NUREG/CR-4674
ORNL/NOAC-232
Vol. 21

Precursors to Potential Severe Core Damage Accidents: 1994 A Status Report

Main Report and Appendices A–H

Prepared by
R. J. Belles, J. W. Cletcher, D. A. Copinger, B. W. Dolan, J. W. Minarick, L. N. Vanden Heuvel

Oak Ridge National Laboratory

Prepared for
U.S. Nuclear Regulatory Commission

AVAILABILITY NOTICE

Availability of Reference Materials Cited in NRC Publications

Most documents cited in NRC publications will be available from one of the following sources:

1. The NRC Public Document Room, 2120 L Street, NW., Lower Level, Washington, DC 20555-0001

2. The Superintendent of Documents, U.S. Government Printing Office, P. O. Box 37082, Washington, DC 20402-9328

3. The National Technical Information Service, Springfield, VA 22161-0002

Although the listing that follows represents the majority of documents cited in NRC publications, it is not intended to be exhaustive.

Referenced documents available for inspection and copying for a fee from the NRC Public Document Room include NRC correspondence and internal NRC memoranda; NRC bulletins, circulars, information notices, inspection and investigation notices; licensee event reports; vendor reports and correspondence; Commission papers; and applicant and licensee documents and correspondence.

The following documents in the NUREG series are available for purchase from the Government Printing Office: formal NRC staff and contractor reports, NRC-sponsored conference proceedings, international agreement reports, grantee reports, and NRC booklets and brochures. Also available are regulatory guides, NRC regulations in the *Code of Federal Regulations*, and *Nuclear Regulatory Commission Issuances*.

Documents available from the National Technical Information Service include NUREG-series reports and technical reports prepared by other Federal agencies and reports prepared by the Atomic Energy Commission, forerunner agency to the Nuclear Regulatory Commission.

Documents available from public and special technical libraries include all open literature items, such as books, journal articles, and transactions. *Federal Register* notices, Federal and State legislation, and congressional reports can usually be obtained from these libraries.

Documents such as theses, dissertations, foreign reports and translations, and non-NRC conference proceedings are available for purchase from the organization sponsoring the publication cited.

Single copies of NRC draft reports are available free, to the extent of supply, upon written request to the Office of Administration, Distribution and Mail Services Section, U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001.

Copies of industry codes and standards used in a substantive manner in the NRC regulatory process are maintained at the NRC Library, Two White Flint North, 11545 Rockville Pike, Rockville, MD 20852-2738, for use by the public. Codes and standards are usually copyrighted and may be purchased from the originating organization or, if they are American National Standards, from the American National Standards Institute, 1430 Broadway, New York, NY 10018-3308.

DISCLAIMER NOTICE

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, expressed or implied, or assumes any legal liability or responsibility for any third party's use, or the results of such use, of any information, apparatus, product, or process disclosed in this report, or represents that its use by such third party would not infringe privately owned rights.

NUREG/CR-4674
ORNL/NOAC-232
Vol. 21

Precursors to Potential Severe Core Damage Accidents: 1994 A Status Report

Main Report and Appendices A–H

Manuscript Completed: December 1995
Date Published: December 1995

Prepared by
R. J. Belles, J. W. Cletcher, D. A. Copinger, B. W. Dolan,* J. W. Minarick,* L. N. Vanden Heuvel

Oak Ridge National Laboratory
Managed by Lockheed Martin Energy Systems, Inc.

Oak Ridge National Laboratory
Oak Ridge, TN 37831-6285

Prepared for
Safety Programs Division
Office for Analysis and Evaluation of Operational Data
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001
NRC FIN B0435

*Science Applications International Corporation, Oak Ridge, TN 37831

Previous Reports in Series

1. J. W. Minarick and C. A. Kukielka, Union Carbide Corp., Nuclear Div., Oak Ridge Natl. Lab.; and Science Applications, Inc., *Precursors to Potential Severe Core Damage Accidents: 1969-1979, A Status Report*, USNRC Report NUREG/CR-2497 (ORNL/NSIC-18/V1 and V2), June 1982.

2. W. B. Cottrell, J. W. Minarick, P. N. Austin, E. W. Hagen, and J. D. Harris, Martin Marietta Energy Systems, Inc., Oak Ridge Natl. Lab.; and Science Applications International Corp., *Precursors to Potential Severe Core Damage Accidents: 1980-81. A Status Report*, USNRC Report NUREG/CR-3591, Vols. 1 and 2 (ORNL/NSIC-217/V1 and V2), July 1984.

3. J. W. Minarick et al., Martin Marietta Energy Systems, Inc., Oak Ridge Natl. Lab.; Science Applications International Corp.; and Professional Analysis, Inc., *Precursors to Potential Severe Core Damage Accidents: 1985, A Status Report*, USNRC Report NUREG/CR-4674 (ORNL/NOAC-232), Vols. 1 and 2, December 1986.

4. J. W. Minarick et al., Martin Marietta Energy Systems, Inc., Oak Ridge Natl. Lab.; Science Applications International Corp.; and Professional Analysis, Inc., *Precursors to Potential Severe Core Damage Accidents: 1984, A Status Report*, USNRC Report NUREG/CR-4674 (ORNL/NOAC-232), Vols. 3 and 4, May 1987.

5. J. W. Minarick et al., Martin Marietta Energy Systems, Inc., Oak Ridge Natl. Lab.; Science Applications International Corp.; and Professional Analysis, Inc., *Precursors to Potential Severe Core Damage Accidents: 1986, A Status Report*, USNRC Report NUREG/CR-4674 (ORNL/NOAC-232), Vols. 5 and 6, May 1988.

6. J. W. Minarick et al., Martin Marietta Energy Systems, Inc., Oak Ridge Natl. Lab.; Science Applications International Corp.; and Professional Analysis, Inc., *Precursors to Potential Severe Core Damage Accidents: 1987, A Status Report*, USNRC Report NUREG/CR-4674 (ORNL/NOAC-232), Vols. 7 and 8, July 1989.

7. J. W. Minarick et al., Martin Marietta Energy Systems, Inc., Oak Ridge Natl. Lab.; Science Applications International Corp.; and Professional Analysis, Inc., *Precursors to Potential Severe Core Damage Accidents: 1988, A Status Report*, USNRC Report NUREG/CR-4674 (ORNL/NOAC-232), Vols. 9 and 10, February 1990.

8. J. W. Minarick et al., Martin Marietta Energy Systems, Inc., Oak Ridge Natl. Lab.; Science Applications International Corp.; and Professional Analysis, Inc., *Precursors to Potential Severe Core Damage Accidents: 1989, A Status Report*, USNRC Report NUREG/CR-4674 (ORNL/NOAC-232), Vols. 11 and 12, August 1990.

9. J. W. Minarick et al., Martin Marietta Energy Systems, Inc., Oak Ridge Natl. Lab.; Science Applications International Corp.; and Professional Analysis, Inc., *Precursors to Potential Severe Core Damage Accidents: 1990, A Status Report*, USNRC Report NUREG/CR-4674 (ORNL/NOAC-232), Vols. 13 and 14, August 1991.

10. J. W. Minarick et al., Martin Marietta Energy Systems, Inc., Oak Ridge Natl. Lab., and Science Applications International Corp., *Precursors to Potential Severe Core Damage Accidents: 1991, A Status Report*, USNRC Report NUREG/CR-4674 (ORNL/NOAC-232), Vols. 15 and 16, September 1992.

11. D. A. Copinger et al., Martin Marietta Energy Systems, Inc., Oak Ridge Natl. Lab., and Science Applications International Corp., *Precursors to Potential Severe Core Damage Accidents: 1992, A Status Report*, USNRC Report NUREG/CR-4674 (ORNL/NOAC-232), Vols. 17 and 18, December 1993.

12. L. N. Vanden Heuvel et al., Martin Marietta Energy Systems, Inc., Oak Ridge Natl. Lab., and Science Applications International Corp., *Precursors to Potential Severe Core Damage Accidents: 1993, A Status Report*, USNRC Report NUREG/CR-4674 (ORNL/NOAC-232),Vols. 19 and 20, September 1994.

ABSTRACT

Nine operational events that affected eleven commercial light-water reactors (LWRs) during 1994 and that are considered to be precursors to potential severe core damage are described. All these events had conditional probabilities of subsequent severe core damage greater than or equal to 1.0×10^{-6}. These events were identified by computer-screening the 1994 licensee event reports from commercial LWRs to identify those that could be potential precursors. Candidate precursors were then selected and evaluated in a process similar to that used in previous assessments. Selected events underwent engineering evaluation that identified, analyzed, and documented the precursors. Other events designated by the Nuclear Regulatory Commission (NRC) also underwent a similar evaluation. Finally, documented precursors were submitted for review by licensees and NRC headquarters and regional offices to ensure that the plant design and its response to the precursor were correctly characterized. This study is a continuation of earlier work, which evaluated 1969-1981 and 1984-1993 events. The report discusses the general rationale for this study, the selection and documentation of events as precursors, and the estimation of conditional probabilities of subsequent severe core damage for events. This document is bound in two volumes: Vol. 21 contains the main report and Appendices A-H; Vol. 22 contains Appendix I.

Contents

Appendices

List of Figures

List of Tables

PREFACE

The Accident Sequence Precursor (ASP) Program was established by the Nuclear Operations Analysis Center at Oak Ridge National Laboratory (ORNL) in the summer of 1979. The first major report of that program was published in June 1982 and received extensive review. Twelve reports documenting the review of operational events for precursors have been published in this program (see Chap. 5). These reports describe events that occurred from 1969 through 1993, excluding 1982 and 1983. They have been completed on a yearly basis since 1987.

The current effort was undertaken on behalf of the Office for Analysis and Evaluation of Operational Data of the Nuclear Regulatory Commission (NRC). The NRC Project Manager is P. D. O'Reilly.

The methodology developed and utilized in the ASP Program permits a reasonable estimate of the significance of operational events, including observed human and system interactions. The present effort for 1994 is a continuation of the assessment undertaken in the previous reports for operational events that occurred in 1969-1981 and 1984-1993.

The preliminary analyses of the 1994 events were sent for review to NRC staff and licensees for those plants for which potential ASP events were identified. This is similar to the review process used for the 1992 and 1993 events. In addition, the 1994 events were also independently reviewed as part of NRC's policy regarding probabilistic risk assessment (PRA) activities. All comments were evaluated, and analyses were revised as appropriate.

Reanalyses typically focused on and gave credit for equipment and procedures that provided additional protection against core damage. These additional features were beyond what was normally included in ASP analyses of events prior to 1992. Therefore, comparing and trending analysis results from prior years is more difficult because analysis results before 1992 may have been different if additional information had been solicited from the licensees and incorporated.

For 1994 the total number of precursors identified is less than that of past years. This is due at least in part to incorporating feedback on equipment, systems, procedures, etc., such that events initially identified as potential precursors with a conditional core damage probability somewhat greater than 10^{-6} were reanalyzed resulting in a value less than 10^{-6}, which is the threshold for rejection. In addition, new models were used for the analysis of 1994 events. These models utilize ASP class-based event trees and plant-specific linked fault trees. The models are based on previous work performed by ORNL. The models were converted into the Integrated Reliability and Risk Analysis System software by the Idaho National Engineering Laboratory. These new models, which obviously influence the calculation of conditional core damage probabilities for events, represent another factor for consideration when comparing results for 1994 with those from previous years.

The operational events selected in the ASP Program form a unique data base of historical system failures, multiple losses of redundancy, and infrequent core damage initiators. These events are useful in identifying significant weaknesses in design and operation, for trends analysis concerning industry performance and the impact of regulatory actions, and for PRA-related information.

Gary T. Mays, Director
Nuclear Operations Analysis Center
Oak Ridge National Laboratory
P. O. Box 2009
Oak Ridge, Tennessee 37831-8065
(423) 574-0394

FOREWORD

This report provides the results of the review and evaluation of 1994 operational experience data by the Nuclear Regulatory Commission's ongoing Accident Sequence Precursor (ASP) Program. The ASP Program provides a safety significance perspective of nuclear plant operational experience. The program uses probabilistic risk assessment (PRA) techniques to provide estimates of operating event significance in terms of the potential for core damage. The types of events evaluated include initiators, degradations of plant conditions, and safety equipment failures that could increase the probability of postulated accident sequences.

The primary objective of the ASP Program is to systematically evaluate U.S. nuclear plant operating experience to identify, document, and rank those operating events which were most significant in terms of the potential for inadequate core cooling and core damage. In addition, the program has the following secondary objectives: (1) to categorize the precursor events for plant specific and generic implications, (2) to provide a measure which can be used to trend nuclear plant core damage risk, and (3) to provide a partial check on PRA-predicted dominant core damage scenarios.

This year marked the completion of the initial development of improvements in the methods used for the ASP analysis of operational events. The ASP analyses of 1994 operational experience were performed using the staff's recently developed simplified, plant-specific, train-level models for analyzing operational events. These models are based on the staff's Integrated Reliability and Risk Analysis System (IRRAS), which uses fault tree linking techniques to quantify accident sequences.

In recent years, licensees of U.S. nuclear plants have added safety equipment and have improved plant and emergency operating procedures. Some of these changes, particularly those involving use of alternate equipment or recovery actions in response to specific accident scenarios, can have a significant effect on the calculated conditional core damage probabilities for certain accident sequences. In keeping with established practice, the 1994 preliminary ASP analyses were transmitted to the pertinent nuclear plant licensees and to the NRC staff for review. The licensees were requested to review and comment on the technical adequacy of the analyses, including the depiction of their plant equipment and equipment capabilities. Each of the review comments received from licensees and the NRC staff was evaluated for reasonableness and pertinence to the ASP analysis in an attempt to use realistic values. All of the preliminary precursor events were reviewed, and the conditional core damage probability calculations were revised where appropriate. The objective of this review process was to provide as realistic an analysis of the significance of the event as possible. In addition, consistent with the recommendations of the NRC's interoffice PRA Working Group, each of the analyses has been independently peer reviewed. This review provided a quality check of the analysis, ensured consistency with the ASP analysis guidelines, and verified the adequacy of the modeling approach and appropriateness of the assumptions used in the analysis.

The total number of precursors (9) identified for 1994 is less than last year. The two most important precursor events for 1994 consisted of an intersystem loss-of-coolant accident (LOCA) which occurred at a PWR during shutdown, and the unavailability of both pressurizer power-operated relief valves (PORVs) for an extended period of time, which was discovered at another PWR.

Charles E. Rossi, Director
Safety Programs Division
Office for Analysis and Evaluation
of Operational Data

ACKNOWLEDGMENTS

The authors are grateful for the assistance of the Nuclear Regulatory Commission's Office for Analysis and Evaluation of Operational Data (AEOD). The AEOD project manager, P. D. O'Reilly, was instrumental in obtaining timely comments from the NRC staff and licensees and providing guidance on technical issues. Heather Schriner, Susan Dingman, Allen Camp, Jeff LaChance, and Donnie Whitehead of Sandia National Laboratories provided an independent technical review of each analysis. The authors wish to thank the following individuals for their technical review and analysis; their assistance was vital to the completion of this report.

Oak Ridge National Laboratory

W. E. Kohn

Reliability and Performance Associates

W. Lau

Nuclear Regulatory Commission

L. L. Collins

N. Watanabe*

In addition, the authors wish to thank the report staff for their assistance in word processing, technical editing, graphics preparation, and reproduction. The rapid turnaround of materials by these individuals was greatly appreciated.

A. G. Andrews
A. R. Bush
L. B. Dockery
D. S. Queener
D. G. Sharp
B. J. Smith
C. C. Southmayd
L. W. Xiques

Finally, the authors wish to express their thanks to T. W. Horning for her valuable assistance in preparing this document for publication.

*On loan from the Japan Atomic Energy Research Institute.

1. Introduction

The Accident Sequence Precursor (ASP) Program involves the review of licensee event reports (LERs) for operational events that have occurred at light-water reactors (LWRs). The ASP Program identifies and categorizes precursors to potential severe core damage accident sequences. The present report is a continuation of the work published in NUREG/CR-2497, *Precursors to Potential Severe Core Damage Accidents: 1969-1979, A Status Report,* [1] as well as ir earlier versions of this document.[2-12] This report details the review and evaluation of operational events that occurred in 1994. The requirements for LERs are described in Title 10 of the Code of Federal Regulations, Part 50.73 (10CFR50.73). Guidance on complying with these requirements is contained in NUREG-1022, *Licensee Event Report System, Description of System and Guidelines for Reporting.*[13-15]

1.1 Background

The ASP Program owes its genesis to the Risk Assessment Review Group,[16] which concluded that "unidentified event sequences significant to risk might contribute... a small increment...[to the overall risk]." The report continues, "It is important, in our view, that potentially significant [accident] sequences, and precursors, as they occur, be subjected to the kind of analysis contained in WASH-1400."[17] Evaluations done for the 1969-1981 period were the first efforts in this type of analysis.

This study focuses on accident sequences in which, if additional failures had occurred, inadequate core cooling would have resulted and, as a consequence, could have caused severe core damage. For example, a postulated loss-of-coolant accident with a failure of a high-pressure injection (HPI) system may be examined or studied. In this simple example, the precursor would be the HPI system failure.

Events considered to be potential precursors are analyzed, and a conditional probability of subsequent core damage is calculated. This is done by mapping the event onto ASP accident sequence models. Those events with conditional probabilities of subsequent severe core damage $\geq 1.0 \times 10^{-6}$ are identified and documented as precursors.

