrid
J Gutierrez Abascal, 2
28006 Madrid
SPAIN

Christopher Amos
Science Applications International
Corporation
2109 Air Park Road SE
Albuquerque, NM 87106

Richard C. Anoba
Project Engr., Corp. Nuclear Safety
Carolina Power and Light Co.
P. O. Box 1551
Raleigh, NC 27602

George Apostolakis
UCLA
Boelter Hall, Room 5532
Los Angeles, CA 90024

James W. Ashkar
Boston Edison Company
800 Boylston Street
Boston, MA 02199

Donald H. Ashton
Bechtel Power Corporation
15740 Shady Grove Road
Gaithersburg, MD 20877

J. de Assuncao
Cabinete de Proteccao e Seguranca
Nuclear
Secretario de Estado de Energia
Ministerio da Industria
av. da Republica, 45-6°
1000 Lisbon
PORTUGAL

Mark Averett
Florida Power Corporation
P.O. Box 14042
St. Petersburg, FL 33733

Raymond O. Bagley
Northeast Utilities
P.O. Box 270
Hartford, CT 06141-0270

Juan Bagues
Consejo de Seguridad Nucleare
Sarangela de la Cruz 3
28020 Madrid
SPAIN

George F. Bailey
Washington Public Power Supply
System
P. O. Box 968
Richland, WA 99352

H. Bairiot
Belgonucleaire S A
Rue de Champ de Mars 25
B-1050 Brussels
BELGIUM

Louis Baker
Reactor Analysis and Safety
Division
Building 207
Argonne National Laboratory
9700 South Cass Avenue
Argonne, IL 60439

H-P. Balfanz
TUV-Norddeutschland
Grosse Bahnstrasse 31,
2000 Hamburg 54
FEDERAL REPUBLIC OF GERMANY

Patrick Baranowsky
USNRC-NRR/OEAB
MS: 11E-22

H. Bargmann
Dept. de Mecanique
Inst. de Machines Hydrauliques
et de Mecaniques des Fluides
Ecole Polytechnique de Lausanne
CH-1003 Lausanne
M.E. (ECUBLENS)
CH. 1015 Lausanne
SWITZERLAND

Robert A. Bari
Brookhaven National Laboratory
Building 130
Upton, NY 11973

Richard Barrett
USNRC-NRR/[illegible]RAB
MS: 10A[illegible]

Kenneth S. Baskin
S. California Edison Company
P.O. Box 800
Rosemead, CA 91770

J. Basselier
Belgonucleaire S A
Rue du Champ de Mars 25, B-1050
Brussels
BELGIUM

Werner Bastl
Gesellschaft Fur Reaktorsicherheit
Forschungsgelande
D-8046 Garching
FEDERAL REPUBLIC OF GERMANY

Anton Bayer
BGA/ISH/ZDB
Postfach 1108
D-8042 Neuherberg
FEDERAL REPUBLIC OF GERMANY

Ronald Bayer
Virginia Electric Power Co.
P. O. Box 26666
Richmond, VA 23261

Eric S. Beckjord
Director
USNRC-RES
MS: NL/S-007

Bruce B. Beckley
Public Service Company
P.O. Box 330
Manchester, NH 03105

William Beckner
USNRC-RES/SAIB
MS: NL/S-324

Robert M. Bernero
Director
USNRC-NMSS
MS: 6A-4

Ronald Berryman [2]
Virginia Electric Power Co.
P. O. Box 26666
Richmond, VA 23261

Robert C. Bertucio
NUS Corporation
1301 S. Central Ave, Suite 202
Kent, WA 98032

John H. Bickel
EG&G Idaho
P.O. Box 1625
Idaho Falls, ID 83415

Peter Bieniarz
Risk Management Association
2309 Dietz Farm Road, NW
Albuquerque, NM 87107

Adolf Birkhofer
Gesellschaft Fur Reaktorsicherheit
Forschungsgelande
D-8046 Garching
FEDERAL REPUBLIC OF GERMANY

James Blackburn
Illinois Dept. of Nuclear Safety
1035 Outer Park Drive
Springfield, IL 62704

Dennis C. Bley
Pickard, Lowe & Garrick, Inc.
2260 University Drive
Newport Beach, CA 92660

Roger M. Blond
Science Applications Int. Corp.
20030 Century Blvd., Suite 201
Germantown, MD 20874

Simon Board
Central Electricity Generating Board
Technology and Planning Research Division
Berkeley Nuclear Laboratory
Berkeley Gloucestershire, GL139PB
UNITED KINGDOM

Mario V. Bonace
Northeast Utilities Service Company
P.O. Box 270
Hartford, CT 06101

Gary J. Boyd
Safety and Reliability Optimization Services
9724 Kingston Pike, Suite 102
Knoxville, TN 37922

Robert J. Breen
Electric Power Research Institute
3412 Hillview Avenue
Palo Alto, CA 94303

Charles Brinkman
Combustion Engineering
7910 Woodmont Avenue
Bethesda, MD 20814

K. J. Brinkmann
Netherlands Energy Res. Fdtn.
P.O. Box 1
1755ZG Petten NH
NETHERLANDS

Allan R. Brown
Manager, Nuclear Systems and Safety Department
Ontario Hydro
700 University Ave.
Toronto, Ontario M5G1X6
CANADA

Robert G. Brown
TENERA L.P.
1340 Saratoga-Sunnyvale Rd.
Suite 206
San Jose, CA 95129

Sharon Brown
EI Services
1851 So. Central Place, Suite 201
Kent, WA 98031

R. H. Buchholz
Nutech
6835 Via Del Oro
San Jose, CA 95119

Ben Buchbinder
NASA, Code QS
600 Maryland Ave. SW
Washington, DC 20546

Robert J. Budnitz
Future Resources Associates
734 Alameda
Berkeley, CA 94707

Gary R. Burdick
USNRC-RES/DSR
MS: NL/S-007

M. Bustraan
Netherlands Energy Res. Fdtn.
P.O. Box 1
1755ZG Petten NH
NETHERLANDS

Nigel E. Buttery
Central Electricity Generating
Board
Booths Hall
Chelford Road, Knutsford
Cheshire, WA168QG
UNITED KINGDOM

Jose I. Calvo Molins
Probabilistic Safety Analysis
Group
Consejo de Seguridad Nuclear
Sor Angela de la Cruz 3, Pl. 6
28020 Madrid
SPAIN

J. F. Campbell
Nuclear Installations Inspectorate
St. Peters House
Balliol Road, Bootle
Merseyside, L20 3LZ
UNITED KINGDOM

Kenneth S. Canady
Duke Power Company
422 S. Church Street
Charlotte, NC 28217

Lennart Carlsson
IAEA A-1400
Wagramerstrasse 5
P.O. Box 100
Vienna, 22
AUSTRIA

Annick Carnino
Electricite de France
32 Rue de Monceau 8EME
Paris, F5008
FRANCE

G. Caropreso
Dept. for Envir. Protect. & Hlth.
ENEA Cre Casaccia
Via Anguillarese, 301
00100 Roma
ITALY

James C. Carter, III
TENERA L.P.
Advantage Place
308 North Peters Road
Suite 280
Knoxville, TN 37922

Eric Cazzoli
Brookhaven National Laboratory
Building 130
Upton, NY 11973

John G. Cesare
SERI
Director Nuclear Licensing
5360 I-55 North
Jackson, MS 39211

S. Chakraborty
Radiation Protection Section
Div. De La Securite Des Inst. Nuc.
5303 Wurenlingen
SWITZERLAND

Sen-I Chang
Institute of Nuclear Energy
Research
P.O. Box 3
Lungtan, 325
TAIWAN

J. R. Chapman
Yankee Atomic Electric Company
1671 Worcester Road
Framingham, MA 01701

Robert F. Christie
Tennessee Valley Authority
400 W. Summit Hill Avenue, W10D190
Knoxville, TN 37902

T. Cianciolo
BWR Assistant Director
ENEA DISP TX612167 ENEUR
Rome
ITALY

Thomas Cochran
Natural Resources Defense Council
1350 New York Ave. NW, Suite 300
Washington, D.C. 20005

Frank Coffman
USNRC-RES/HFB
MS: NL/N-316

Larry Conradi
NUS Corporation
16835 W. Bernardo Drive
Suite 202
San Diego, CA 92127

Peter Cooper
U.K. Atomic Energy Authority
Wigshaw Lane, Culcheth
Warrington, Cheshire, WA3 4NE
UNITED KINGDOM

C. Allin Cornell
110 Coquito Way
Portola Valley, CA 94025

Michael Corradini
University of Wisconsin
1500 Johnson Drive
Madison, WI 53706

E. R. Corran
Nuclear Technology Division
ANSTO Research Establishment
Lucas Heights Research Laboratories
Private Mail Bag 7
Menai, NSW 2234
AUSTRALIA

James Costello
USNRC-RES/SSEB
MS: NL/S-217A

George R. Crane
1570 E. Hobble Creek Dr.
Springville, UT 84663

Mat Crawford
SERI
5360 I-55 North
Jackson, MS 39211

Michael C. Cullingford
Nuclear Safety Division
IAEA
Wagramerstrasse, 5
P.O. Box 100
A-1400 Vienna
AUSTRIA

Garth Cummings
Lawrence Livermore Laboratory
L-91, Box 808
Livermore, CA 94526

Mark A. Cunningham
USNRC-RES/PRAB
MS: NL/S-372

James J. Curry
7135 Salem Park Circle
Mechanicsburg, PA 17055

Peter Cybulskis
Battelle Columbus Division
505 King Avenue
Columbus, OH 43201

Peter R. Davis
PRD Consulting
1935 Sabin Drive
Idaho Falls, ID 83401

Jose E. DeCarlos
Consejo de Seguridad Nuclear
Sor Angela de la Cruz 3, Pl. 8
28016 Madrid
SPAIN

M. Marc Decreton
Department Technologie
CEN/SCK
Boeretang 200
B-2400 Mol
BELGIUM

Richard S. Denning
Battelle Columbus Division
505 King Avenue
Columbus, OH 43201

Vernon Denny
Science Applications Int. Corp.
5150 El Camino Real, Suite 3
Los Altos, CA 94303

J. Devooget
Faculte des Sciences Appliques
Universite Libre de Bruxelles
av. Franklin Roosevelt
B-1050 Bruxelles
BELGIUM

R. A. Diederich
Supervising Engineer
Environmental Branch
Philadelphia Electric Co.
2301 Market St.
Philadelphia, PA 19101

Raymond DiSalvo
Battelle Columbus Division
505 King Avenue
Columbus, OH 43201

Mary T. Drouin
Science Applications International
Corporation
2109 Air Park Road S.E.
Albuquerque, NM 87106

Andrzej Drozd
Stone and Webster
Engineering Corp.
243 Summer Street
Boston, MA 02107

N. W. Edwards
NUTECH
145 Martinville Lane
San Jose, CA 95119

Ward Edwards
Social Sciences Research Institute
University of Southern California
Los Angeles, CA 90089-1111