1.2 Current Process

The current process for identifying, analyzing, and documenting precursors is described in detail in Chapter 2. Preliminary precursor analyses were reviewed by licensees and Nuclear Regulatory Commission (NRC) headquarters and regional office staff. Each documented precursor analysis also received an independent review by an NRC contractor.

In addition to the events selected as accident sequence precursors, events involving (1) loss of containment function, (2) unusual failure modes or initiators, and (3) events that are impractical to analyze were identified. These events are also documented in this report.

The primary source of event information is the NRC's Sequence Coding and Search System (SCSS) data base. It contained 1374 LERs for 1994, and the ASP computer search algorithm selected 586 of these for two-engineer review as potential precursors. In addition, the NRC independently screens a number of data sources for potential precursors, including emergency notifications (as required by 10CFR50.72), LERs, inspection reports, Augmented Inspection Team (AIT) reports, and NRC-designated Significant Events. As a result of this process the NRC identified 36 events for review. From all of these sources for event information, the two-engineer review process identified 58 events (culled from 77 reports such as LERs and their revisions, AITs, etc.) as potentially significant events. Twenty-three of these events were rejected after detailed review, 12 events were determined to be impractical to analyze, 1 event was documented as a containment event, and 9 events were documented as "interesting" events. The remaining 13 events were found to be significant. Of these 13 events, 1 event was determined to be a shutdown precursor, 7 events were found to be individual at-pow‹r precursors, and the remaining 5 events were combined and analyzed as one precursor event. The results of these ar.alyses are tabulated in Chapter 3.

Chapter 2 describes the selection and analysis process used for the review of 1994 events. Chapter 3 provides a tabulation of the precursor events, a summary of the more important precursors, and insights on the results. The remainder of this report is divided into nine appendices: Appendix A describes the process used to model events, Appendix B describes the ASP models, Appendix C contains the at-power precursors, Appendix D contains shutdown precursors, Appendix E contains potentially significant events considered impractical to analyze, Appendix F contains the containment-related event, Appendix G contains the "interesting" events, Appendix H contains the resolution of licensee and NRC staff review comments, and Appendix I includes the LERs, Inspection Reports, and Augmented Inspection Team reports cited in Appendices C–G.

2. Selection Criteria and Quantification

2.1 Accident Sequence Precursor Selection Criteria

The Accident Sequence Precursor (ASP) Program is concerned with the identification and documentation of operational events that have involved portions of core damage sequences and with the estimation of associated frequencies and probabilities.

Identification of precursors requires the review of operational events for instances in which plant functions that provide protection against core damage have been challenged or compromised. Based on previous experience with reactor plant operational events, it is known that most operational events can be directly or indirectly associated with four initiators: trip [which includes loss of main feedwater (LOFW) within its sequences], loss-of-offsite power (LOOP), small-break loss-of-coolant accident (LOCA), and steam generator tube rupture (SGTR) (PWRs only). These four initiators are primarily associated with loss of core cooling. ASP Program staff members examine licensee event reports (LERs) and other event documentation to determine the impact that operational events have on potential core damage sequences.

2.1.1 Precursors

This section describes the steps used to identify events for quantification. Figure 2.1 illustrates this process.

A computerized search of the Sequence Coding and Search System (SCSS) data base at the Nuclear Operations Analysis Center (NOAC) of the Oak Ridge National Laboratory was conducted to identify LERs that met minimum selection criteria for precursors. This computerized search identified LERs potentially involving failures in plant systems that provide protective functions for the plant and core-damage-related initiating events. Based on a review of the 1984-1987 precursor evaluations and all 1990 LERs, this computerized search successfully identifies almost all precursors within a subset of approximately one-third to one-half of all LERs.

Events were also selected for review if an Augmented Inspection Team (AIT) or Incident Investigation Team (IIT) report was written regarding the event. In addition, the Nuclear Regulatory Commission (NRC) screens a number of other data sources to identify events for review. These sources include Significant Events for the NRC's Performance Indicator Program, events documented in NRC inspection reports, events reported in emergency notifications (as required by 10CFR50.72), as well as LERs.

Those events selected for review underwent at least two independent reviews by different NOAC staff members. Each LER was reviewed to determine if the reported event should be examined in greater detail. This initial review was a bounding review, meant to capture events that in any way appeared to deserve detailed review and to eliminate events that were clearly unimportant. This process involved eliminating events that satisfied predefined criteria for rejection and accepting all others as potentially significant and requiring analysis. Events also were eliminated from further review if they had little impact on core damage sequences or provided little new information on the risk impacts of plant operation; for example, short-term single failures in redundant systems, uncomplicated reactor trips, and LOFW events.

Events were eliminated from further consideration as precursors if they involved, at most, only one of the following:

- a component failure with no loss of redundancy,
- a short-term loss of redundancy in only one system,
- a seismic design or qualification error,
- an environmental design or qualification error,
- a structural degradation,
- an event that occurred prior to initial criticality,
- a design error discovered by reanalysis,

- an event bounded by a reactor trip or LOFW,
- an event with no appreciable impact on safety systems, or
- an event involving only post core-damage impacts.

Events identified for further consideration typically included the following:

- unexpected core damage initiators (LOOP, SGTR, and small-break LOCA);
- all events in which a reactor trip was demanded and a safety-related component failed;
- all support system failures, including failures in cooling water systems, instrument air, instrumentation and control, and electric power systems;
- any event in which two or more failures occurred;
- any event or operating condition that was not predicted or that proceeded differently from the plant design basis; and
- any event that, based on the reviewers' experience, could have resulted in or significantly affected a chain of events leading to potential severe core damage.

Events determined to be potentially significant as a result of this initial review were then subjected to a thorough, detailed analysis. This extensive analysis was intended to identify those events considered to be precursors to potential severe core damage accidents, either because of an initiating event or because of failures that could have affected the course of postulated off-normal events or accidents. These detailed reviews were not limited to the LERs; they also used final safety analysis reports (FSARs) and their amendments, individual plant examinations (IPEs), and other information available at NOAC and from the NRC, related to the events of interest.

The detailed review of each event considered the immediate impact of an initiating event or the potential impact of the equipment failures or operator errors on the readiness of systems in the plant for mitigation of off-normal and accident conditions. In the review of each selected event, three general scenarios (involving both the actual event and postulated additional failures) were considered.

1. If the event or failure was immediately detectable and occurred while the plant was at power, then the event was evaluated according to the likelihood that it and the ensuing plant response could lead to severe core damage.
2. If the event or failure had no immediate effect on plant operation (i.e., if no initiating event occurred), then the review considered whether the plant would require the failed items for mitigation of potential severe core damage sequences should a postulated initiating event occur during the failure period.
3. If the event or failure occurred while the plant was not at power, then the event was first assessed to determine whether it could have occurred while at power or at hot shutdown immediately following power operation. If the event could only occur at cold shutdown or refueling shutdown, or the condition clearly did not impact at-power operation, then its impact on continued decay heat removal during shutdown was assessed; otherwise it was analyzed as if the plant were at power.

For each actual occurrence or postulated initiating event associated with a selected operational event, the sequence of operation of various mitigating systems required to prevent core damage was considered. Events were selected and documented as precursors to potential severe core damage accidents (accident sequence precursors) if the conditional probability of subsequent core damage was at least 1.0×10^{-6} (see Sect. 2.2) and the event satisfied at least one of the four precursor selection criteria: (1) a core damage initiator requiring safety system response, (2) the failure of a system required to mitigate the consequences of a core damage initiator, (3) degradation of more than one system required for mitigation, or (4) a trip or loss-of-feedwater with a degraded mitigating system. Events of low significance were thus excluded, allowing attention to be focused on the more important events. This approach is consistent with the approach used to define 1988-1993 precursors, but differs from that of earlier ASP reports, which addressed all events meeting the precursor selection criteria regardless of conditional core damage probability.

Nine operational events with conditional probabilities of subsequent severe core damage $\geq 1.0 \times 10^{-6}$ were identified as accident sequence precursors. Eight of these were analyzed as at-power events, while the remaining event was analyzed as a shutdown event.

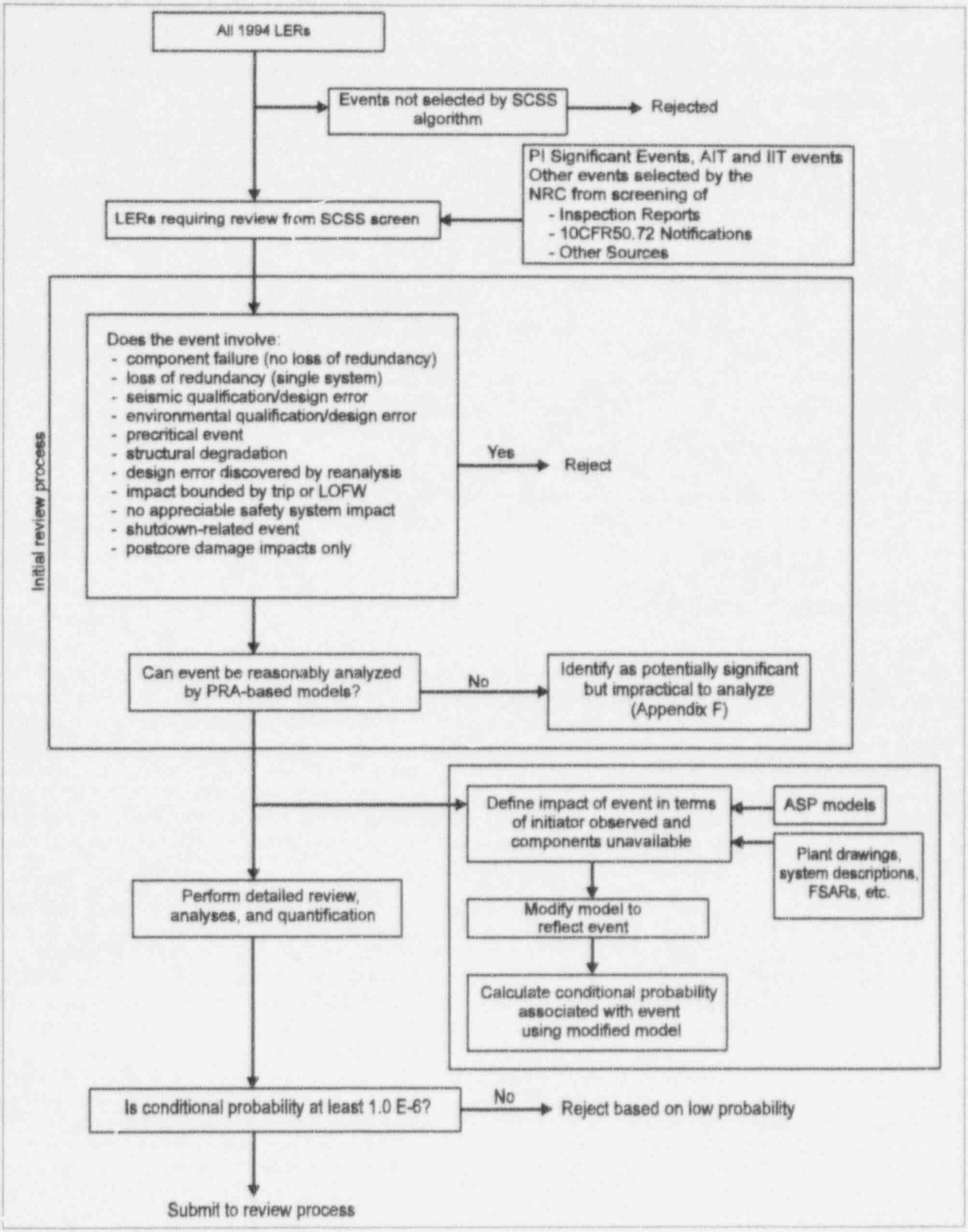

All 1994 LERs
Events not selected by SCSS algorithm
Rejected
PI Significant Events, AIT and IIT events
Other events selected by the NRC from screening of
- Inspection Reports
- 10CFR50.72 Notifications
- Other Sources
LERs requiring review from SCSS screen
Initial review process
Does the event involve:
- component failure (no loss of redundancy)
- loss of redundancy (single system)
- seismic qualification/design error
- environmental qualification/design error
- precritical event
- structural degradation
- design error discovered by reanalysis
- impact bounded by trip or LOFW
- no appreciable safety system impact
- shutdown-related event
- postcore damage impacts only
Yes
Reject
Can event be reasonably analyzed by PRA-based models?
No
Identify as potentially significant but impractical to analyze (Appendix F)
Define impact of event in terms of initiator observed and components unavailable
ASP models
Plant drawings, system descriptions, FSARs, etc.
Modify model to reflect event
Calculate conditional probability associated with event using modified model
Perform detailed review, analyses, and quantification
Is conditional probability at least 1.0 E-6?
No
Reject based on low probability
Submit to review process

Figure 2.1. ASP analysis process.

2.1.2 Potentially Significant Events Considered Impractical to Analyze

In some cases, events are impractical to analyze due to a lack of information or the inability to reasonably model the event within a probabilistic risk assessment (PRA) framework, considering the level of detail typically available in PRA models and the resources available to the ASP Program.

Several events identified as potentially significant were considered impractical to analyze. It is thought that such events are capable of impacting core damage sequences. However, the events usually involve component degradations in which the extent of the degradation could not be determined or the impact of the degradation on plant response could not be ascertained. Descriptions of events considered impractical to analyze are provided in Appendix E.

2.1.3 Containment-Related Events

In addition to accident sequence precursors, events involving loss of containment functions, such as containment cooling, containment spray, containment isolation (direct paths to the environment only), or hydrogen control, were identified in the yearly review of 1994 events and are documented in Appendix F.

2.1.4 "Interesting" Events

Other events that provided insight into unusual failure modes with the potential to compromise continued core cooling but that were determined not to be precursors were also identified. These are documented as "interesting" events in Appendix G.

2.2 Precursor Quantification

Quantification of accident sequence precursor significance involves determination of a conditional probability of subsequent severe core damage, given the failures observed during an operational event. This is estimated by mapping failures observed during the event onto the ASP accident sequence models, which depict potential paths to severe core damage, and calculating a conditional probability of core damage through the use of event trees and linked fault trees modified to reflect the event. The effect of a precursor on accident sequences is assessed by reviewing the operational event specifics against system design information. Quantification results in a revised conditional probability of core damage, given the operational event. The conditional probability estimated for each precursor is useful in ranking because it provides an estimate of the measure of protection against core damage that remains once the observed failures have occurred.

Two important changes were made this year to the calculation approach used in the ASP Program. Linked fault trees are used instead of the earlier event tree based models. The use of linked fault trees allows the impact of individual component failures to be correctly addressed; this could only be approximated in the earlier models. In addition, the probability calculated for condition assessments (events in which components are unavailable for a period of time during which an initiating event could have occurred) has been modified. In the current report, the conditional core damage probability (CCDP) during the time period given the failures observed is used to rank the condition assessment events. In previous reports, the difference between the CCDP and the core damage probability (CDP) was used. This difference was referred to as the conditional core damage probability in previous reports (although this is actually an importance measure). To determine the importance measure, the conditional core damage probability given the failures that were observed was calculated. Then the CDP was calculated for the same time period by assuming nominal failure rates for all components, even those that were failed during the event. The difference between these values was used to rank the condition assessments. For most of the condition assessments that meet the ASP selection criteria, the observed failures significantly impact the core damage model. In these cases, there is little numeric difference between the CCDP and the importance measure that was previously used (CCDP–CDP). For some events, however, nominal plant response during the time period dominates the results. In these cases, the CCDP can be considerably higher than the importance measure. For conditions that involve extended time periods, the CCDP can be quite large, even though the impact of the condition on the plant response is minimal. For example, the assessment of LER 250/94-005 (see p. C.5-4) resulted in a CCDP of 9.7×10^{-5}, a CDP of 9.5×10^{-5}, and an importance measure of 1.8×10^{-6}. Because the reported event covers a one-year period of time, the assessment of the nominal plant response over the time period yields a baseline plant CDP of 9.5×10^{-5}. The observed failures increase the CCDP to 9.7×10^{-5}. By only looking at the CCDP for this event, its importance may be overestimated. Therefore, for condition assessments, the CCDP, CDP, and the difference between the two values are provided for each condition assessment.

For initiating events, the CCDP used in the current report is the same as that used in previous reports. That is, the CCDP is calculated by setting the initiating event probability to 1.0 and modifying the other basic event probabilities based on the observed performance of systems and components. Additional discussion concerning the analysis methods used can be found in Appendix A.

Some of the frequencies and failure probabilities used in the calculations were developed from plant-specific data while others are derived from data obtained across the light-water reactor (LWR) population. It is the goal of the ASP Program to make the models as plant-specific as possible, reflecting plant-specific configuration, component reliability, and operator actions. However, due to programmatic limitations, the current versions of the models still contain some nonplant-specific data. The conditional probabilities determined using plant-specific data for each event may differ slightly from those obtained with the current set of data. Appendix B documents the event trees and fault trees used in the 1994 precursor analyses.

As a result of the changes made in the processes and the models used for the analysis of the 1994 events, the results are not directly comparable to the results of previous years.

2.3 Review of Precursor Documentation

This section describes the steps involved in the review of the event analyses. Figure 2.2 illustrates this process.