Joachim Ehrhardt
Kernforschungszentrum Karlsruhe/INR
Postfach 3640
D-7500 Karlsruhe 1
FEDERAL REPUBLIC OF GERMANY

Adel A. El-Bassioni
USNRC-NRR/PRAB
MS: 10A-2

J. Mark Elliott
International Energy Associates,
Ltd., Suite 600
600 New Hampshire Ave., NW
Washington, DC 20037

Farouk Eltawila
USNRC-RES/AEB
MS: NL/N-344

Mike Epstein
Fauske and Associates
P. O. Box 1625
16W070 West 83rd Street
Burr Ridge, IL 60521

Malcolm L. Ernst
USNRC-RGN II

F. R. Farmer
The Long Wood, Lyons Lane
Appleton, Warrington
WA4 5ND
UNITED KINGDOM

P. Fehrenback
Atomic Energy of Canada, Ltd.
Chalk River Nuclear Laboratories
Chalk River Ontario, K0J1P0
CANADA

P. Ficara
ENEA Cre Casaccia
Department for Thermal Reactors
Via Anguillarese, 301
00100 ROMA
ITALY

A. Fiege
Kernforschungszentrum
Postfach 3640
D-7500 Karlsruhe
FEDERAL REPUBLIC OF GERMANY

John Flack
USNRC-RES/SAIB
MS: NLS-324

George F. Flanagan
Oak Ridge National Laboratory
P.O. Box Y
Oak Ridge, TN 37831

Karl N. Fleming
Pickard, Lowe & Garrick, Inc.
2260 University Drive
Newport Beach, CA 92660

Terry Foppe
Rocky Flats Plant
P. O. Box 464, Building T886A
Golden, CO 80402-0464

Joseph R. Fragola
Science Applications International
Corporation
274 Madison Avenue
New York, NY 10016

Wiktor Frid
Swedish Nuclear Power Inspectorate
Division of Reactor Technology
P. O. Box 27106
S-102 52 Stockholm
SWEDEN

James Fulford
NUS Corporation
910 Clopper Road
Gaithersburg, MD 20878

Urho Fulkkinen
Technical Research Centre of
Finland
Electrical Engineering Laboratory
Otakaari 7 B
SF-02150 Espoo 15
FINLAND

J. B. Fussell
JBF Associates, Inc.
1630 Downtown West Boulevard
Knoxville, TN 37919

John Garrick
Pickard, Lowe & Garrick, Inc.
2260 University Drive
Newport Beach, CA 92660

John Gaunt
British Embassy
3100 Massachusetts Avenue, NW
Washington, DC 20008

Jim Gieseke
Battelle Columbus Division
505 King Avenue
Columbus, OH 43201

Frank P. Gillespie
USNRC-NRR/PMAS
MS: 12G-18

Ted Ginsburg
Department of Nuclear Energy
Building 820
Brookhaven National Laboratory
Upton, NY 11973

James C. Glynn
USNRC-RES/PRAB
MS: NL/S-372

P. Govaerts
Departement de la Surete Nucleaire
Association Vincotte
avenue du Roi 157
B-1060 Bruxelles
BELGIUM

George Greene
Building 820M
Brookhaven National Laboratory
Upton, NY 11973

Carrie Grimshaw
Brookhaven National Laboratory
Building 130
Upton, NY 11973

H. J. Van Grol
Energy Technology Division
Energieonderzoek Centrum Nederland
Westerduinweg 3
Postbus 1
NL-1755 Petten ZG
NETHERLANDS

Sergio Guarro
Lawrence Livermore Laboratories
P. O. Box 808
Livermore, CA 94550

Sigfried Hagen
Kernforschungzentrum Karlsruhe
P. O. Box 3640
D-7500 Karlsruhe 1
FEDERAL REPUBLIC OF GERMANY

L. Hammar
Statens Karnkraftinspektion
P.O. Box 27106
S-10252 Stockholm
SWEDEN

Stephen Hanauer
Technical Analysis Corp.
6723 Whittier Avenue
Suite 202
McLean, VA 22101

Brad Hardin
USNRC-RES/TRAB
MS: NL/S-169

R. J. Hardwich, Jr.
Virginia Electric Power Co.
P.O. Box 26666
Richmond, Va 23261

Michael R. Haynes
UKAEA Harwell Laboratory
Oxfordshire
Didcot, Oxon., OX11 ORA
ENGLAND

Michael J. Hazzan
Stone & Webster
3 Executive Campus
Cherry Hill, NJ 08034

A. Hedgran
Royal Institute of Technology
Nuclear Safety Department
Bunellvagen 60
10044 Stockholm
SWEDEN

Sharif Heger
UNM Chemical and Nuclear
Engineering Department
Farris Engineering
Room 209
Albuquerque, NM 87131

Jon C. Helton
Dept. of Mathematics
Arizona State University
Tempe, AZ 85287

Robert E. Henry
Fauske and Associates, Inc.
16W070 West 83rd Street
Burr Ridge, IL 60521

P. M. Herttrich
Federal Ministry for the
Environment, Preservation of
Nature and Reactor Safety
Husarenstrasse 30
Postfach 120629
D-5300 Bonn 1
FEDERAL REPUBLIC OF GERMANY

F. Heuser
Giesellschaft Fur Reaktorsicherheit
Forschurgsgelande
D-8046 Garching
FEDERAL REPUBLIC OF GERMANY

E. F. Hicken
Giesellschaft Fur Reaktorsicherheit
Forschungsgelande
D-8046 Garching
FEDERAL REPUBLIC OF GERMANY

D. J. Higson
Radiological Support Group
Nuclear Safety Bureau
Australian Nuclear Science and
Technology Organisation
P.O. Box 153
Rosebery, NSW 2018
AUSTRALIA

Daniel Hirsch
University of California
A. Stevenson Program on
Nuclear Policy
Santa Cruz, CA 95064

H. Hirschmann
Hauptabteilung Sicherheit und
Umwelt
Swiss Federal Institute for
Reactor Research (EIR)
CH-5303 Wurenlingen
SWITZERLAND

Mike Hitchler
Westinghouse Electric Corp.
Savanna River Site
Aiken, SC 29808

Richard Hobbins
EG&G Idaho
P. O. Box 1625
Idaho Falls, ID 83415

Steven Hodge
Oak Ridge National Laboratory
P.O. Box Y
Oak Ridge, TN 37831

Lars Hoegberg
Office of Regulation and Research
Swedish Nuclear Power Inspectorate
P. O. Box 27106
S-102 52 Stockholm
SWEDEN

Lars Hoeghort
IAEA A-1400
Wagranerstraase 5
P.O. Box 100
Vienna, 22
AUSTRIA

Edward Hofer
Giesellschaft Fur Reaktorsicherheit
Forschurgsgelande
D-8046 Garching
FEDERAL REPUBLIC OF GERMANY

Peter Hoffmann
Kernforschingszentrum Karlsruhe
Institute for Material
Und Festkorperforsching I
Postfach 3640
D-7500 Karlsruhe 1
FEDERAL REPUBLIC OF GERMANY

N. J. Holloway
UKAEA Safety and Reliability
Directorate
Wigshaw Lane, Culcheth
Warrington, Cheshire, WA34NE
UNITED KINGDOM

Stephen C. Hora
University of Hawaii at Hilo
Division of Business Administration
and Economics
College of Arts and Sciences
Hilo, HI 96720-4091

J. Peter Hoseman
Swiss Federal Institute for
Reactor Research
CH-5303, Wurenlingen
SWITZERLAND

Thomas C. Houghton
KMC, Inc.
1747 Pennsylvania Avenue, NW
Washington, DC 20006

Dean Houston
USNRC-ACRS
MS: P-315

Der Yu Hsia
Taiwan Atomic Energy Council
67, Lane 144, Keelung Rd.
Sec. 4
Taipei
TAIWAN

Alejandro Huerta-Bahena
National Commission on Nuclear
Safety and Safeguards (CNSNS)
Insurgentes Sur N. 1776
Col. Florida
C. P. 04230 Mexico, D.F.
MEXICO

Kenneth Hughey [2]
SERI
5360 I-55 North
Jackson, MS 39211

Won-Guk Hwang
Kzunghee University
Yongin-Kun
Kyunggi-Do 170-23
KOREA

Michio Ichikawa
Japan Atomic Energy Research
Institute
Dept. of Fuel Safety Research
Tokai-Mura, Naka-Gun
Ibaraki-Ken, 319-1
JAPAN

Sanford Israel
USNRC-AEOD/ROAB
MS: MNBB-9715

Krishna R. Iyengar
Louisiana Power and Light
200 A Huey P. Long Avenue
Gretna, LA 70053

R. E. Jaquith
Combustion Engineering, Inc.
1000 Prospect Hill Road
M/C 9490-2405
Windsor, CT 06095

S. E. Jensen
Exxon Nuclear Company
2101 Horn Rapids Road
Richland, WA 99352

Kjell Johannson
Studsvik Energiteknik AB
S-611 82, Nykoping
SWEDEN

Richard John
SSM, Room 102
927 W. 35th Place
USC, University Park
Los Angeles, CA 90089-0021

D. H. Johnson
Pickard, Lowe & Garrick, Inc.
2260 University Drive
Newport Beach, CA 92660

W. Reed Johnson
Department of Nuclear Engineering
University of Virginia
Reactor Facility
Charlottesville, VA 22901

Jeffery Julius
NUS Corporation
1301 S. Central Ave., Suite 202
Kent, WA 98032

H. R. Jun
Korea Adv. Energy Research Inst.
P.O. Box 7, Daeduk Danju
Chungnam 300-31
KOREA

Peter Kafka
Gesellschaft Fur Reaktorsicherheit
Forschungsgelande
D-8046 Garching
FEDERAL REPUBLIC OF GERMANY

Geoffrey D. Kaiser
Science Application Int. Corp.
1710 Goodridge Drive
McLean, VA 22102

William Kastenberg
UCLA
Boelter Hall, Room 5532
Los Angeles, CA 90024

Walter Kato
Brookhaven National Laboratory
Associated Universities, Inc.
Upton, NY 11973

M. S. Kazimi
MIT, 24-219
Cambridge, MA 02139

Ralph L. Keeney
101 Lombard Street
Suite 704W
San Francisco, CA 94111

Henry Kendall
Executive Director
Union of Concerned Scientists
Cambridge, MA

Frank King
Ontario Hydro
700 University Avenue
Bldg. H11 G5
Toronto
CANADA M5G1X6

Oliver D. Kingsley, Jr.
Tennessee Valley Authority
1101 Market Street
GN-38A Lookout Place
Chattanooga, TN 37402

Stephen R. Kinnersly
Winfrith Atomic Energy
Establishment
Reactor Systems Analysis Division
Winfrith, Dorchester
Dorset DT2 8DH
ENGLAND

Ryohel Kiyose
University of Tokyo
Dept. of Nuclear Engineering
7-3-1 Hongo Bunkyo
Tokyo 113
JAPAN