After completion of the preliminary analyses of the events, the analyses were transmitted to the pertinent nuclear plant licensees and to the NRC staff for review. The licensees were requested to review and comment on the technical adequacy of the analyses, including the depiction of their plant equipment and equipment capabilities. Each of the review comments was evaluated for reasonableness and pertinence to the ASP analysis. Although all of the preliminary precursor events were sent out for review, comments were not received from all the licensees. Each of the comments received was reviewed to determine the effect on the modeling of the events.

As with the 1993 events, the 1994 precursor analyses were also sent to an NRC contractor, Sandia National Laboratories (SNL), for an independent review. The review was intended to (1) provide an independent quality check of the analyses, (2) ensure consistency with the ASP analysis guidelines and with other ASP analyses for the same event type, and (3) verify the adequacy of the modeling approach and appropriateness of the assumptions used in the analyses.

After the preliminary analyses were revised based on licensee, NRC, and SNL comments, the analyses were sent back to the NRC and SNL for additional comments. The analyses were revised again, as necessary, based on the additional NRC and SNL comments.

The comments received on the preliminary analyses fell into three basic categories: (1) additional plant-specific equipment and event mitigation strategies available for the initiating events of interest, (2) clarification of event conditions and actual or potential licensee actions in response to the event, and (3) plant-specific probability data. The comments varied in level of detail and completeness. Due to program limitations, the applicability of the comments was restricted to the associated analysis and no effort was made to assess the potential applicability of the comments to the other analyses or the effects of modifying the remaining analyses in a similar manner. Reviewing the applicability of each comment across all of the events would have affected the conditional core damage probability for some of the events. It is possible that this would affect the ranking of the events.

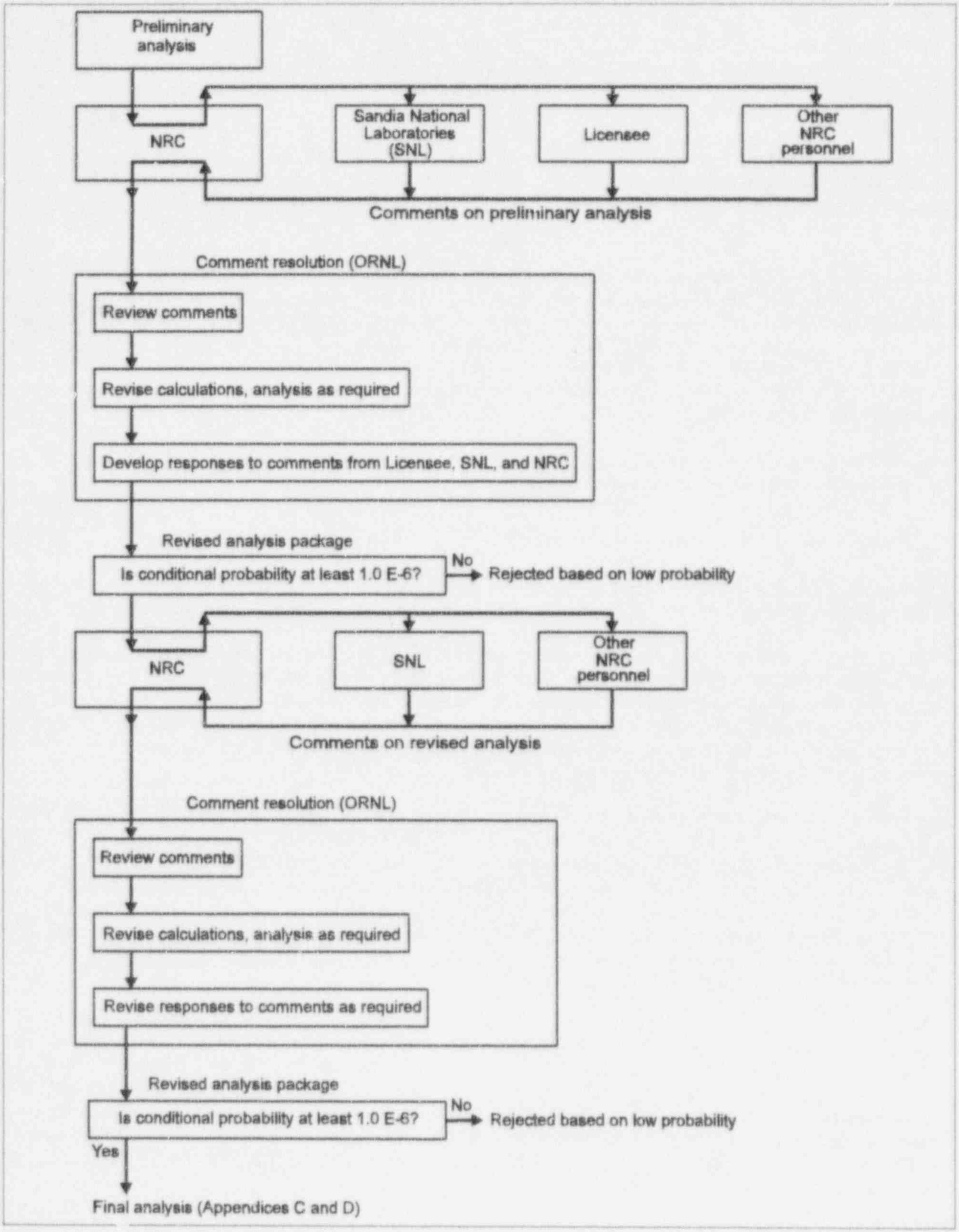

Preliminary analysis
NRC
Sandia National Laboratories (SNL)
Licensee
Other NRC personnel
Comments on preliminary analysis
Comment resolution (ORNL)
Review comments
Revise calculations, analysis as required
Develop responses to comments from Licensee, SNL, and NRC
Revised analysis package
Is conditional probability at least 1.0 E-6?
No
Rejected based on low probability
NRC
SNL
Other NRC personnel
Comments on revised analysis
Comment resolution (ORNL)
Review comments
Revise calculations, analysis as required
Revise responses to comments as required
Revised analysis package
Is conditional probability at least 1.0 E-6?
No
Rejected based on low probability
Yes
Final analysis (Appendices C and D)

Figure 2.2.ASP review process.

A summary of the comments received from the licensees and the NRC staff, as well as a response to each comment, can be found in Appendix H.

2.4 Precursor Documentation Format

The 1994 precursors are documented in Appendices C and D. The eight at-power events are contained in Appendix C, and the shutdown event is contained in Appendix D. A description of each event is provided with additional information relevant to the assessment of the event, the ASP modeling assumptions and approach used in the analysis, and analysis results. A figure indicating the dominant core damage sequence associated with each event is also included.

For most events the conditional core damage probability calculation is documented in a series of tables. The tables include selected basic event probabilities; sequence logic; probabilities, importance, and system names for higher probability sequences; and selected cut sets for higher probability sequences. For the remaining events, the calculational methods are described in the text. Copies of the LERs, NRC inspection reports, and AIT reports relevant to the events are contained in Appendix I.

2.5 Potential Sources of Error

As with any analytic procedure, the availability of information and modeling assumptions can bias the results. In this section, several of these potential sources of error are addressed.

1. *Evaluation of only a subset of 1994 LERs.* For 1969–1981 and 1984–1987, all LERs reported during the year were evaluated for precursors. For 1988–1994, only a subset of the LERs was evaluated in the ASP Program after a computerized search of the SCSS data base and screening by NRC personnel. While this subset is thought to include most serious operational events, it is possible that some events that would normally be selected as precursors were missed because they were not included in the subset that resulted from the screening process. Since 1993, this likelihood has been reduced due to the augmentation of the LER screening process within the ASP Program by the NRC's daily review of other sources of operational event data.
2. *Inherent biases in the selection process.* Although the criteria for identification of an operational event as a precursor are fairly well-defined, the selection of an event for initial review can be somewhat judgmental. Events selected in the study were more serious than most, so the majority of the events selected for detailed review would probably have been selected by other reviewers with experience in LWR systems and their operation. However, some differences would be expected to exist; thus, the selected set of precursors should not be considered unique. With the augmentation of the LER screening process by multiple NRC reviews of operational data sources, the influence of this error source on the results should be significantly reduced.
3. *Lack of appropriate event information.* The accuracy and completeness of the LERs and other event-related documentation in reflecting pertinent operational information are questionable in some cases. Requirements associated with LER reporting (i.e., 10 CFR 50.73), plus the approach to event reporting practiced at particular plants, can result in variation in the extent of events reported and report details among plants. Although the LER Rule of 1984 has reduced the variation in reported details, some variation still exists. In addition, only details of the sequence (or partial sequences for failures discovered during testing) that actually occurred are usually provided; details concerning potential alternate sequences of interest in this study must often be inferred.
4. *Accuracy of the ASP models and probability data.* The event trees used in the analysis are plant-class specific and reflect differences between plants in the eight plant classes that have been defined. The fault trees are structured to reflect the plant-specific systems. While major differences between plants are represented in this way, the plant models utilized in the analysis may not adequately reflect all important differences. Known problems concern ac power recovery following a LOOP and battery depletion (station blackout issues). Modeling improvements that address these problems are being pursued in the ASP Program.

Several problems have been noted with the new IRRAS-based models supplied to ORNL by the NRC that were used to analyze the 1994 events identified. Not all of these problems could be resolved prior to the completion of this report. ORNL event analysts identified and corrected those problems that were judged to have a significant impact on the analysis results. Determining the impact of the remaining problems is currently beyond the scope of the ASP Program resources. However, it is believed that the remaining modeling problems will not significantly impact the results presented.

Because of the sparseness of system failure events, data from many plants must be combined to estimate the failure probability of a multitrain system or the frequency of low- and moderate-frequency events (such as LOOPs and small-break LOCAs). Because of this, the modeled response for each event will tend toward an average response for the plant class. If systems at the plant at which the event occurred are better or worse than average (difficult to ascertain without extensive operating experience), the actual conditional probability for an event could be higher or lower than that calculated in the analysis.

Known plant-specific equipment and procedures that can provide additional protection against core damage beyond the features included in the ASP models were addressed in the 1994 precursor analysis. This information was not uniformly available; much of it was provided in licensee comments on preliminary analyses and in IPE documentation available at the time this report was prepared. As a result, consideration of additional features may not be consistent in precursor analyses of events at different plants. However, multiple events that occurred at an individual plant or at similar units at the same site have been consistently analyzed.

5. *Difficulty in determining the potential for recovery of failed equipment.* Assignment of recovery credit for an event can have a significant impact on the assessment of the event. The approach used to assign recovery credit is described in detail in Appendix B. The actual likelihood of failing to recover from an event at a particular plant is difficult to assess and may vary substantially from the values currently used in the ASP analyses. This difficulty is demonstrated in the genuine differences in opinion among analysts, operations and maintenance personnel, and others, concerning the likelihood of recovering from specific failures (typically observed during testing) within a time period that would prevent core damage following an actual initiating event.

6. *Assumption of a 1-month test interval.* The core damage probability for precursors involving unavailabilities is calculated on the basis of the exposure time associated with the event. For failures discovered during testing, the time period is related to the test interval. A test interval of 1 month was assumed unless another interval was specified in the event documentation. See Reference 2 for a more comprehensive discussion of test interval assumptions.

3. Results

This chapter summarizes results of the review and evaluation of 1994 operational events. The primary result of the ASP Program is the identification of operational events with conditional core damage probabilities of $\geq 1.0 \times 10^{-6}$ that satisfy at least one of the four precursor selection criteria: (1) a core damage initiator requiring safety system response, (2) the failure of a system required to mitigate the consequences of a core damage initiator, (3) degradation of more than one system required for mitigation, or (4) a trip or loss-of-feedwater with a degraded mitigating system. Nine such events identified for 1994 are documented in Appendices C and D.

Direct comparison of results with those of earlier years is not possible without substantial effort to reconcile analysis differences. The plant-class event trees and plant-specific fault trees were first used to model the current year's events. Additional equipment and procedures (beyond those addressed in the ASP models described in Appendix A of Vol. 17) were incorporated into the analysis of 1992 and 1993 events. The models used in the analysis of 1988–1993 events differ from those used in 1984–1987 analyses. Starting in 1988, the project team evaluated only a portion of the LERs (as described in Sect. 2.1.1). Before 1988, all LERs were reviewed. Beginning with the review of 1993 events, the screening and review of LERs in the ASP Program were supplemented by the NRC's screening and review of other operating event data. Because of the differences in review and analysis methods, only limited observations are provided here. Refer to the 1986 precursor report[5] for a discussion of observations for 1984–1986 results and to the 1987–1991 reports[6-10] for the results of those years.

3.1 Tabulation of Precursor Events

The 1994 accident sequence precursor events are listed in Tables 3.1–3.6. The following information is included in each table:

- Docket/document number associated with the event (Event Identifier)
- Name of the plant where the event occurred (Plant)
- A brief description of the event (Description)
- Conditional probability of potential core damage associated with the event [p(cd)]
- Date of the event (Event Date)
- Plant type (Plant Type)
- Initiator associated with the event or unavailability if no initiator was involved (Event Type)

The tables are sorted as follows:

- Table 3.1–At-power precursors involving unavailabilities sorted by plant
- Table 3.2–At-power precursors involving initiating events sorted by plant
- Table 3.3–Shutdown precursors involving initiating events sorted by plant
- Table 3.4–At-power precursors involving unavailabilities sorted by conditional core damage probability
- Table 3.5–At-power precursors involving initiating events sorted by conditional core damage probability
- Table 3.6–Shutdown precursors involving initiating events sorted by conditional core damage probability

Table 3.1. At-power precursors involving unavailabilities sorted by plant

Plant	Event identifier	Description	Plant type	Event date	p(cd)	Event type
Dresden 2	LER 237/94-018	Motor Control Center Trips Due to Improper Breaker Settings	BWR	6/8/94	6.1×10^{-6}	Unavail.
Dresden 2	LER 237/94-021	Long-Term Unavailability of High Pressure Coolant Injection	BWR	8/4/94	3.1×10^{-6}	Unavail.
Haddam Neck	LERs 213/94-004, -005, -007, -013, IR 213/94-03	Power-Operated Relief Valves and Vital 480-V ac Bus Degraded	PWR	2/16/94	1.4×10^{-4}	Unavail.
Point Beach 1 and 2	LER 266/94-002	Both Diesel Generators Inoperable	PWR	2/8/94	1.2×10^{-5}	Unavail.
Turkey Point 3 and 4	LER 250/94-005	Load Sequencers Periodically Inoperable	PWR	11/3/94	1.8×10^{-6}	Unavail.
Zion 2	LER 304/94-002	Unavailability of Turbine-Driven Auxiliary Feedwater Pump and Emergency Diesel Generator	PWR	3/7/94	2.3×10^{-5}	Unavail.

Table 3.2. At-power precursors involving initiating events sorted by plant

Plant	Event identifier	Description	Plant type	Event date	p(cd)	Event type
Calvert Cliffs 2	LER 318/94-001	Trip, Loss of 13.8-kV Bus, and Short-Term Saltwater Cooling System Unavailable	PWR	1/12/94	1.3×10^{-5}	Reactor Trip
River Bend	LER 458/94-023	Scram, Main Turbine-Generator Fails to Trip, Reactor Core Isolation Cooling and Control Rod Drive Systems Unavailable	BWR	9/8/94	1.8×10^{-5}	Reactor Trip

Table 3.3. Shutdown precursors involving initiating events sorted by plant

Plant	Event identifier	Description	Plant type	Event date	p(cd)	Event type
Wolf Creek	IR 482/94-018	Reactor Coolant System Blows Down to Refueling Water Storage Tank During Hot Shutdown	PWR	9/17/94	3.0×10^{-3}	Interfacing LOCA

Table 3.4. At-power precursors involving unavailabilities sorted by conditional core damage probability

p(cd)	Plant	Plant type	Event identifier	Description	Event date	Event type
1.4×10^{-4}	Haddam Neck	PWR	LERs 213/94-004, -005, -007, -013, IR 213/94-03	Power-Operated Relief Valves and Vital 480-V ac Bus Degraded	2/16/94	Unavail.
2.3×10^{-5}	Zion 2	PWR	LER 304/94-002	Unavailability of Turbine-Driven Auxiliary Feedwater Pump and Emergency Diesel Generator	3/7/94	Unavail.
1.2×10^{-5}	Point Beach 1 and 2	PWR	LER 266/94-002	Both Diesel Generators inoperable	2/8/94	Unavail.
6.1×10^{-6}	Dresden 2	BWR	LER 237/94-018	Motor Control Center Trips Due to Improper Breaker Settings	6/8/94	Unavail.
3.1×10^{-6}	Dresden 2	BWR	LER 237/94-021	Long-Term Unavailability of High Pressure Coolant Injection	8/4/94	Unavail.
1.8×10^{-6}	Turkey Point 3 and 4	PWR	LER 250/94-005	Load Sequencers Periodically Inoperable	11/3/94	Unavail.