George Klopp
Commonwealth Edison Company
P.O. Box 767, Room 35W
Chicago, IL 60690

Klaus Koberlein
Gesellschaft Fur Reaktorsicherheit
Forschungsgelande
D-8046 Garching
FEDERAL REPUBLIC OF GERMANY

E. Kohn
Atomic Energy Canada Ltd.
Candu Operations
Mississauga
Ontario, L5K 1B2
CANADA

Alan M. Kolaczkowski
Science Applications International
Corporation
2109 Air Park Road, S.E.
Albuquerque, NM 87106

S. Kondo
Department of Nuclear Engineering
Facility of Engineering
University of Tokyo
3-1, Hongo 7, Bunkyo-ku
Tokyo
JAPAN

Herbert J. C. Kouts
Brookhaven National Laboratory
Building 179C
Upton, NY 11973

Thomas Kress
Oak Ridge National Laboratory
P.O. Box Y
Oak Ridge, TN 37831

W. Kroger
Institut fur Nukleare
Sicherheitsforschung
Kernforschungsanlage Julich GmbH
Postfach 1913
D-5170 Julich 1
FEDERAL REPUBLIC OF GERMANY

Greg Krueger [3]
Philadelphia Electric Co.
2301 Market St.
Philadelphia, PA 19101

Bernhard Kuczera
Kernforschungzentrum Karlsruhe
LWR Safety Project Group (PRS)
P. O. Box 3640
D-7500 Karlsruhe 1
FEDERAL REPUBLIC OF GERMANY

Jeffrey L. LaChance
Science Applications International
Corporation
2109 Air Park Road S.E.
Albuquerque, NM 87106

H. Larsen
Riso National Laboratory
Postbox 49
DK-4000 Roskilde
DENMARK

Wang L. Lau
Tennessee Valley Authority
400 West Summit Hill Avenue
Knoxville, TN 37902

Timothy J. Leahy
EI Services
1851 South Central Place, Suite 201
Kent, WA 98031

John C. Lee
University of Michigan
North Campus
Dept. of Nuclear Engineering
Ann Arbor, MI 48109

Tim Lee
USNRC-RES/RPSB
MS: NL/N-353

Mark T. Leonard
Science Applications International
Corporation
2109 Air Park Road, SE
Albuquerque, NM 87106

Leo LeSage
Director, Applied Physics Div.
Argonne National Laboratory
Building 208, 9700 South Cass Ave.
Argonne, IL 60439

Milton Levenson
Bechtel Western Power Company
50 Beale St.
San Francisco, CA 94119

Librarian
NUMARC/USCEA
1776 I Street NW, Suite 400
Washington, DC 80006

Eng Lin
Taiwan Power Company
242, Roosevelt Rd., Sec. 3
Taipei
TAIWAN

N. J. Liparulo
Westinghouse Electric Corp.
P. O. Box 355
Pittsburgh, PA 15230

Y. H. (Ben) Liu
Department of Mechanical
Engineering
University of Minnesota
Minneapolis, MN 55455

Bo Liwnang
IAEA A-1400
Swedish Nuclear Power Inspectorate
P.O. Box 27106
S-102 52 Stockholm
SWEDEN

J. P. Longworth
Central Electric Generating Board
Berkeley Gloucester
GL13 9PB
UNITED KINGDOM

Walter Lowenstein
Electric Power Research Institute
3412 Hillview Avenue
P. O. Box 10412
Palo Alto, CA 94303

William J. Luckas
Brookhaven National Laboratory
Building 130
Upton, NY 11973

Hans Ludewig
Brookhaven National Laboratory
Building 130
Upton, NY 11973

Robert J. Lutz, Jr.
Westinghouse Electric Corporation
Monroeville Energy Center
EC-E-371, P. O. Box 355
Pittsburgh, PA 15230-0355

Phillip E. MacDonald
EG&G Idaho, Inc.
P.O. Box 1625
Idaho Falls, ID 83415

Jim Mackenzie
World Resources Institute
1735 New York Ave. NW
Washington, DC 20006

David P. Mackowiak
Idaho Nat. Engineering Laboratory
P.O. Box 1625
Idaho Falls, ID 83415

A. P. Malinauskas
Oak Ridge National Laboratory
P.O. Box Y
Oak Ridge, TN 37831

Giuseppe Mancini
Commission European Comm.
CEC-JRC Eraton
Ispra Varese
ITALY

Lasse Mattila
Technical Research Centre of Finland
Lonnrotinkatu 37, P. O. Box 169
SF-00181 Helsinki 18
FINLAND

Roger J. Mattson
SCIENTECH Inc.
11821 Parklawn Dr.
Rockville, MD 20852

Donald McPherson
USNRC-NRR/DONRR
MS: 12G-18

Jim Metcalf
Stone and Webster Engineering Corporation
245 Summer St.
Boston, MA 02107

Mary Meyer
A-1, MS F600
Los Alamos National Laboratory
Los Alamos, NM 87545

Ralph Meyer
USNRC-RES/AEB
MS: NL/N-344

Charles Miller
8 Hastings Rd.
Momsey, NY 10952

Joseph Miller
Gulf States Utilities
P. O. Box 220
St. Francisville, LA 70775

William Mims
Tennessee Valley Authority
400 West Summit Hill Drive.
W10D199C-K
Knoxville, TN 37902

Jocelyn Mitchell
USNRC-RES/SAIB
MS: NL/S-324

Kam Mohktarian
CBI Na-Con Inc.
800 Jorie Blvd.
Oak Brook, IL 60521

James Moody
P.O. Box 641
Rye, NH 03870

S. Mori
Nuclear Safety Division
OECD Nuclear Energy Agency
38 Blvd. Suchet
75016 Paris
FRANCE

Walter B. Murfin
P.O. Box 550
Mesquite, NM 88048

Joseph A. Murphy
USNRC-RES/DSR
MS: NL/S-007

V. I. Nath
Safety Branch
Safety Engineering Group
Sheridan Park Research Community
Mississauga, Ontario L5K 1B2
CANADA

Susan J. Niemczyk
1545 18th St. NW, #112
Washington, DC 20036

P. K. Niyogi
USNRC-RES/PRAB
MS: NL/S-372

Paul North
EG&G Idaho, Inc.
P. O. Box 1625
Idaho Falls, ID 83415

Edward P. O'Donnell
Ebasco Services, Inc.
2 World Trade Center, 89th Floor
New York, NY 10048

David Okrent
UCLA
Boelter Hall, Room 5532
Los Angeles, CA 90024

Robert L. Olson
Tennessee Valley Authority
400 West Summit Hill Rd.
Knoxville, TN 37902

Simon Ostrach
Case Western Reserve University
418 Glenman Bldg.
Cleveland, OH 44106

D. Paddleford
Westinghouse Electric Corporation
Savanna River Site
Aiken, SC 29808

Robert L. Palla, Jr.
USNRC-NRR/PRAB
MS: 10A-2

Chang K. Park
Brookhaven National Laboratory
Building 130
Upton, NY 11973

Michael C. Parker
Illinois Department of Nuclear
Safety
1035 Outer Park Dr.
Springfield, IL 62704

Gareth Parry
NUS Corporation
910 Clopper Road
Gaithersburg, MD 20878

J. Pelce
Departement de Surete Nucleaire
IPSN
Centre d'Estudes Nucleaires du CEA
B.P. no. 6, Cedex
F-92260 Fontenay-aux-Roses
FRANCE

G. Petrangeli
ENEA Nuclear Energy ALT Disp
Via V. Brancati, 48
00144 Rome
ITALY

Marty Plys
Fauske and Associates
16W070 West 83rd St.
Burr Ridge, IL 60521

Mike Podowski
Department of Nuclear Engineering
and Engineering Physics
RPI
Troy, NY 12180-3590

Robert D. Pollard
Union of Concerned Scientists
1616 P Street, NW, Suite 310
Washington, DC 20036

R. Potter
UK Atomic Energy Authority
Winfrith, Dorchester
Dorset, DT2 8DH
UNITED KINGDOM

William T. Pratt
Brookhaven National Laboratory
Building 130
Upton, NY 11973

M. Preat
Chef du Service Surete Nucleaire et
Assurance Qualite
TRACTEBEL
Bd. du Regent 8
B-100 Bruxells
BELGIUM

David Pyatt
USDOE
MS: EH-332
Washington, DC 20545

William Raisin
NUMAEC
1726 M St. NW
Suite 904
Washington, DC 20036

Joe Rashid
ANATECH Research Corp.
3344 N. Torrey Pines Ct.
Suite 1320
La Jolla, CA 90237

Dale M. Rasmuson
USNRC-RES/PRAB
MS: NL/S-372

Ingvard Rasmussen
Riso National Laboratory
Postbox 49
DK-4000, Roskilde
DENMARK

Norman C. Rasmussen
Massachusetts Institute of
Technology
77 Massachusetts Avenue
Cambridge, MA 02139

John W. Reed
Jack R. Benjamin & Associates, Inc.
444 Castro St., Suite 501
Mountain View, CA 94041

David B. Rhodes
Atomic Energy of Canada, Ltd.
Chalk River Nuclear Laboratories
Chalk River, Ontario K0J1P0
CANADA

Dennis Richardon
Westinghouse Electric Corporation
P.O. Box 355
Pittsburgh, PA 15230

Doug Richeard
Virginia Electric Power Co.
P.O.Box 26666
Richmond, VA 23261

Robert Ritzman
Electric Power Research Institute
3412 Hillview Avenue
Palo Alto, CA 94304

Richard Robinson
USNRC-RES/PRAB
MS: NL/S-372

Jack E. Rosenthal
USNRC-AEOD/ROAB
MS: MNBB-9715

Denwood F. Ross
USNRC-RES
MS: NL/S-007

Frank Rowsome
9532 Fern Hollow Way
Gaithersburg, MD 20879

Wayne Russell
SERI
5360 I-55 North
Jackson, MS 39211

Jorma V. Sandberg
Finnish Ctr. Rad. Nucl. and Safety
Department of Nuclear Safety
P.O. Box 268
SF-00101 Helsinki
FINLAND

G. Saponaro
ENEA Nuclear Engineering Alt.
Zia V Brancati 4B
00144 ROME
ITALY

M. Sarran
United Engineers
P. O. Box 8223
30 S 17th Street
Philadelphia, PA 19101

Marty Sattison
EG&G Idaho
P. O. Box 1625
Idaho Falls, ID 83415

George D. Sauter
Electric Power Research Institute
3412 Hillview Avenue
Palo Alto, CA 94303

Jorge Schulz
Bechtel Western Power Corporation
50 Beale Street
San Francisco, CA 94119

B. R. Sehgal
Electric Power Research Institute
3412 Hillview Avenue
Palo Alto, CA 94303

Subir Sen
Bechtel Power Corp.
15740 Shady Grove Road
Location 1A-7
Gaithersburg, MD 20877