Table 3.5. At-power precursors involving initiating events sorted by conditional core damage probability

p(cd)	Plant	Plant type	Event identifier	Description	Event date	Event type
1.8×10^{-5}	River Bend	BWR	LER 458/94-023	Scram, Main Turbine-Generator Fails to Trip, Reactor Core Isolation Cooling and Control Rod Drive Systems Unavailable	9/8/94	Reactor Trip
1.3×10^{-5}	Calvert Cliffs 2	PWR	LER 318/94-001	Trip, Loss of 13.8-kV Bus, and Short-Term Saltwater Cooling System Unavailable	1/12/94	Reactor Trip

Table 3.6. Shutdown precursors involving initiating events sorted by conditional core damage probability

p(cd)	Plant	Plant type	Event identifier	Description	Event date	Event type
3.0×10^{-3}	Wolf Creek	PWR	IR 482/94-018	Reactor Coolant System Blows Down to Refueling Water Storage Tank During Hot Shutdown	9/17/94	Interfacing LOCA

3.1.1 Potentially Significant Events That Were Impractical to Analyze

Twelve potentially significant events were considered impractical to analyze for 1994. Typically, this event category includes events that are impractical to analyze due to lack of information or the inability to reasonably model the event within a probabilistic risk assessment framework, considering the level of detail typically available in probabilistic risk analysis models. These potentially significant events are documented in Appendix E of this report.

3.1.2 Containment-Related Events

One containment-related event was found for 1994. This event category includes losses of containment functions, such as containment cooling, containment spray, containment isolation (direct paths to the environment only), or hydrogen control. A description of this event is located in Appendix F.

3.1.3 "Interesting" Events

Nine "interesting" events were found for 1994. This event category includes events that were not selected as precursors and events rejected on low probability that provided insight into unusual failure modes with the potential for compromise of continued core cooling. For example, a particularly interesting event occurred at Salem 1. Following an unexpected reactor trip at Salem 1, two safety injections (SI) were automatically initiated. The first SI was caused by a main steam pressure pulse and resulted in the pressurizer filling completely with water. This is called a "solid condition." The second SI was caused by a rapid decrease in reactor system pressure when a secondary-side safety valve opened with the pressurizer "solid." The pressurizer power-operated relief valves actuated over 300 times during this event. Complete descriptions of this event and other "interesting" events are located in Appendix G of this report.

3.2 Important Precursors

Two precursors with conditional core damage probabilities of $\geq 10^{-4}$ were identified for 1994. Events with such conditional probabilities have traditionally been considered important in the ASP Program. For 1994, these events include the following:

3.2.1 Wolf Creek, RCS Blows Down to Refueling Water Storage Tank During Hot Shutdown

At 0400 hours on September 17, 1994, Wolf Creek was in Mode 4 preparing to begin a refueling outage with a reactor coolant system (RCS) pressure of 340 psig and temperature of 300°F. Two reactor coolant pumps (RCPs) were in service, the steam generators were filled, and the condenser and condensate systems were secured. The safety injection (SI) pumps and one of two centrifugal charging pumps were out of service with breakers open to prevent low-temperature overpressurization. Residual heat removal (RHR) train A was in service to provide shutdown cooling.

Maintenance work was being performed on RHR valve 8716A, the A RHR to safety injection system hot leg recirculation isolation valve, and efforts were in progress to ready RHR train B for use.

RHR train B was being lined up for recirculation back to the refueling water storage tank (RWST) to raise boron concentration before placing the train in service. This required the opening of valve 8717, a manual valve in the 8-in. common line from the RHR pump discharge headers to the RWST emergency core cooling systems (ECCS) pump suction header. A nuclear station operator (NSO) was dispatched to locally open valve 8717. The operators then received a call from a plant electrician requesting that valve 8716A be stroked (closed and reopened) in support of a test procedure. Meanwhile, the NSO had arrived at valve 8717 and prepared to open it.

Approximately 3 ft from the NSO, the electrician was working on valve 8716A, but neither he nor the NSO recognized the significance of opening valves 8717 and 8716A simultaneously. When opened together, valves 8716A and 8717 provide a direct pathway from the RHR pump discharge to the RWST ECCS suction header. When the control room operator closed valve 8716A from the control room, the operator stationed at valve 8717 apparently had only begun opening it. As water flowed from the RCS to the RWST, pressurizer level dropped about 2%, but this was not noted until the event was reviewed later. After valve 8716A closed, the control room operator waited about 30 s and then reopened it.

Valve 8717 was fully open by this time and reactor coolant inventory began rapidly flowing to the RWST. The operator stationed at 8717 observed loud flow and water hammer noises, called the control room to report them, and was instructed to close the valve. This instruction was apparently based on good operating practice to reclose a valve when unexpected flow and noise result from opening it, rather than from an understanding of the circumstances of the event. At the same time, control room personnel received a high RWST level alarm, the pressurizer level high annunciator cleared, and the pressurizer level instrumentation "pegged low."

Operators responded by tripping the RCPs, increasing charging flow, and manually isolating letdown. A relief supervising operator who was present at the time identified the flow path through valves 8716A and 8717 to the RWST. Operators closed valve 8716A, isolating the blowdown about 66 s into the event.

During the time that the blowdown was in progress, about 9,200 gal flowed from the RCS to the RWST, causing the RWST to overflow. Approximately 650 gal overflowed from the RWST to the waste holdup tank. The RHR and charging systems remained in service, and RCS level was gradually restored.

Subsequent analysis determined that, had the blowdown not been quickly isolated, the primary system could have drained down to the RCS loop elevation in as little as 3 min. The RWST ECCS suction header could have been filled with steam shortly thereafter. It was further determined that an operating RHR pump could have been damaged by as little as 0.5 min of operation after the primary system drained down to the RCS loop elevation. Unisolated, the blowdown could have led to core uncovery in as little as 30 min, based on a Westinghouse analysis of the event.

The Westinghouse analysis, performed after the event, suggests that once the RWST ECCS suction header voided, operation of the multistage SI pumps would have resulted in their failure. Isolation of the blowdown path would have allowed water to flow back from the RWST into the suction header; however, there is no assurance that the ECCS pumps could fulfill their functions while drawing water from the RWST following such an event.

The Westinghouse analysis also indicates that if the suction header voided, recovery of the RHR pumps would be problematic even if they were shut off in time. In less than the time required to fill, vent, and restart an RHR pump, reactor pressure could exceed the RHR reactor high-pressure shutoff point.

Evaluation of this event is strongly influenced by assumptions regarding human reliability, the time and degree of effort required to recover ECCS systems, and the viability of the "reflux" cooling method, wherein steam from a boiling core may be condensed in the steam generator tubes with the condensate draining back to the reactor. Substantial uncertainty is associated with each of these assumptions.

Approximately 3 min were available for the operators to diagnose and isolate the blowdown before all RHR and ECCS pumps were rendered inoperable. Even though procedures did not address the response to this condition, the operators' understanding of the existing system alignment allowed them to rapidly diagnose and correct the problem. During the event, the blowdown was isolated after a period of 66 s.

To estimate the likelihood that operators would fail to isolate the blowdown prior to uncovering the RCS loops, the time reliability correlation (TRC) models from *Human Reliability Analysis* (Dougherty and Fragola, Wiley, 1988) were employed. Operator response within the first 3 min was assumed to be rule-based and without hesitancy. This is considered appropriate based on the indications available to the operators at the time. Setting the median response time to the response time observed in this event (~60 s), and using Table 10-8 of Dougherty and Fragola, results in an estimated crew error probability of 0.06.

Had operators failed to isolate the blowdown path within 3 min, a direct vent path would have been established from the RCS through the RWST. Analyses were performed showing that core damage could have occurred as little as 27 min later.

After the RCS loops voided at 3 min, the ECCS common suction header would have begun to void. Additional consequences of a failure to terminate the event prior to this point would require more difficult operator actions. These actions were considered recovery (general diagnosis that must be used in the absence of rules) with hesitancy (due to conflict, burden and uncertainty) within the context of the TRC model. Based on Table 10-11 in Dougherty and Fragola, a crew failure probability of 0.05 is estimated for the 27-min time period.

If the blowdown had been isolated after the loops voided (after 3 min, but before 30 min), substantial time and effort would have been required to refill and vent the RWST ECCS suction header and the ECCS pump suctions, which are aligned to it. An analysis performed by Westinghouse indicates that significant voids entrained in the suction supply (5–20%) would guarantee a loss of ECCS prime, and other analyses have shown that operation in that condition for more than a minute or two would cause pump failure.

Without extensive venting and priming, the high-pressure pumps would be expected to fail after loop voiding. The high-pressure ECCS pumps were, therefore, assumed in this analysis to be unavailable once the RWST ECCS suction header voided.

A conservative analysis (without consideration of steam generator secondary side inventory that existed during the event) showed that, without some form of decay heat removal, pressure in the RCS could exceed the RHR pump shutoff head within as little as 15 min. This is less than the time that would likely be required to restore the RHR system to service. As the power-operated relief valves (PORVs) were found to be inoperable subsequent to this event, it was assumed that depressurization of the RCS would have been difficult to achieve. The RHR pumps were, therefore, assumed to be inoperable once the RWST ECCS suction header voided. The only remaining decay-heat removal path would be reflux cooling via the steam generators (SGs). The SGs were available during the event, and reflux cooling was considered a viable core cooling method. In the short term, the water inventory in the SG would provide decay heat removal. Eventually, SG makeup and the opening of atmospheric vent valves would be required for continued heat removal via this method. Reflux cooling requires two SGs for success. Assuming both motor-driven auxiliary feedwater pumps and all four steam generators and their atmospheric dump valves are available, a failure probability of ~ 7.0×10^{-4} is estimated for reflux cooling based on component failure probabilities used in the IRRAS-based ASP models for Wolf Creek. It should be noted that this estimate addresses equipment availability only and not the uncertainty in the viability of the reflux cooling method. Since consideration of such uncertainty is beyond the scope of this analysis, the potential impact of reflux cooling being unavailable or ineffective was addressed in a sensitivity analysis.

The probability of core damage for this event is 3.0×10^{-3}. This estimate is probably conservative in that it assumes all ECCS pumps are unavailable once significant voiding occurs in the ECCS common suction header. Assumptions concerning the viability of reflux cooling play an important role in the core damage probability estimated for this event. For example, an assumed failure probability of ~0.05 for reflux cooling raises the estimated core damage probability by a factor of 2, to 6.0×10^{-3}.

3.2.2 Haddam Neck, Power-Operated Relief Valves and Vital 480-V ac Bus Degraded

During testing on February 16, 1994, it was discovered that one of two feed breakers to motor control center-5 (MCC-5) could jam and fail to close when demanded. MCC-5 supplies power to a number of vital components in both safety system trains. During testing on February 19, 1994, it was discovered that air operators for the pressurizer PORVs were experiencing control air leaks and that the PORVs could not be operated properly from their safety-grade control air supply. Investigation revealed that repairs to fix a prior PORV failure were made incorrectly during the previous refueling outage. The PORV diaphragms were not seated correctly and were coated with a lubricant rather than a required sealant. A substantial air leak resulted, and the PORVs could not be opened more than 50%. The combined conditional core damage probability estimated for these events is 1.4×10^{-4}.

Surveillance testing of the PORVs in May 1993 identified that one valve was experiencing leakage from its diaphragm assembly. This leak, in conjunction with failure of the associated air pressure regulator, resulted in excessive air consumption. Had the system been demanded, operator action to isolate the leaking PORV would have been required to ensure an adequate long-term supply of control air to the other PORV. Repairs to the system, including replacement of the PORV diaphragms, were completed prior to the end of the 1993 refueling outage.

The design of the new diaphragms varied somewhat from the original ones, which may have contributed to the difficulties experienced during the replacement process. Errors were made during the replacement, including the use of a lubricant instead of a sealant around the diaphragm's bolt circle. This allowed the diaphragm to extrude out between the sections of its housing, creating a pathway for air leakage. An NRC inspection team report related to this event indicates that both valves could only be opened about 50% during testing. The LER for the event indicates that two safety functions were potentially compromised by the PORV failures: feed-and-bleed cooling and high-pressure safety injection (HPSI) makeup during certain small-break LOCAs.

The HPSI pumps at Haddam Neck do not develop sufficient discharge head to force adequate flow for feed-and-bleed cooling through the pressurizer safety valves. Accordingly, the operators must be able to open a PORV for feed-and-bleed cooling to succeed. Air is supplied to the PORVs from the containment air compressors. The containment air compressors, which are located within the containment building, are not rated for the environmental conditions that could occur during feed-and-bleed cooling, and the compressors could be expected to fail under such conditions. The PORVs are also provided with safety-related control air accumulators that maintain a reserve supply of control air in the event of compressor failure, but these accumulators were inadequate to operate the PORVs during the time that the air-operator diaphragms were damaged. As a result of their incorrect installation, the PORV air-operator diaphragms were damaged and subject to leakage from some unknown time after they were replaced during the 1993 refueling outage until the condition was discovered on February 19, 1994.

During a period of time overlapping the PORV unavailability, the automatic bus transfer (ABT) circuit for MCC-5 failed when tested. At the time of the event, MCC-5 supplied many pieces of important equipment in both trains, including equipment that would have been required for successful operation of HPSI, low-pressure safety injection (LPSI), recirculation, long-term cooling, containment spray, reactor coolant (RC) system loop isolation, one PORV block valve, emergency boration, feedwater isolation, RC pump seal cooling, service water, control air, and the closed cooling water system. Subsequent to this event, modifications were made to reduce the dependency upon MCC-5.

MCC-5 can be supplied from either 480-V ac bus 5 (emergency train A) or bus 6 (emergency train B). Normally, it is aligned such that bus 5 is the preferred supply, and bus 6 is the alternate supply. At the time of the event, if the preferred supply was lost, an ABT system aligned MCC-5 to the alternate bus. If power was restored to the preferred bus, the ABT would realign back to the preferred bus. During a test of the ABT system, bus 5 was deenergized. As designed, the breaker supplying MCC-5 from bus 5 opened, and the supply breaker from bus 6 automatically closed to restore power. When bus 5 was reenergized, MCC-5 automatically realigned itself to bus 5. During the second part of the test, the preferred power source selector switch (PPSSS) for the ABT is moved to make bus 6 the preferred power supply and bus 5 the alternate. When the PPSSS was moved to the bus 6 position, the bus 5 supply breaker opened as expected but the bus 6 supply breaker failed to automatically close, deenergizing MCC-5.

Subsequent investigation revealed that a mechanical defect in the MCC-5 feeder breaker from bus 6 prevented it from closing. This mechanical defect caused the breaker to randomly fail. With bus 6 still energized and selected as the preferred power source to MCC-5, the bus 5 supply to MCC-5 was prevented from closing by the ABT system logic.

The event was modeled as an unavailability of the PORVs for feed-and-bleed cooling and the bus 6 feeder breaker for MCC-5. The last successful operation of the PORVs was during an outage in May and June of 1993 following installation of the new diaphragms. The likely cause of the PORV failure was incorrect installation of the air-operator diaphragms during the 1993 outage. It was, therefore, assumed that the PORVs were inoperable for feed-and-bleed cooling from July 1993 until the leakage was discovered on February 19, 1994.

The defect that led to the intermittent failure of the bus 6 feeder breaker was presumed to have existed from the time of the previous failure during the June 1993 refueling outage until the time of this event in February 1994. The interval analyzed was the period from July 21, 1993, until February 19, 1994; a period of 234 days (4728 h).

The analysis of this event is similar to the analysis of LER 213/93-007 and AIT Report 213/93-80 provided in the 1993 ASP Program Annual Report (NUREG /CR-4674, ORNL/NOAC-232, Vols. 19 and 20). That analysis also dealt with failures of PORV control air system components coincident with inoperability of the MCC-5 ABT.

The conditional core damage probability estimated for the combined event is 1.4×10^{-4}. Postulated LOOPs contribute approximately 78% of the core damage probability. The dominant sequence, which contributes about 30% of the total involves a postulated LOOP, emergency power success, recovery of ac power and MCC-5, and failure of AFW and feed-and-bleed cooling.

3.3 Number of Precursors Identified

Nine precursors [p(core damage) $\geq 10^{-6}$] affecting 11 units were identified in 1994. The distribution of precursors as a function of conditional probability is shown in Table 3.7. The distribution of 1988-1993 precursors is also shown for comparison purposes.

Table 3.7. Number of precursors by year

Year	$10^{-3} \leq p(cd) < 1$	$10^{-4} \leq p(cd) < 10^{-3}$	$10^{-5} \leq p(cd) < 10^{-4}$	$10^{-6} \leq p(cd) < 10^{-5}$	Total number of precursors
1988	0	7	14	11	32
1989	0	7	11	12	30
1990	0	6	11	11	28
1991	1	12	8	6	27
1992	0	7	7	13	27
1993	0	4	7	5	16
1994	1	1	4	3	9

As described previously, differences in the ASP models and the analysis methods from year to year preclude a direct comparison between the number of events identified for different calendar years. In particular, the conditional core damage probabilities estimated for the 1992 through 1994 events are lower for equivalent events in earlier years because supplemental and plant-specific mitigating systems beyond those included in the ASP models were incorporated into the analyses. In addition, new modeling techniques were adopted for the analysis of the 1994 events.

3.4 Insights

A review of the analyses for all nine precursors for 1994 revealed the following trends across the different analyses.

1. As can be seen in Tables 3.4 through 3.6, five of the six events with p(cd) greater than 10^{-5} are pressurized-water reactor (PWR) events. For all 1994 precursors, six were associated with PWRs and three with boiling-water reactors (BWRs).
2. Only two events involved at-power initiators. Six events involved at-power unavailabilities. The number of at-power unavailabilities decreased from eight in 1993 to six in 1994. The number of at-power initiators decreased from eight in 1993 to two in 1994.
3. Five of the precursors associated with at-power unavailabilities involved the degradation or unavailability of electrical equipment: (1) the degradation of the bus transfer scheme for MCC-5 at Haddam Neck, (2) the degradation of the emergency load sequencers at Turkey Point Units 3 and 4, (3) improper breaker settings for a motor control center at Dresden Unit 2, (4) both emergency diesel generators (EDGs) inoperable at Point Beach Units 1 and 2 (one removed from service for maintenance, the other had a failed electrical fuel pump and exciter), and (5) Zebra Mussel shells were found in the lube oil and jacket water coolers for one of the EDGs at Zion Unit 2.

Table 3.8. Number of precursors by event type

Event category	$\geq 10^{-3}$	$10^{-4} \leq p(cd) < 10^{-3}$	$10^{-5} \leq p(cd) < 10^{-4}$	$10^{-6} \leq p(cd) < 10^{-5}$	Total
At-power unavailabilities	0	1	2	3	6
At-power initiators	0	0	2	0	2
Shutdown initiators	1	0	0	0	1

4. Four of the six precursors associated with unavailabilities occurred at PWRs. One of the precursors associated with the initiating events occurred at a BWR and the other occurred at a PWR.

5. Six of the nine events (67%) occurred at multiunit sites. This is about the same as the percentage of units at multiunit sites (71%). Two of the precursor events affected both units at a dual-unit site.

A review of the ASP reports for 1990–1994 indicates the following trends.

1. Long-term unavailabilities and LOOP initiators typically dominate the events with the highest conditional core damage probabilities.

2. The events with the highest conditional core damage probabilities are dominated by PWRs.

3. The number of precursors identified for 1994 is lower than for previous years. This decrease is due in part to the differences in the ASP models for 1994. In addition, the conditional core damage probabilities estimated for the 1994 events are lower than equivalent events in earlier years because of consideration of supplemental and plant-specific mitigating systems beyond those modeled in the ASP models. A number of events that would have met the precursor criteria for prior years were rejected on low probability following the incorporation of additional mitigating systems in the models.

4. Glossary

Accident. An unexpected event (frequently caused by equipment failure or some misoperation as the result of human error) that has undesirable consequences.

Accident sequence precursor. A historically observed element or condition in a postulated sequence of events leading to some undesirable consequence. For purposes of the ASP Program, the undesirable consequence is usually severe core damage. The identification of an operational event as an accident sequence precursor does not of itself imply that a significant potential for severe core damage existed. It does mean that at least one of a series of protective features designed to prevent core damage was compromised. The likelihood of severe core damage, given the occurrence of an accident sequence precursor, depends on the effectiveness of the remaining protective features and, in the case of precursors that do not include initiating events, the probability of such an initiator.

Availability. The characteristic of an item expressed by the probability that it will be operational on demand or at a randomly selected future instant in time. Availability is the complement of unavailability.

Common-cause failures. Multiple failures attributable to a common cause.

Common-mode failures. Multiple, concurrent, and dependent failures of identical equipment that fails in the same mode.

Components. Items from which equipment trains and/or systems are assembled (e.g., pumps, pipes, valves, and vessels).

Conditional probability. The probability of an outcome given certain conditions.

Core damage. See *Severe core damage.*

Core-melt accident. An event in a nuclear power plant in which core materials melt.

Degraded system. A system with failed components that still meets minimum operability standards.

Demand. A test or an operating condition that requires the availability of a component or a system. In this study, a demand includes actuations required during testing and because of initiating events. One demand is assumed to consist of the actuation of all redundant components in a system, even if these were actuated sequentially (as is typical in testing multiple-train systems).

Dependent failure. A failure in which the likelihood of failure is influenced by the failure of other items. Common-cause failures and common-mode failures are two types of dependent failures.

Dominant sequence. The sequence in a set of sequences that has the highest probability of leading to a common end state.

Emergency-core-cooling systems. Systems that provide for removal of heat from a reactor following either a loss of normal heat removal capability or a loss-of-coolant accident.

Engineered safety features. Equipment and/or systems (other than reactor trip or those used only for normal operation) designed to prevent, limit, or mitigate the release of radioactive material.

Event. An abnormal occurrence that is typically in violation of a plant's Technical Specifications.

Event sequence. A particular path on an event tree.

Event tree. A logic model that represents existing dependencies and combinations of actions required to achieve defined end states following an initiating event.

Failure. The inability to perfo:m a required function. In this study, a failure was considered to have occurred if some component or system performed at a level below its required minimum performance level without human intervention. The likelihood of recovery was accounted for through the use of recovery factors. See *Nonrecovery factor*.

Failure probability. The long-term frequency of occurrence of failures of a component, system, or combination of systems to operate at a specified performance level when required. In this study, failure includes both failure to start and failure to operate once started.

Failure rate. The expected number of failures of a given type, per item, in a given time interval (e.g., capacitor short-circuit failures per million capacitor hours).

Fault tree. A logic model that represents the combinations of events that can lead to system failure. Typcially, fault trees consist of basic hardware-related events and operator actions linked with logic gates to define sets of events that result in failure of the system.

Front-line system. A system that directly provides a mitigative function included on the event trees used to model sequences to an undesired end state, in contrast to a support system, which is required for operability of other systems.

Immediately detectable. A term used to describe a failure resulting in a plant response that is apparent at the time of the failure.

Independence. A condition existing when two or more entities do not exhibit a common failure mode for a particular type of event.

Initial criticality. The date on which a plant goes critical for the first time in first-cycle operation.

Initiating event. An event that starts a transient response in the operating plant systems. In the ASP Program, the concern is only with those initiating events that could lead to severe core damage.

Licensee Event Reports (LERs). Those reports submitted to the Nuclear Regulatory Commission (NRC) by the utilities that operate nuclear plants as required by 10CFR50.72. Guidance on complying with these requirements is contained in NUREG-1022. LERs describe abnormal operating occurrences that generally involve violation of the plant's Technical Specifications.

Multiple failure events. Events in which more than one failure occurs. These may involve independent or dependent failures.

Operational event. An event that occurs in a plant and generally constitutes a reportable occurrence under NUREG-1022 as an LER.

Postulated event. An event that may happen at some time in the course of a plant's operation.

Potential severe core damage. A plant operating condition in which, following an initiating event, one or more protective functions fail to meet minimum operability requirements over a period sufficiently long that core damage could occur. This condition has been called in other studies "core melt," "core damage," and "severe core damage," even though actual core damage may not result unless further degradation of mitigation functions occurs.

Precursor. See *Accident sequence precursor*.

Reactor years. The accumulated total number of years of reactor operation. For the ASP Program, operating time starts when a reactor goes critical, ends when it is permanently shut down, and includes all intervening outages and plant shutdowns.

Recovery factor (recovery class). A measure of the likelihood of not recovering from a failure. Failures were assigned to a particular recovery class based on an assessment of likelihood that recovery would not be affected, given event specifics. Considered in the likelihood of recovery was whether such recovery would be required in a moderate- to high-stress situation following a postulated initiating event.

Redundant equipment or system. A system or some equipment that duplicates the essential function of another system or other equipment to the extent that either may perform the required function regardless of the state of operation or failure of the other.

Reliability. The characteristic of an item expressed by the probability that it will perform a required function under stated conditions for a stated period of time.

Risk. A measure of the frequency and severity of undesired effects.

Sensitivity analysis. An analysis that determines the variation of a given function caused by changes in one or more parameters about a selected reference value.

Severe core damage. The result of an event in which inadequate core cooling was provided, resulting in damage to the reactor core. See *Potential severe core damage.*

Technical Specifications. A set of safety-related limits on process variables, control system settings, safety system settings, and the performance levels of equipment that are included as conditions of an operating license .

Unavailability. The probability that an item or system will not be operational at a future instant in time. Unavailability may be a result of the item being tested or may occur as a result of malfunctions. Unavailability is the complement of availability.

Unit. A nuclear steam supply system, its associated turbine generator, auxiliaries, and engineered safety features.

5. References

1. J. W. Minarick and C. A. Kukielka, Union Carbide Corp., Nuclear Div., Oak Ridge Natl. Lab., and Science Applications, Inc., *Precursors to Potential Severe Core Damage Accidents: 1969-1979, A Status Report*, USNRC Report NUREG/CR-2497 Vols. 1 and 2 (ORNL/NSIC-18/V1 and V2), June 1982.*

2. W. B. Cottrell et al., Martin Marietta Energy Systems, Inc., Oak Ridge Natl. Lab., and Science Applications International Corp., *Precursors to Potential Severe Core Damage Accidents: 1980-81, A Status Report*, USNRC Report NUREG/CR-3591, Vols. 1 and 2 (ORNL/NSIC-217/V1 and V2), July 1984.*

3. J. W. Minarick et al., Martin Marietta Energy Systems, Inc., Oak Ridge Natl. Lab., Science Applications International Corp., and Professional Analysis, Inc., *Precursors to Potential Severe Core Damage Accidents: 1985, A Status Report*, USNRC Report NUREG/CR-4674 (ORNL/NOAC-232), Vols. 1 and 2, December 1986.*

4. J. W. Minarick et al., Martin Marietta Energy Systems, Inc., Oak Ridge Natl. Lab., Science Applications International Corp., and Professional Analysis, Inc., *Precursors to Potential Severe Core Damage Accidents: 1984, A Status Report*, USNRC Report NUREG/CR-4674 (ORNL/NOAC-232), Vols. 3 and 4, May 1987.*

5. J. W. Minarick et al., Martin Marietta Energy Systems, Inc., Oak Ridge Natl. Lab., Science Applications International Corp., and Professional Analysis, Inc., *Precursors to Potential Severe Core Damage Accidents: 1986, A Status Report*, USNRC Report NUREG/CR-4674 (ORNL/NOAC-232), Vols. 5 and 6, May 1988.*

6. J. W. Minarick et al., Martin Marietta Energy Systems, Inc., Oak Ridge Natl. Lab., Science Applications International Corp., and Professional Analysis, Inc., *Precursors to Potential Severe Core Damage Accidents: 1987, A Status Report*, USNRC Report NUREG/CR-4674 (ORNL/NOAC-232), Vols. 7 and 8, July 1989.*

7. J. W. Minarick et al., Martin Marietta Energy Systems, Inc., Oak Ridge Natl. Lab., Science Applications International Corp., and Professional Analysis, Inc., *Precursors to Potential Severe Core Damage Accidents: 1988, A Status Report*, USNRC Report NUREG/CR-4674 (ORNL/NOAC-232), Vols. 9 and 10, February 1990.*

8. J. W. Minarick et al., Martin Marietta Energy Systems, Inc., Oak Ridge Natl. Lab., Science Applications International Corp., and Professional Analysis, Inc., *Precursors to Potential Severe Core Damage Accidents: 1989, A Status Report*, USNRC Report NUREG/CR-4674 (ORNL/NOAC-232), Vols. 11 and 12, August 1990.*

9. J. W. Minarick et al., Martin Marietta Energy Systems, Inc., Oak Ridge Natl. Lab., Science Applications International Corp., and Professional Analysis, Inc., *Precursors to Potential Severe Core Damage Accidents: 1990, A Status Report*, USNRC Report NUREG/CR-4674 (ORNL/NOAC-232), Vols. 13 and 14, August 1991.*

10. J. W. Minarick et al., Martin Marietta Energy Systems, Inc., Oak Ridge Natl. Lab., and Science Applications International Corp., *Precursors to Potential Severe Core Damage Accidents: 1991, A Status Report*, USNRC Report NUREG/CR-4674 (ORNL/NOAC-232), Vols. 15 and 16, September 1992.*

11. D. A. Copinger et al., Martin Marietta Energy Systems, Inc., Oak Ridge Natl. Lab., and Science Applications International Corp., *Precursors to Potential Severe Core Damage Accidents: 1992, A Status Report*, USNRC Report NUREG/CR-4674 (ORNL/NOAC-232), Vols. 17 and 18, December 1993.*

12. L. N. Vanden Heuvel et al., Martin Marietta Energy Systems, Inc., Oak Ridge Natl. Lab., and Science Applications International Corp., *Precursors to Potential Severe Core Damage Accidents: 1993, A Status Report*, USNRC Report NUREG/CR-4674 (ORNL/NOAC-232), Vols. 19 and 20, September 1994.*

13. U.S. Nuclear Regulatory Commission, *Licensee Event Report System, Description of System and Guidelines for Reporting*, USNRC Report NUREG-1022, September 1983.*

14. U.S. Nuclear Regulatory Commission, *Licensee Event Report System, Description of System and Guidelines for Reporting*, USNRC Report NUREG-1022, Supplement 1, February 1984.*

15. U.S. Nuclear Regulatory Commission, *Licensee Event Report System, Evaluation of First Year Resvlts, and Recommendations for Improvements*, USNRC Report NUREG-1022, Supplement 2, September 1985.*

16. U.S. Nuclear Regulatory Commission, *Risk Assessment Review Group Report*, USNRC Report NUREG/CR-0400, September 1978.*

17. U.S. Nuclear Regulatory Commission, *Reactor Safety Study: An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants*, USNRC Report WASH-1400 (NUREG-75/014), October 1975.*

* Available for purchase from National Technical Information Service, Springfield, Virginia 22161.

Appendix A:

ASP Calculational Methodology

A.1 Introduction

This appendix describes the approach used in the Accident Sequence Precursor (ASP) Program to estimate the significance of an operational event. The process used to screen the operational event data base for potential precursors and the characteristics of events ultimately selected as precursors are described in Chapter 2 of this report.

The ASP Program performs retrospective analyses of operating experience. These analyses require that certain methodological assumptions be made to estimate the risk significance of an event. If one assumes, following an operational event in which core cooling was successful, that components observed failed were "failed" with probability 1.0, and components that functioned successfully were "successful" with probability 1.0, then one can conclude that the risk of core damage was zero and that the only potential sequence was the combination of events that occurred. To avoid such trivial results, the status of certain components must be considered latent. In the ASP Program, this latency is associated with components that operated successfully—these components are considered to have been capable of failing during the operational event.

Quantification of precursor significance involves the determination of a conditional probability of subsequent severe core damage given the failures and other undesirable conditions (such as an initiating event or an unexpected relief valve challenge) observed during an operational event. The effect of a precursor on basic events in the core damage models is assessed by reviewing the operational event specifics against plant design and operating information, and translating the results of the review into a revised model for the plant that reflects the observed failures. The precursor's significance is estimated by calculating a conditional probability of core damage given the observed failures. The conditional probability calculated in this way is useful in ranking because it provides an estimate of the measure of protection against core damage remaining once the observed failures have occurred.

The accident sequence models used to estimate the significance of 1994 precursors consist of fault-tree models that depict the logical combination of component failures (basic events) that would result in failure of each system that provides protection against core damage. The fault trees are linked together in a logical structure based on event trees that describe potential combinations of system successes and failures that would result in core damage following postulated initiating events. The resulting Boolean equations, when reduced to their simplest form, consist of a series of combinations of basic events (cut sets), any of which would result in core damage if all of the basic events in the cut set occurred. A detailed description of the use of linked fault trees in probabilistic risk assessment (PRA) analysis is included in Reference 1. The current ASP models are described in Appendix B. These models are constructed and solved using the SAPHIRE suite of PRA software.[2]

A.2 Types of Events Analyzed

Two different types of events are addressed in precursor quantitative analysis. In the first, an initiating event such as a loss-of-offsite power (LOOP) or small-break loss-of-coolant accident (LOCA) occurs as a part of the precursor. The probability of core damage for this type of event is calculated based on the required plant response to the particular initiating event and other failures that may have occurred at the same time. The assessment of an observed initiating event is referred to as an Initiating Event Assessment.

The second type of event involves a failure condition that existed over a period of time during which an initiating event could have, but did not, occur. The probability of core damage is calculated based on the required plant response to a set of postulated initiating events, considering the failures that were observed. Unlike an initiating event assessment, where the analysis uses a probability of 1.0 to account for the given failure in the sequence cut set equations, each initiating event is assumed to occur with a probability based on the initiating event frequency and the failure duration. The assessment of failed equipment over a period of time is referred to as a Condition Assessment.

A.3 Modification of Basic Event Probabilities to Reflect Observed Failures

The ASP models describe sequences to core damage in terms of combinations of basic events (cut sets). Each basic event represents the failure of a particular component or group of components in a system at a plant, an occurrence such as a relief valve lift, or an operator action. Failures observed during an operational event must be represented in a model in terms of changes to one or more of the basic events.

If a failed component is included as a basic event in a model, the failure is reflected by setting its basic event probability to 1.0 (failed). In actuality, such a basic event must be set to the logical state "true" if a new minimum set of cut sets reflecting the conditional state of the plant is to be generated.*

In addition to revising the basic events associated with failed components, basic events related to the common-cause failure (CCF) of similar components may also have to be revised to reflect the observed failures. In addition to revising the status of basic events for failed components (to failed), the failure probabilities of basic events that represent CCFs associated with the failed components may also need revision. In particular, if the failure could have occurred in similar components during the same time interval, the failure probability of the CCF basic event will be changed to reflect this situation. If the failure could not simultaneously occur in the other components (for example, if a component was removed from service for preventive maintenance), then the CCF probability is also revised, but only to reflect "removal" of the unavailable component from the CCF model. The Multiple Greek Letter (MGL) method is used to quantify the common cause basic events (see Reference 3 for a description of the MGL model).

If a failed component is not specifically included as a basic event in a model, then the failure is addressed by appropriately modifying the basic events impacted by the failure. For example, support systems are not completely developed in the current ASP models. A breaker failure that results in the loss of power to a group of components would be represented by setting the basic events for each component in the group to "true."