S. Serra
Ente Nazionale per l'Energia
Electtrica (ENEL)
via G. B. Martini 3
Rome
ITALY

Bonnie J. Shapiro
Science Applications International
Corporation
360 Bay Street
Suite 200
Augusta, GA 30901

H. Shapiro
Licensing and Risk Branch
Atomic Energy of Canada Ltd.
Sheridan Park Research Community
Mississauga, Ontario L5K 1B2
CANADA

Dave Sharp
Westinghouse Savannah River Co.
Building 773-41A, P. O. Box 616
Aiken, SC 29802

John Sherman
Tennessee Environmental Council
1719 West End Avenue, Suite 227
Nashville, TN 37203

Brian Sheron
USNRC-RES/DSR
MS: NL/N-007

Rick Sherry
JAYCOR
P. O. Box 85154
San Diego, CA 92138

Steven C. Sholly
MHB Technical Associates
1723 Hamilton Avenue, Suite K
San Jose, CA 95125

Louis M. Shotkin
USNRC-RES/RPSB
MS: NL/N-353

M. Siebertz
Chef de la Section Surete' des
Reacteurs
CEN/SCK
Boeretang, 200
B-2400 Mol
BELGIUM

Melvin Silberberg
USNRC-RES/DE/WNB
MS: NL/S-260

Gary Smith
SERI
5360 I-55 North
Jackson, MS 39211

Gary L. Smith
Westinghouse Electric Corporation
Hanford Site
Box 1970
Richland, WA 99352

Lanny N. Smith
Science Applications International
Corporation
2109 Air Park Road SE
Albuquerque, NM 87106

K. Soda
Japan Atomic Energy Res. Inst.
Tokai-Mura Naka-Gun
Ibaraki-Ken 319-11
JAPAN

Leonard Soffer
USNRC-RES/SAIB
MS: NL/S-324

David Sommers
Virginia Electric Power Company
P. O. Box 26666
Richmond, VA 23261

Herschel Spector
New York Power Authority
123 Main Street
White Plains, NY 10601

Themis P. Speis
USNRC-RES
MS: NL/S-007

Klaus B. Stadie
OECD-NEA, 38 Bld. Suchet
75016 Paris
FRANCE

John Stetkar
Pickard, Lowe & Garrick, Inc.
2216 University Drive
Newport Beach, CA 92660

Wayne L. Stiede
Commonwealth Edison Company
P.O. Box 767
Chicago, IL 60690

William Stratton
Stratton & Associates
2 Acoma Lane
Los Alamos, NM 87544

Soo-Pong Suk
Korea Advanced Energy Research
Institute
P. O. Box 7
Daeduk Danji, Chungnam 300-31
KOREA

W. P. Sullivan
GE Nuclear Energy
175 Curtner Ave., M/C 789
San Jose, CA 95125

Tony Taig
U.K. Atomic Energy Authority
Wigshaw Lane, Culcheth
Warrington, Cheshire, WA3 4NE
UNITED KINGDOM

John Taylor
Electric Power Research Institute
3412 Hillview Avenue
Palo Alto, CA 94303

Harry Teague
U.K. Atomic Energy Authority
Wigshaw Lane, Culcheth
Warrington, Cheshire, WA3 4NE
UNITED KINGDOM

Technical Library
Electric Power Research Institute
P.O. Box 10412
Palo Alto, CA 94304

Mark I. Temme
General Electric, Inc.
P.O. Box 3508
Sunnyvale, CA 94088

T. G. Theofanous
University of California, S.B.
Department of Chemical and Nuclear
Engineering
Santa Barbara, CA 93106

David Teolis
Westinghouse-Bettis Atomic Power
Laboratory
P. O. Box 79, ZAP 34N
West Mifflin, PA 15122-0079

Ashok C. Thadani
USNRC-NRR/SAD
MS: 7E-4

Garry Thomas
L-499 (Bldg. 490)
Lawrence Livermore National
Laboratory
7000 East Ave.
P.O. Box 808
Livermore, CA 94550

Gordon Thompson
Institute for Research and
Security Studies
27 Ellworth Avenue
Cambridge, MA 02139

Grant Thompson
League of Women Voters
1730 M. Street, NW
Washington, DC 20036

Arthur Tingle
Brookhaven National Laboratory
Building 130
Upton, NY 11973

Rich Toland
United Engineers and Construction
30 S. 17th St., MS 4V7
Philadelphia, PA 19101

Brian J. R. Tolley
DG/XII/D/1
Commission of the European
Communities
Rue de la Loi, 200
B-1049 Brussels
BELGIUM

David R. Torgerson
Atomic Energy of Canada Ltd.
Whiteshell Nuclear
Research Establishment
Pinawa, Manitoba, ROE 1LO
CANADA

Alfred F. Torri
Pickard, Lowe & Garrick, Inc.
191 Calle Magdalena, Suite 290
Encinitas, CA 92024

Klau Trambauer
Gesellschaft Fur Reaktorsicherheit
Forschungsgelande
D-8046 Garching
FERERAL REPUBLIC OF GERMANY

Nicholas Tsoulfanidis
Nuclear Engineering Dept.
University of Missouri-Rolla
Rolla, MO 65401-0249

Chao-Chin Tung
c/o H.B. Bengelsdorf
ERC Environmental Services Co.
P. O. Box 10130
Fairfax, VA 22030

Brian D. Turland
UKAEA Culham Laboratory
Abingdon, Oxon OX14 3DB
ENGLAND

Takeo Uga
Japan Institute of Nuclear Safety
Nuclear Power Engineering Test
  Center
3-6-2, Toranomon
Minato-ku, Tokyo 108
JAPAN