Occasionally, a precursor occurs that cannot be modeled by modifying existing basic event probabilities. In such a case, the model is revised as necessary to address the event, typically by adding basic events to a fault tree or by addressing an unusual initiating event through the use of an additional event tree.

A.4 Recovery from Observed Failures

If recovery of a system is dominated by operator response time, and if information concerning the time available for recovery is provided in the event report, then the probability of failing to recover from the failure is estimated using a Time-Reliability Correlation (TRC) model. The available time to respond, the underlying type of response (rule- or knowledge-based), and whether unusual conflict or burden would exist in response to an actual initiating event are addressed when developing an estimate of the operator (crew) error probability. The basic model structure is described in Reference 4. The probability of operator error is described using a log normal distribution with the following parameters:

Type of action	Median	Error factor
Rule-based, unburdened	2	3.2
Rule-based, burdened	2	6.4
Knowledge-based, unburdened	4	3.2
Knowledge-based, burdened	4	6.4

*Practical considerations in the solution of large linked fault trees, primarily the use of the DeleteTerm process to solve sequences involving system success, also require failed basic events to be represented as "true" if correct sequence probabilities are to be calculated.

For an available time t_{avail}, the probability of operator error is estimated as

$$1 - \Phi[(\ln t_{avail} - m)/\sigma]$$

where Φ is the normal distribution, $m = \ln(\text{median})$, and $\sigma = \ln(\text{error factor})/1.645$.

The potential for recovery from observed failures considers the time available and the nature of the failures. If information concerning response time is unavailable, then the likelihood of not recovering system failures is determined by assigning the failure to one of four broad recovery classes.

This is a carryover from the earlier event tree based ASP models (cut-set-based recovery may be added to the models in the future). In the current approach, the potential for recovery is addressed by assigning a recovery action to each system failure and initiating event. Four classes are currently used to describe the different types of recovery that could be involved:

Recovery class	Likelihood of nonrecovery	Recovery characteristic
R1	1.00	The failure did not appear to be recoverable in the required period, either from the control room or at the failed equipment.
R2	0.34	The failure appeared recoverable in the required period at the failed equipment, and the equipment was accessible; recovery from the control room did not appear possible.
R3	0.12	The failure appeared recoverable in the required period from the control room, but recovery was not routine or involved substantial operator burden.
R4	0.04	The failure appeared recoverable in the required period from the control room and was considered routine and procedurally based.

The assignment of an event to a recovery class is based on engineering judgment, which considers the specifics of each operational event and the likelihood of not recovering from the observed failure in a moderate- to high-stress situation following an initiating event.

It must be noted that the actual likelihood of failing to recover from an event at a particular plant is difficult to assess and may vary substantially from the va!ues listed. This difficulty is demonstrated in the genuine differences in opinion among analysts, operations and maintenance personnel, etc., concerning the likelihood of recovering specific failures (typically observed during testing) within a time period that would prevent core damage following an actual initiating event.

A.5 Conditional Probability Associated with Each Precursor

As described earlier in this appendix, the calculation process for each precursor involves a determination of initiators that must be modeled, plus any modifications to system probabilities necessitated by failures observed in an operational event. Once the basic event probabilities that reflect the conditions of the precursor are established, the sequences leading to core damage are calculated to estimate the conditional probability for the precursor. This calculational process is summarized in Table A.1, on page A.1-9.

Several simplified examples that illustrate the basics of the precursor calculational process follow. It is not the intent of the examples to describe a detailed precursor analysis, but instead to provide a basic understanding of the process. The examples are presented in terms of branch probabilities that are multiplied to calculate sequence probabilities. Readers familiar with the use of linked fault trees for PRA can readily extrapolate the process illustrated in the example calculations to analyses employing fault trees.

The hypothetical core damage model for these examples, shown in Figure A.1.1, consists of initiator I and four single-component systems that provide protection against core damage: systems A, B, C, and D. In Figure A.1.1, the up branch represents success and the down branch failure for each of the systems. (In an accident sequence model for a real reactor plant, the fault tree logic for each system could involve hundreds of components, and thousands of cut sets could be required to represent the basic event failure combinations that constitute the core damage sequences.) Three sequences result in core damage if completed: sequence 3 [I /A ("/" represents system success) C D], sequence 6 (I A /B C D), and sequence 7 (I A B). In a conventional PRA approach, the frequency of core damage would be calculated from the initiating event frequency of I, $\lambda(I)$ and the failure probabilities for A, B, C, and D [p(A), p(B), p(C), and p(D), respectively]. Assuming $\lambda(I) = 0.1\ \text{yr}^{-1}$ and $p(A \mid I) = 0.003$, $p(B \mid IA) = 0.01$, $p(C \mid I) = 0.05$, and $p(D \mid IC) = 0.1$[*], the frequency of core damage is determined by calculating the frequency of each of the three core damage sequences and adding the frequencies:

$$0.1\ \text{yr}^{-1} \times (1 - 0.003) \times 0.05 \times 0.1 \text{ (sequence 3)} +$$

$$0.1\ \text{yr}^{-1} \times 0.003 \times (1 - 0.01) \times 0.05 \times 0.1 \text{ (sequence 6)} +$$

$$0.1\ \text{yr}^{-1} \times 0.003 \times 0.01 \text{ (sequence 7)}$$

$$= 4.99 \times 10^{-4}\ \text{yr}^{-1} \text{ (sequence 3)} + 1.49 \times 10^{-6}\ \text{yr}^{-1} \text{ (sequence 6)} + 3.00 \times 10^{-6}\ \text{yr}^{-1} \text{ (sequence 7)}$$

$$= 5.03 \times 10^{-4}\ \text{yr}^{-1}.$$

In a nominal PRA, sequence 3 would be the dominant core damage sequence.

As described earlier, the ASP Program calculates a conditional probability of core damage, given an initiating event or component failures. This probability is different than the frequency calculated above and cannot be directly compared with it.

[*] The notation p(B | IA) means the probability that B fails, given I occurred and A failed.

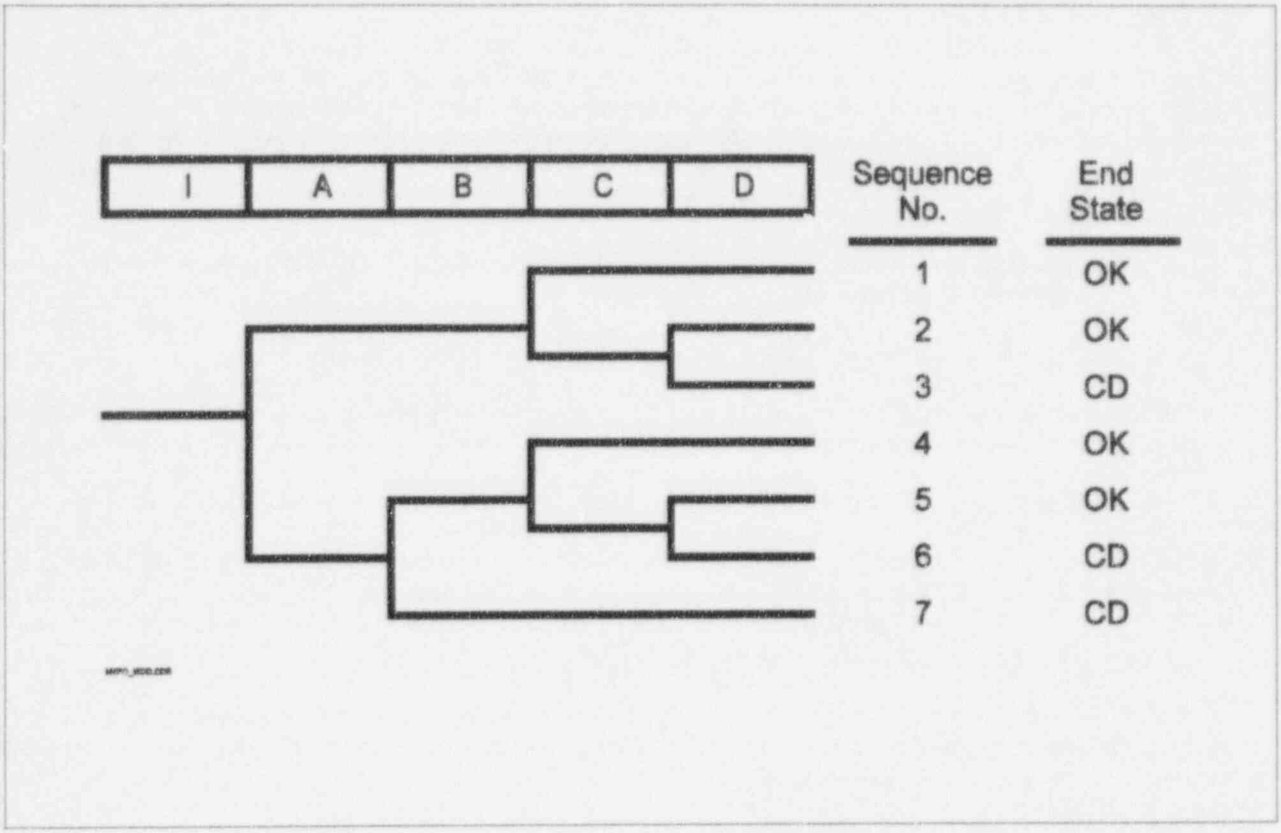


Figure A.1.1. Hypothetical core damage model.

A.5.1 Example 1: Initiating Event Assessment

Assume that a precursor involving initiating event I occurs. In response to I, systems A, B, and C start and operate correctly, and system D is not demanded. In a precursor initiating event assessment, the probability of I is set to 1.0. Although systems A, B, and C were successful, nominal failure probabilities are assumed. Since system D was not demanded, a nominal failure probability is assumed for it as well. The conditional probability of core damage associated with precursor I is calculated by summing the conditional probabilities for the three sequences:

$$1.0 \times (1 - 0.003) \times 0.05 \times 0.1 \text{ (sequence 3)} +$$

$$1.0 \times 0.003 \times (1 - 0.01) \times 0.05 \times 0.1 \text{ (sequence 6)} +$$

$$1.0 \times 0.003 \times 0.01 \text{ (sequence 7)}$$

$$= 5.03 \times 10^{-3}.$$

If, instead, B had failed when demanded following I, its probability would have been set to 1.0. The conditional core damage probability for precursor IB would be calculated as

$$1.0 \times (1 - 0.003) \times 0.05 \times 0.1 \text{ (sequence 3)} + 1.0 \times 0.003 \times 1.0 = 7.99 \times 10^{-3}.$$

Since B is failed, sequence 6 cannot occur.

A.5.2 Example 2: Condition Assessment

Assume that during a monthly test, system B is found to be failed, and that the failure could have occurred at any time during the month. The best estimate for the duration of the failure is one-half of the test period, or 360 h. To estimate the probability of initiating event I during the 360-h period, the yearly frequency of I must be converted to an hourly rate. If I can only occur at power, and the plant is at power for 70% of a year, then the frequency for I is estimated to be 0.1/yr/(8760 h/yr × 0.7) = 1.63×10^{-5} h^{-1}.

If, as in Example 1, B is always demanded following I, the probability of I in the 360-h period is the probability that at least one I occurs (since the failure of B will then be discovered), or

$$1 - e^{-\lambda(I) \times \text{failure duration}} = 1 - e^{-1.63E\text{-}5 \times 360} = 5.85 \times 10^{-3} .$$

Using this value for the probability of I, and setting p(B) = 1.0, the conditional probability of core damage for precursor B is calculated by again summing the conditional probabilities for the core damage sequences in Figure A.1.1:

$$5.85 \times 10^{-3} \times (1 - 0.003) \times 0.05 \times 0.1 \text{ (sequence 3)} + 5.85 \times 10^{-3} \times 0.003 \times 1.0 = 4.67 \times 10^{-5} .$$

As before, since B is failed, sequence 6 cannot occur. The conditional probability is the probability of core damage in the 360-h period, given the failure of B. Note that the dominant core damage sequence is sequence 3, with a conditional probability of 2.92×10^{-5}. This sequence is unrelated to the failure of B. The potential failure of systems C and D over the 360-h period still drive the core damage risk.

To understand the significance of the failure of system B, another calculation, an importance measure, is required. The importance measure that is used is equivalent to risk achievement worth on an interval scale.[5] In this calculation, the increase in core damage probability over the 360-h period due to the failure of B is estimated: p(cd | B) - p(cd). In this example, the value is $4.67 \times 10^{-5} - 2.94 \times 10^{-5} = 1.73 \times 10^{-5}$, where the second term on the left side of the equation is calculated using the previously developed probability of I in the 360-h period and nominal failure probabilities for A, B, C, and D.

The importance measure for unavailabilities (condition assessments) like this event was referred to as the conditional core damage probability in earlier annual precursor reports. For most conditions identified as precursors in the ASP Program, its value and the conditional core damage probability are numerically close, and the conditional core damage probability can be used as a significance measure for the precursor. However, for some events—typically those in which the components that are failed are not the primary mitigating plant features—the conditional core damage probability can be significantly higher than the importance (i.e., LER 250/94-005). In such cases, it is important to note that the potential failure of other components, unrelated to the precursor, are still dominating the plant risk (i.e., the impact of the precursor on plant risk is not substantial). Condition assessments documented in this report include both an estimate of the conditional core damage probability and the importance of the event.

A.5.3 References

1. *PRA Procedures Guide,* NUREG/CR-2300, January 1983, Section 6.3.2.
2. *Systems Analysis Programs for Hands-on Integrated Reliability Evaluations (SAPHIRE) Version 5.0,* NUREG/CR-6116, Vols. 1–10.
3. *Procedures for Treating Common Cause Failures in Safety and Reliability Studies*, NUREG/CR-4780, January 1989, Appendix C.
4. E. M. Dougherty and J. R. Fragola, *Human Reliability Analysis,* John Wiley and Sons, New York, 1988.
5. W. E. Vesely, T. C. Davis, R. S. Denning, and N. Saltos, *Measures of Risk Importance and Their Applications*, NUREG/CR-3385, July 1983.

Table A.1. Rules for Precursor Calculation

Event sequences requiring calculation. If an initiating event occurs as part of a precursor (i.e., the precursor consists of an initiating event plus possible additional failures), then use the accident sequence model associated with the initiator; otherwise, use all accident sequence models impacted by the observed unavailability.
Initiating event probability. If an initiating event occurs as part of the precursor, then the initiating event probability used in the calculation is 1.0. If an initiating event does not occur as part of the precursor, then the probability used for the initiating event is developed assuming a constant hazard rate. Event durations (the period of time during which the failure existed) are based on information included in the event report, if provided. If the event is discovered during testing, then one-half of the test period (15 d for a 30-d test interval) is typically assumed, unless a specific failure duration is identified.
Component failure probability estimation. For components that are observed failed during the precursor, the associated basic event is set to "true." Associated common-cause basic events are revised to reflect the type of failure that occurred. For components that are observed to operate successfully, or are not challenged during the event, a failure probability equal to the nominal component failure probability is utilized.
Nonrecovery probability. If an initiating event or a total system failure occurred as a part of the precursor, the basic event representing the probability of not recovering from the failure is revised to reflect the potential for recovery of the specific failures observed during the event. For condition assessments, the probability of nonrecovery is estimated under the assumption that an initiating event has occurred.
Failures in Support Systems. If the support system is not included in the ASP models, the impact of the failure is addressed by setting impacted components to failed. The modeling of a support system failure recognizes that as long as the failure remains unrecovered, all impacted components are unavailable; but if the support system failure is recovered, all impacted components are also recovered. This can be modeled through multiple calculations which address the impact of failure and success of the failed component. Calculated core damage probabilities for associated cut sets for each case are normalized based on the likelihood of not recovering the support system failure. (Support systems, except for emergency power, are not modeled in the current ASP models.)

Appendix B:

ASP Models

B.1 Introduction

This appendix describes the models used to estimate the significance of 1994 precursors. These models include important changes from those previously used in the Accident Sequence Precursor (ASP) Program—linked supercomponent-based fault trees are utilized, additional systems capable of providing protection against core damage are addressed, and sequences associated with steam generator tube ruptures (SGTR) [in pressurized water reactors (PWRs)] and anticipated transients without scram (ATWS) [both PWRs and boiling water reactors (BWRs)] are included in the base models.

B.2 Overview of ASP Event Tree and Fault Tree Models

Models used to rank the 1994 precursors by significance consist of system-based, plant-class event trees and plant-specific fault tree system models. These models describe mitigation sequences for the following initiating events: a nonspecific reactor trip [which includes loss of feedwater (LOFW) within the model], loss-of-offsite power (LOOP), small-break loss-of-coolant accident (LOCA), and SGTR (PWRs only). The models are developed using the SAPHIRE suite of probabilistic risk assessment (PRA) software (Ref. 1).

Plant classes were defined based on the use of similar systems in providing protective functions in response to transients, LOOPs, and small-break LOCAs. System designs and specific nomenclature may differ among plants included in a particular class; but functionally, they are similar in response. Plants where certain mitigating systems do not exist, but which are largely analogous in their initiator response, are grouped into the appropriate plant class. ASP plant categorization is described in the following section.

The event trees consider two end states: success (OK), in which core cooling exists, and core damage (CD), in which adequate core cooling is believed not to exist. In the ASP models, core damage is assumed to occur following core uncovery. It is acknowledged that clad and fuel damage will occur at later times, depending on the criteria used to define "damage," and that time may be available to recover core cooling once core uncovery occurs but before the onset of core damage. However, this potential recovery is not addressed in the models. Each event tree describes combinations of systems that will prevent core cooling—and makeup if required—in both the short and long term. Primary systems designed to provide these functions and alternate systems capable of also performing these functions are addressed. The event trees are described in Section B.4.

The fault trees used to model system failure are supercomponent-based and address those components such as pumps, motor-operated and manual valves, and check valves that must function for successful operation of the system. Common-cause failures of like components are addressed, as are operator actions required to start a system when no automatic actuation is expected and to recover a failed system. Additional information concerning the fault tree models is provided in Section B.7.

The system fault trees are combined (linked) based on the sequences included in each event tree. Conceptually, this involves describing the sequence in terms of a single fault tree "and" gate, with each branch of the sequence an input to the gate. For example, if a CD sequence involved the success of system A, failure of system B, success of system C, and failure of system D, it would be logically represented as SEQ = $/A \wedge B \wedge /C \wedge D$, where "/" implies success and "$\wedge$" is the logical "and" operator. A fault tree logic solver could then combine the logic from the fault trees for systems A-D and generate a set of component failure combinations (cut sets) that, if any occurred, would result in core damage.

This approach is often impractical, however, when success branches exist in a sequence. The requirement to logically invert fault trees to represent system success is computationally intensive, and many cut sets with component successes as well as failures are generated, making it difficult to understand the set of component failures that can lead to core damage. This problem can be avoided through the use of an approach often called DeleteTerm (see Ref. 2 for a description of this approach). Using this approach, only component failure combinations that will result in core damage are generated.

Changes made to models used to analyze 1994 precursors include the use of linked fault trees instead of the earlier event tree based models (the earlier models are described in Ref. 3). The use of linked fault trees allows the impact of individual component failures to be correctly addressed; this could only be approximated in the earlier models. The linked fault tree models will also allow the impact of support system failures to be easily addressed once support systems are added to the models. The new models also address additional systems that can provide core protection and initiating events not included in the earlier plant-class models. Response to a failure to trip the reactor is now included, as is a SGTR in PWRs. In PWRs, the potential use of the residual heat removal system following a small-break LOCA (to avoid sump recirculation) is addressed, as is long-term recovery of secondary side cooling following the initiation of feed and bleed. In BWRs, the potential use of venting for containment heat removal is addressed, as is the use of reactor core isolation cooling (RCIC) and the control rod drive (CRD) system for makeup if a single relief valve sticks open. The new models better reflect the capabilities of plant systems in preventing core damage and result in lower calculated conditional core damage probabilities for certain types of precursors.

B.3 Plant Categorization

It was recognized early in the ASP Program that plant designs were sufficiently different that multiple models would be required to correctly describe the impact of an operational event in different plants. In 1985, substantial effort was expended to develop a categorization scheme for all U.S. light water reactors (LWRs) that would permit grouping of plants with similar response to a transient or accident at the system or functional level and subsequently to develop eight sets of plant-class specific event tree models. Much of the categorization and early event sequence work was done at the University of Maryland.[4,5] The ASP Program has generally employed these categorizations; however, some modifications have been required to reflect more closely the specific needs of the precursor evaluations.

In developing the plant categorizations, each reactor plant was examined to determine the systems used to perform the following plant functions required in response to initiating events to prevent core damage: reactor subcriticality, reactor coolant system (RCS) integrity, reactor coolant inventory, short-term core heat removal, and long-term core heat removal.

Functions solely related to containment integrity (containment overpressure protection and containment heat removal) and post-accident activity removal are not included in the present ASP models (which only concern core damage sequences) and are not addressed in the categorization scheme.

For each plant, systems utilized to perform each function were identified. Plants were grouped based on the use of nominally identical systems to perform each function, that is, systems of the same type and function without accounting for the differences in the design of those systems.

Three BWR plant classes were defined. BWR Class A consists of the older plants, which are characterized by isolation condensers (ICs) and feedwater coolant injection (FWCI) systems that employ the main feedwater (MFW) pumps. BWR Class B consists of plants that have ICs but a separate high-pressure coolant injection (HPCI) system instead of FWCI. BWR Class C includes the modern plants that have neither ICs nor FWCI. However, they have an RCIC system that Classes A and B lack. The Class C plants could be separated into two subgroups: those plants with turbine-driven HPCI systems and those with motor-driven high-pressure core spray (HPCS) systems. This difference is addressed instead in the fault tree models of the different plant systems.

PWRs are separated into five classes. One class represents most Babcock & Wilcox Company plants (Class D). These plants have the capability of performing feed and bleed without the need to open the power-operated relief valve (PORV). Combustion Engineering plants are separated into two classes: those that provide feed and bleed capability (Class G) and those that provide for secondary-side depressurization and the use of the condensate system as an alternate core cooling method and for which no feed and bleed is available (Class H).*

* Maine Yankee Atomic Power Plant was built by Combustion Engineering but has a response to initiating events more akin to the Westinghouse Electric Corporation design, so it is grouped in a class with other Westinghouse plants. Davis-Besse Nuclear Power Station was also placed in a Westinghouse plant class because its high-pressure injection (HPI) system design requires the operator to open the PORV for feed and bleed, as in most Westinghouse plants. The requirement to open the PORV for feed and bleed is a primary difference between event trees for Westinghouse and Babcock and Wilcox plants. The requirement to open PORVs for feed and bleed is addressed in the feed and bleed fault tree in the current models. Because of this, the event trees for PWR Class D are similar to those for PWR Class B. Plant response differences resulting from the use of different steam generator designs are not addressed in the models.

The remaining two classes address Westinghouse plants—Class A is associated with plants that require the use of spray systems for core heat removal following a LOCA, and Class B is associated with plants that can utilize low-to-high pressure recirculation for core heat removal.

Table B.1 lists the plant class associated with each plant.

B.4 Event Tree Models

The plant class event trees describe core damage sequences for four initiating events: nonspecific reactor trip, LOOP, small-break LOCA, and SGTR (in PWRs only). A separate event tree describes ATWS sequences. Failure to trip sequences on the transient event tree are transferred to this tree. The event trees constructed are system-based and include an event tree applicable to each plant class defined. For operational events that cannot be described using existing models, unique models are developed to describe sequences to core damage.

This section (1) describes the potential plant response to the initiating events listed above, (2) identifies the combinations of systems required for the successful mitigation of each initiator, and (3) briefly describes the criteria for success of each system-based function. The sequences are considered first for PWRs and then separately for BWRs. PWR Class B event trees are described first, along with those for Class D, which are similar. The event trees for the combined group apply to the greatest number of operating PWRs and therefore are discussed first, followed by those for PWR Classes G, H, and then A. For the BWR event trees, the plant Class C models are described first, because these are applicable to the majority of the BWRs, followed by discussions for the Classes A and B BWRs, respectively.

The event trees are constructed with branch success as the upper branch and failure as the lower branch [unlike earlier ASP models, relief valve opening and the occurrence of a reactor coolant pump (RCP) seal LOCA are indicated by down branches in the current models]. Each sequence path is read from left to right, beginning with the initiator and followed by subsequent systems required to preclude or mitigate core damage. Each sequence represents a series of branch successes and failures required to reach the sequence end state (OK or CD). The sequence as depicted on the event tree represents the logical combination of successes and failures required to reach the end state; it does not necessarily represent the actual sequence in which systems and functions would respond to an initiating event. However, short-term plant response is generally presented earlier in the sequence than long-term plant response.

The event trees can be found following the discussion sections and are grouped according to plant classes, beginning with the PWR classes and followed by the BWR classes. The trees are presented in the order shown in the following list. The abbreviations used in the event tree models are defined in the event tree branch descriptions in this section.

Figure No.	Event tree
Figure B.1	PWR Class A nonspecific reactor trip
Figure B.2	PWR Class A loss-of-offsite power
Figure B.3	PWR Class A small-break loss-of-coolant accident
Figure B.4	PWR Class A steam generator tube rupture
Figure B.5	PWR Class A anticipated transient without scram
Figure B.6	Classes B and D nonspecific reactor trip
Figure B.7	Classes B and D loss-of-offsite power
Figure B.8	Classes B and D small-break loss-of-coolant accident
Figure B.9	Classes B and D steam generator tube rupture
Figure B.10	Classes B and D anticipated transient without scram
Figure B.11	PWR Class G nonspecific reactor trip
Figure B.12	PWR Class G loss-of-offsite power
Figure B.13	PWR Class G small-break loss-of-coolant accident
Figure B.14	PWR Class G steam generator tube rupture
Figure B.15	PWR Class G anticipated transient without scram
Figure B.16	PWR Class H nonspecific reactor trip
Figure B.17	PWR Class H loss-of-offsite power
Figure B.18	PWR Class H small-break loss-of-coolant accident
Figure B.19	PWR Class H steam generator tube rupture
Figure B.20	PWR Class H anticipated transient without scram
Figure B.21	BWR Class A nonspecific reactor trip
Figure B.22	BWR Class A loss-of-offsite power
Figure B.23	BWR Class A small-break loss-of-coolant accident
Figure B.24	BWR Class A anticipated transient without scram
Figures B.25–28	BWR Class B nonspecific reactor trip
Figures B.29–32	BWR Class B loss-of-offsite power
Figure B.33	BWR Class B small-break loss-of-coolant accident
Figure B.34	BWR Class B anticipated transient without scram
Figures B.35–36	BWR Class C nonspecific reactor trip
Figures B.37–38	BWR Class C loss-of-offsite power
Figure B.39	BWR Class C small-break loss-of-coolant accident
Figure B.40	BWR Class C anticipated transient without scram

B.5 PWR Event Tree Models

The PWR event trees describe the impact of the availability and unavailability of front-line systems in each plant class on core protection following four initiating events: reactor trip, LOOP, small-break LOCA, and SGTR. The systems modeled in the event trees are those associated with the generic functions required in response to an initiating event. The systems that are assumed capable of providing these functions are as follows:

Function	System
Reactor subcriticality	Reactor trip and boration (following ATWS)
Reactor coolant system integrity	Addressed in small-break LOCA, SGTR, and ATWS models plus trip and LOOP sequences involving failure of primary relief valves to close and RCP seal LOCA
Reactor coolant inventory	High-pressure injection (assumed required only following a LOCA)
Short-term core heat removal	Auxiliary feedwater
	Main feedwater
	Feed and bleed (high-pressure injection and PORV, PWR Classes A, B, D, and G)
	Secondary-side depressurization and use of condensate system (PWR Class H)
Long-term core heat removal	Auxiliary feedwater
	Main feedwater
	RCS cooldown and the use of the residual heat removal (RHR) system (following a LOCA with successful high pressure injection).
	High-pressure recirculation (PWR Classes B and D) (also required to support RCS inventory for all classes)
	Secondary-side depressurization and use of condensate system (PWR Class H)
	Containment spray recirculation (PWR Classes A and G)

B.5.1 PWR Nonspecific Reactor Trip

The PWR nonspecific reactor trip event tree constructed for plant Classes B and D is shown in Figure B.6. The event tree branch descriptions follow [event tree branch designations are shown in brackets].

1. Initiating event (transient) [IE-TRANS]. The initiating event for the tree is a transient or upset event that requires or is followed by a rapid shutdown of the plant. LOOP, small-break LOCA, and SGTR initiators are modeled in separate event trees. Medium- and large-break LOCA and steam-line break (SLB) initiators are not addressed in the models described here.

2. Reactor trip [RT]. To achieve reactor subcriticality and thus halt the fission process, the reactor protection system (RPS) is required to insert control rods into the core. If the automatically initiated RPS fails, a reactor trip may be initiated manually. Failure to trip results in ATWS response, described later.

3. Auxiliary feedwater [AFW]. AFW flow to the steam generators (SGs) must be provided following trip to remove the decay heat still being generated in the reactor core. Successful AFW operation requires flow from one or more AFW pumps to one or more SGs over a period of time ranging from 12 to 24 h (typically, one pump to one SG is adequate).

4. Main feedwater [MFW]. In lieu of AFW, MFW can be utilized to remove the post-shutdown decay heat. Depending on the individual plant design, either MFW or AFW may be used as the primary source of secondary-side heat removal.

5. PORV challenged [PORV]. For sequences in which both reactor trip and steam generator feedwater flow (MFW or AFW) have been successful, the pressurizer PORV may or may not lift, depending on the peak pressurizer pressure following the transient. (In most transients, these valves do not lift.) The lower branch indicates that the valve or valves were challenged and opened. Because of the multiplicity of relief and safety valves, it is assumed that a sufficient number would open if the demand from a pressure transient exists.

   The upper branch indicates that the pressurizer pressure was not sufficiently high to open a relief valve. For the sequences in which AFW fails following a reactor trip, PORVs are assumed to open for overpressure protection.

6. PORV reseats [PORV-RES]. Success for this branch requires the closure of any open relief valve once pressurizer pressure has decreased below the relief valve set point. If a PORV sticks open, PWR Class B and D plants are equipped with an isolation valve that allows for manual termination of the blowdown. Failure of a primary-side relief valve to close results in a transient-induced LOCA that is modeled as part of this event tree.

7. High-pressure injection [HPI]. In the case of a transient-induced LOCA, HPI is required to provide RCS makeup to keep the core covered. Success for this branch requires introduction of sufficient borated water to keep the core covered, considering core decay heat. (Typically, one HPI train is sufficient for this purpose.)

8. Feed and bleed [F&B]. If normal methods of achieving decay heat removal via the SGs (MFW and AFW) are unavailable, core cooling can be accomplished on most plants by establishing a feed and bleed operation. This operation (1) allows heat removal via discharge of reactor coolant to the containment through the PORVs and (2) RCS makeup via injection of borated water from the HPI system. Except at Class D plants, successful feed and bleed requires the operator to open the PORVs manually. At Class D plants, the HPI discharge pressure is high enough to lift the primary-side safety valves, and feed and bleed can be accomplished without the operator manually opening a PORV. HPI success for feed and bleed is dependent on plant design but requires the introduction of sufficient amounts of borated water into the RCS to remove decay heat and provide sufficient reactor coolant makeup to prevent core damage. PORV success for feed and bleed typically requires all PORVs at the plant to be opened.

9. Recovery of secondary-side cooling [SGCOOL]. Secondary-side cooling may be recovered following failure of AFW and MFW and successful initiation of feed and bleed but prior to refueling water storage tank (RWST) depletion, eliminating the need to use containment sump recirculation for continued core cooling. Successful long-term recovery of secondary-side cooling (since the steam generators are dry, flow from one motor-driven AFW or MFW pump is required) and termination of feed and bleed cooling results in core cooling success.

10. RCS cooldown to RHR initiation pressure [COOLDOWN]. Following initiation of HPI for RCS makeup following a transient-induced LOCA, substantial time (typically ~6 h) is available before the RWST is depleted and sump recirculation is required. An RCS cooldown to the RHR initiation pressure [using the turbine bypass valves (TBVs) and main condenser or the atmospheric dump valves (ADVs), in conjunction with AFW or MFW] and initiation of RHR will provide core cooling without the need for sump recirculation. This approach has been used in the mitigation of all historic PWR small-break LOCAs. Because RCS pressure is significantly reduced once on RHR, HPI can provide the limited makeup for a substantial period of time. Success for this branch requires an RCS cooldown to the RHR initiation pressure in time to allow initiation of RHR prior to RWST depletion.

11. Residual heat removal [RHR]. If the RCS can be cooled down and depressurized to the RHR initiation pressure, then the RHR system can be used for core cooling. Success for this branch requires the operation of one train of the RHR system. Many PWR Class B and D plants employ a common RHR pump suction line to supply RCS flow to both RHR trains. Multiple valves in this line must open for RHR success.

12. High-pressure recirculation [HPR]. Following a transient-induced LOCA or failure of secondary-side cooling and initiation of feed and bleed, continued core cooling and makeup are required. This requirement is satisfied by using HPI in the recirculation mode once the RWST is depleted, unless the plant can be placed on the RHR system beforehand. In this mode the HPI pumps recirculate reactor coolant collected in the containment sump and pass it through heat exchangers for heat removal. When MFW or AFW is available, heat removal is assumed to be required only to prevent HPI pump damage; if AFW or MFW is not available, HPR is required to remove

decay heat as well. Typically, at Class B and D plants, the low-pressure injection (LPI) pumps are utilized in the HPR mode, taking suction from the containment sump, passing the pumped water through heat exchangers, and providing net positive suction head to the HPI pumps.

The event tree applicable to a PWR Class G nonspecific reactor trip is shown in Figure B.11. Many of the event tree branches and the sequences leading to successful transient mitigation and core damage are similar to those following a nonspecific reactor trip transient for plant Class B (those branches are not discussed further). At Class G plants, however, the HPR system performs both the high- and low-pressure recirculation (LPR) function, taking suction directly from the containment sump without the aid of the low-pressure pumps. Decay heat removal is accomplished during recirculation by the containment spray recirculation (CSR) system.