Stephen D. Unwin
Battelle Columbus Division
505 King Avenue
Columbus, OH 43201

A. Valeri
DISP
ENEA
Via Vitaliano Brancati, 48
I-00144 Rome
ITALY

Harold VanderMolen
USNRC-RES/PRAB
MS: NL/S-372

G. Bruce Varnado
ERC International
1717 Louisiana Blvd. NE, Suite 202
Albuquerque, NM 87110

Jussi K. Vaurio
Imatran Voima Oy
Loviisa NPS
SF-07900 Loviisa
FINLAND

William E. Vesely
Science Applications International
  Corporation
2929 Kenny Road, Suite 245
Columbus, OH 43221

J. I. Villadoniga Tallon
Div. of Analysis and Assessment
Consejo de Seguridad Nuclear
c/ Sor Angela de la Cruz, 3
28020 Madrid
SPAIN

Willem F. Vinck
Kapellestract 25
1980
Tervuren
BELGIUM

R. Virolainen
Office of Systems Integration
Finnish Centre for Radiation and
  Nuclear Safety
Department of Nuclear Safety
P.O. Box 268
Kumpulantie 7
SF-00520 Helsinki
FINLAND

Raymond Viskanta
School of Mechanical Engineering
Purdue University
West Lafayette, IN 47907

S. Visweswaran
General Electric Company
175 Curtner Avenue
San Jose, CA 95125

Truong Vo
Pacific Northwest Laboratory
Battelle Blvd.
Richland, WA 99352

Richard Vogel
Electric Power Research Institute
P. O. Box 10412
Palo Alto, CA 94303

G. Volta
Engineering Division
CEC Joint Research Centre
CP No. 1
I-21020 Ispra (Varese)
ITALY

Ian B. Wall
Electric Power Research Institute
3412 Hillview Avenue
Palo Alto, CA 94303

Adolf Walser
Sargent and Lundy Engineers
55 E. Monroe Street
Chicago, IL 60603

Edward Warman
Stone & Webster Engineering Corp.
P.O. Box 2325
Boston, MA 02107

Norman Weber
Sargent & Lundy Co.
55 E. Monroe Street
Chicago, IL 60603

Lois Webster
American Nuclear Society
555 N. Kensington Avenue
La Grange Park, IL 60525

Wolfgang Werner
Gesellschaft Fur Reaktorsicherheit
Forschungsgelande
D-8046 Garching
FEDERAL REPUBLIC OF GERMANY

Don Wesley
IMPELL
1651 East 4th Street
Suite 210
Santa Ana, CA 92701

Detlof von Winterfeldt
Institute of Safety and Systems
Management
University of Southern California
Los Angeles, CA 90089-0021

Pat Worthington
USNRC-RES/AEB
MS: NL/N-344

John Wreathall
Science Applications International
Corporation
2929 Kenny Road, Suite 245
Columbus, OH 43221

D. J. Wren
Atomic Energy of Canada Ltd.
Whiteshell Nuclear Research
Establishment
Pinawa, Manitoba, ROE 1LO
CANADA

Roger Wyrick
Inst. for Nuclear Power Operations
1100 Circle 75 Parkway, Suite 1500
Atlanta, GA 30339

Kun-Joong Yoo
Korea Advanced Energy Research
Institute
P. O. Box 7
Daeduk Danji, Chungnam 300-31
KOREA

Faith Young
Energy People, Inc.
Dixou Springs, TN 37057

Jonathan Young
R. Lynette and Associates
15042 Northeast 40th St.
Suite 206
Redmond, WA 98052

C. Zaffiro
Division of Safety Studies
Directorate for Nuclear Safety and
Health Protection
Ente Nazionale Energie Alternative
Via Vitaliano Brancati, 48
I-00144 Rome
ITALY

Mike Zentner
Westinghouse Hanford Co.
P. O. Box 1970
Richland, WA 99352

X. Zikidis
Greek Atomic Energy Commission
Agia Paraskevi, Attiki
Athens
GREECE

Bernhard Zuczera
Kernforschungszentrum
Postfach 3640
D-7500 Karlsruhe
FEDERAL REPUBLIC OF GERMANY

1521	J. R. Weatherby
3141	S. A. Landenberger [5]
3151	W. I. Klein
6344	E. D. Gorham-Bergeron
6400	D. J. McCloskey
6410	D. A. Dahlgren
6412	A. L. Camp
6412	S. L. Daniel
6412	T. M. Hake
6412	D. M. Kunsman
6412	L. A. Miller
6412	D. B. Mitchell
6412	A. C. Payne, Jr.
6412	T. T. Sype
6412	T. A. Wheeler
6412	D. W. Whitehead
6413	R. J. Breeding
6413	T. D. Brown
6413	J. J. Gregory
6413	F. T. Harper [2]
6415	R. M. Cranwell
6415	W. R. Cramond [3]
6415	R. L. Iman
6418	J. E. Kelly
6418	K. J. Maloney
6419	M. P. Bohn
6419	L. D. Bustard
6419	J. A. Lambright
6422	D. A. Powers
6425	S. S. Dosanjh
6425	D. R. Bradley
6429	K. D. Bergeron
6429	D. C. Williams
6453	J. S. Philbin
6500	A. W. Snyder
6510	J. V. Walker
6517	M. Berman
6517	M. P. Sherman
6521	D. D. Carlson
6523	W. A. von Riesemann
6523	D. B. Clauss
8524	J. A. Wackerly
9144	A. S. Benjamin