1. Initiating event (transient) [IE-TRANS]. The initiating event is a nonspecific reactor trip, similar to that described for PWR Classes B and D.
2. Reactor trip [RT].
3. Auxiliary feedwater or main feedwater [AFW or MFW].
4. PORV or SRV challenged/reseats [PORV/PORV-RES].
5. High-pressure injection [HPI].
6. Feed and bleed [F&B].
7. Recovery of secondary-side cooling [SGCOOL].
8. RCS cooldown to RHR initiation pressure [COOLDOWN].
9. Residual heat removal [RHR].
10. Containment spray recirculation [CSR]. When secondary-side cooling and RHR are unavailable to remove decay heat, the CSR system operates to remove decay heat from the reactor coolant being recirculated. This is different from PWR Class B and D, where the decay heat removal function can be performed by HPR.
11. High-pressure recirculation [HPR]. In the event of a transient-induced LOCA or feed and bleed, continued HPI via sump recirculation is needed to provide makeup once the refueling water tank (RWT) is depleted, unless the plant can be placed on the RHR system beforehand. In Class G plants, initiation of HPR realigns the HPI pumps to the containment sump. The use of LPI pumps for suction-pressure boosting is not required.

The event tree for the PWR Class H nonspecific reactor trip is shown in Fig B.16. This class of plants is different from other PWR classes in that PORVs are not included in the plant design and feed and bleed cannot be used to remove decay heat in the event of MFW and AFW unavailability. If MFW or AFW cannot be recovered, the atmospheric dump valves can be used to depressurize the SGs to below the shutoff head of the condensate pumps, and these can be used, if available, for RCS cooling. The following is a description of event tree branches for PWR Class H that are different from those described for previous PWR classes.

1. Initiating event (transient) [IE-TRANS]. The initiating event is a nonspecific reactor trip, similar to that described for the previous PWR classes.
2. Reactor trip [RT].
3. Auxiliary feedwater or main feedwater [AFW or MFW].
4. Safety relief valve (SRV) challenged [SRV]. The lower branch indicates that at least one safety valve has lifted as a result of the transient. In most transients in which reactor trip has been successful and MFW or AFW is available, these valves do not lift. In the case where both MFW and AFW are unavailable, at least one SRV is assumed to lift. The upper branch indicates that the pressurizer pressure was not sufficiently high to cause a relief valve to open.
5. SRV reseat [SRV-RES]. Success for this branch requires the closure of any open safety valve once pressurizer pressure has been reduced below the safety valve set point. Because only safety valves are used on this plant class, no block valves exist that can be closed to terminate flow from a stuck-open relief valve.

6. High-pressure injection [HPI]. In the event of a transient-induced LOCA, HPI is required to provide RCS makeup to keep the core covered.
7. Condensate pumps [COND]. If MFW and AFW are unavailable, the atmospheric dump valves (or turbine bypass valves if the main steam isolation valves are open) may be used on Class H plants to depressurize the SGs to the point that the condensate pumps can be used for SG cooling. Flow from one condensate pump to one SG is assumed adequate. In the event of MFW and AFW unavailability, failure to depressurize one SG to the operating pressure of the condensate system or unavailability of the condensate pumps is assumed to result in core damage.
8. RCS cooldown to RHR initiation pressure [COOLDOWN].
9. Residual heat removal [RHR].
10. High-pressure recirculation [HPR]. The requirement for continued core cooling during mitigation of a transient-induced LOCA and following depletion of the RWT, if RHR has not been initiated, can be satisfied by using HPI in the recirculation mode. At Class H plants, initiation of HPR realigns the HPI pumps to the containment sump. The use of LPI pumps for suction-pressure boosting is not required.

The event tree applicable to PWR plant Class A nonspecific reactor trip is shown in Figure B.1. Many of the event tree branches and the sequences leading to successful transient mitigation and severe core damage are similar to those following a nonspecific reactor trip transient for plant Classes B and G.

Like the Class G plants, the Class A plants have a CSR system that provides decay heat removal during HPR. Use of CSR for decay heat removal was assumed to be required if AFW and MFW were unavailable, unless the plant could be depressurized and placed on the RHR system. LPI pumps are required to provide suction to the HPI pumps during recirculation. The event tree branches and sequences are discussed further below.

1. Initiating event (transient) [IE-TRANS]. The initiating event is a nonspecific reactor trip, similar to that described for the other PWR plant classes.
2. Reactor trip [RT].
3. Auxiliary feedwater or main feedwater [AFW or MFW].
4. PORV challenged and reseats [PORV and PORV-RES].
5. High-pressure injection [HPI].
6. Feed and bleed [F&B].
7. Recovery of secondary-side cooling [SGCOOL].
8. RCS cooldown to RHR initiation pressure [COOLDOWN].
9. Residual heat removal [RHR].
10. Containment spray recirculation [CSR].
11. High-pressure recirculation [HPR]. The LPI pumps provide suction to the high-pressure pumps in the recirculation mode.

B.5.2 Anticipated transient without scram

The event trees constructed define potential plant response following an ATWS. Following a failure to scram, significant AFW flow is required for short-term core cooling, and injection of soluble boric acid is required to shut down the fission reaction. In addition, the primary relief valves, in conjunction with a negative moderator temperature coefficient, must limit RCS pressure to prevent the failure of RCS components. Failure to limit RCS pressure, provide adequate AFW to remove core heat, or inject soluble boric acid is assumed to result in core damage following a failure to trip.

Similar event trees are used for all PWR classes. These are shown in Figures B.5, B.10, B.15, and B.20, respectively, for classes A, B and D, G, and H. Descriptions of event tree branches that are unique to the ATWS event trees follow Branches on the ATWS tree that are also included on the transient event tree for the class are not further described.

1. Initiating event (ATWS) [ATWS]. The initiating event for this tree is a transient with failure to scram the reactor through either automatic or manual actuation of the RPS. This initiating event is an effective transfer from the transient event tree for sequences involving failure to scram (sequence 21 for PWR Class B).
2. Primary pressure limited [RCSPRESS]. ATWS analyses assume RCS components will fail unpredictably above ~3200 psi. If this occurs, core damage is assumed to result. Success for this branch requires RCS pressure to be limited to no greater than ~3200 psi. Primary pressure is limited by an adequately negative moderator temperature coefficient and by the operation of the primary safety valves.
3. Auxiliary feedwater for ATWS [AFW-ATWS]. AFW and the secondary side relief valves are required to remove core heat. Typically, twice the normal AFW flow is required until the fission process is terminated by the addition of boric acid.
4. Emergency boration [BORATION]. Injection of concentrated boric acid via the HPI or charging system is required to terminate the fission process. Emergency boration is manually initiated.
5. SRV and PORV reseat following ATWS pressure relief [PORV-A or SRV-A]. All primary safety valves and the PORVs are assumed (1) to lift as a result of the high RCS pressure that accompanies an ATWS and (2) to discharge water. As a result of the passage of water through the valves, the valve failure-to-close probabilities are considerably higher than in the normal situation when only steam is relieved. Success for this branch requires the closure of all open safety valves and PORVs (if a PORV fails to close, its block valve can be closed by the operators).

   If a relief valve fails to close (down branch), a transient-induced LOCA results. Systems required to mitigate the LOCA are similar to those on the transient event tree. HPI is assumed to be successful because emergency boration is successful.
6. RCS cooldown to RHR initiation pressure [COOLDOWN].
7. Residual heat removal [RHR].
8. High-pressure recirculation [HPR].

B.5.3 PWR Loss-of-Offsite Power

The event trees constructed define representative plant responses to a LOOP. A LOOP (without turbine runback on plants with this feature) will result in reactor trip due to unavailability of power to the CRD mechanisms and a loss of MFW because of the unavailability of power to components in the condensate and condenser cooling systems.

The PWR LOOP tree constructed for plant Classes B and D is shown in Figure B.7. Descriptions of the event tree branches follow.

1. Initiating event (LOOP) [IE-LOOP]. The initiating event for the tree is a grid or switchyard disturbance to the extent that the generator must be separated from the grid and all offsite power sources are unavailable to plant equipment. The capability of a runback of the unit generator from full power to supply house loads exists at some plants but is not considered in the event tree. Only LOOPs that challenge the emergency power system (EPS) and result in plant trip are addressed in the ASP Program.
2. Reactor trip given LOOP [RT-L]. Unavailability of power to the CRD mechanisms is expected to result in a reactor trip and rapid shutdown of the plant. If the reactor trip does not occur following a LOOP, the transient was considered to proceed to core damage (this may be conservative).
3. Emergency power [EP]. Given a LOOP and a reactor trip, electric power would be lost to all loads not backed by battery power. When power is lost, diesel generators (DGs) are automatically started to provide power to the plant safety-related loads. Emergency power success requires the starting and loading of a sufficient number

of DGs to support safety-related loads in systems required to mitigate the transient and maintain the plant in a safe shutdown condition.

4. Auxiliary feedwater [AFW-L]. The AFW system functions to remove decay heat via the SG secondary side. Success requirements for this branch are equivalent to those following a nonspecific reactor trip and unavailability of MFW. Both MFW and condensate pumps would be unavailable following a LOOP. Because specific AFW systems may contain different combinations of turbine-driven and motor-driven AFW pumps, the capability of the system to meet its success requirements will depend on the state of the EPS and the number of turbine-driven AFW pumps that are available.

5. PORV challenged [PORV-L]. The upper and lower states for this branch are similar to those following a nonspecific reactor trip. While a PORV may or may not lift, depending on the peak pressure following a particular event, the ASP models typically assume lift occurs following a LOOP (this is conservative for some plants).

6. PORV reseats [PRVL-RES]. The success requirements for this branch are similar to those following a nonspecific reactor trip. However, for a situation in which emergency power is failed and the PORV fails to reseat, power is unavailable for block valve closure.

7. Seal LOCA [SEALLOCA]. In the event of a loss of emergency power following LOOP, both service water (SW) and component cooling water (CCW) are unavailable. This results in unavailability of RCP seal cooling and seal injection (since the charging pumps are also without power and cooling water). Unavailability of seal cooling and injection may result in seal failure after a period of time, depending on the seal design.

   The lower event tree branch represents the situation in which seal failure occurs prior to restoration of ac power. The upper branch represents the situation in which a seal LOCA does not occur.

8. Electric power recovered (long term). Recovery of offsite power in the long term following failure of emergency power can prevent or allow mitigation of an RCP seal LOCA. If emergency power is successful, recovery of offsite power can still allow recovery of condenser cooling and facilitate placing the plant on the RHR system, thereby preventing the use of sump recirculation following a transient-induced LOCA.

   For sequences involving emergency power failure in which a seal LOCA has occurred, long-term electric power recovery success [OP-SL] requires the restoration of ac power (either through recovery of offsite power or recovery of a DG) prior to core uncovery. For sequences involving emergency power failure in which a seal LOCA does not occur, electric power recovery success [OP-BD] requires the recovery of ac power prior to battery depletion, typically 2 to 4 h.

   If emergency power is successful, recovery of offsite power within 2 h [OP-2H] will allow sufficient time to recover the condenser, cool down the plant, and initiate RHR before depleting the RWST following a transient-induced LOCA, eliminating the need for sump recirculation. Recovery at 6 h [OP-6H] will facilitate recovery of secondary-side cooling in the event of an initial AFW failure.

9. High-pressure injection [HPI-L], feed and bleed [F&B-L], residual heat removal [RHR-L] and high pressure recirculation [HPR-L]. The success requirements for these branches are similar to those following a nonspecific reactor trip. Because the systems use motor-driven pumps, the capability of each system to meet its success requirements depends on the success of emergency power.

10. Recovery of secondary-side cooling [SGCOOL] and RCS cooldown to RHR initiation pressure [COOLDOWN]. Success requirements for these branches are similar to those following a nonspecific reactor trip. Prior recovery of offsite power is necessary to power secondary side balance of plant loads.

The event tree constructed for the PWR Class G LOOP is shown in Figure B.12. Most of the event tree branches and the sequences leading to successful mitigation and core damage are similar to those following a LOOP at Class B plants. However, at Class G plants, decay heat removal during recirculation is provided by the CSR system, not the HPR system. The event tree branches and sequences different from those for PWR B LOOP are discussed below.

1. Initiating event (LOOP) [IE-LOOP]. The initiating event is a LOOP similar to that described for PWR plant Classes B and D. The following branches have functions and success requirements similar to those following a LOOP at PWRs associated with all of the plant classes defined.

2. Reactor trip given LOOP [RT-L].
3. Emergency power [EP].
4. Auxiliary feedwater [AFW-L].
5. PORV challenged and reseats [PORV-L and PRVL-RES].
6. Seal LOCA [SEALLOCA].
7. Electric power recovered (long term) [OP-SL, OP-BD, OP-2H, OP-6H].
8. High-pressure injection, feed and bleed, residual heat removal, and high-pressure recirculation [HPI-L, F&B-L, RHR-L, HPR-L].
9. Recovery of secondary-side cooling and RCS cooldown to RHR initiation pressure [SGCOOL, COOLDOWN, RHR-L].
10. Containment spray recirculation [CSR-L]. The success requirements for this branch are similar to those following a nonspecific reactor trip. The CSR system provides decay heat removal for sequences in which secondary-side cooling is unavailable.

The event tree constructed for a PWR Class H LOOP is shown in B.17. Many of the event tree branches and sequences leading to successful mitigation and core damage are similar to those following a LOOP at Class B plants. However, Class H plants do not have feed and bleed capability and rely instead on secondary-side depressurization and the condensate system as an alternate decay heat removal method. The condensate system is assumed unavailable following a LOOP, which limits the diversity of decay heat removal on this plant class following this initiator. The event branches and sequences are discussed further below.

1. Initiating event (LOOP) [IE-LOOP]. The initiating event is a LOOP similar to that described for BWR Classes B and D. The following branches have functions and success requirements similar to those following a LOOP at PWRs associated with all of the plant classes defined.
2. Reactor trip given LOOP [RT-L].
3. Emergency power [EP].
4. Auxiliary feedwater [AFW-L].
5. SRV challenged [SRV-L]. The function of this branch is similar to that described under the PWR Class H transient.
6. SRV reseat [SRV-RES]. Success requirements for this branch are similar to those described under the PWR Class H transient.
7. Seal LOCA [SEALLOCA].
8. Electric power recovered (long term) [OP-SL, OP-BD].
9. High-pressure injection, residual heat removal, and high-pressure recirculation [HPI-L, RHR-L, HPR-L].
10. RCS cooldown to RHR initiation pressure [COOLDOWN].

The event tree constructed for the plant Class A LOOP is shown in Figure B.2. All of the event-tree branches and the sequences leading to successful mitigation and core damage are analogous to those following a LOOP at Class B plants with the addition of the CSR branch [CSR-L], which is required for decay heat removal during HPR if the plant cannot be cooled down and placed on the RHR system beforehand. Additional information on the use of the CSR system is provided in the discussion of the PWR Class A nonspecific reactor trip event tree.

B.5.4 PWR Small-Break Loss-of-Coolant Accident

Event trees were constructed to define the responses of PWRs to a small-break LOCA. The LOCA chosen for consideration is one that would require a reactor trip and continued HPI for core protection. Because of the limited amount of borated water available, the mitigation sequence also includes the requirement to recirculate borated water from the containment sump, unless the plant can be successfully cooled down and placed on the RHR system prior to RWST depletion.

The LOCA event tree constructed for PWR plant Classes B and D is shown in Figure B.8. The event tree branches and the sequences leading to core damage follow.

1. Initiating event (small-break LOCA) [IE-SLOCA]. The initiating event for the tree is a small-break LOCA that requires reactor trip and continued HPI for core protection.
2. Reactor trip [RT]. Reactor trip success is defined as the rapid insertion of sufficient control rods to place the core in a subcritical condition. Failure to trip was considered to lead to core damage in the ASP models (this may be conservative).
3. Auxiliary feedwater or main feedwater [AFW or MFW]. Use of AFW or MFW was assumed necessary for some small breaks to reduce RCS pressure to the point where HPI is effective. At Class D plants, the HPI pumps operate at a much higher discharge pressure and hence can function without secondary-side cooling from the AFW or MFW systems.
4. High-pressure injection [HPI]. Adequate injection of borated water from the HPI system is required to prevent excessive core temperatures and consequent core damage.
5. Feed and bleed [F&B]. In the event AFW and MFW are unavailable following a small-break LOCA, core cooling can be provided using the feed and bleed mode. Depending on the size of the small break, opening the PORVs may not be required for success (opening a PORV is not required for success for Class D).
6. RCS cooldown to RHR initiation pressure [COOLDOWN]. Following initiation of HPI, substantial time (typically ~6 h) is available before the RWST is depleted and sump recirculation is required. An RCS cooldown to the RHR initiation pressure (using the TBVs and main condenser, or the atmospheric dumps, in conjunction with AFW or MFW) and initiation of RHR will provide core cooling without the need for sump recirculation. This approach has been used in the mitigation of all historic PWR small-break LOCAs. Because RCS pressure is significantly reduced once on RHR, HPI can provide the limited makeup for a substantial period of time. Success for this branch requires an RCS cooldown to the RHR initiation pressure in time to allow initiation of RHR prior to RWST depletion.
7. Residual heat removal [RHR]. If the RCS can be cooled down and depressurized to the RHR initiation pressure, then the RHR system can be used for core cooling. Success for this branch requires the operation of one train of the RHR system. Many PWR Class B and D plants employ a common RHR pump suction line to supply RCS flow to both RHR trains. Multiple valves in this line must open for RHR success.
8. High-pressure recirculation [HPR]. The requirement for continued core cooling following a LOCA is satisfied by using HPI in the recirculation mode once the RWST is depleted, unless the plant can be placed on the RHR system beforehand. In this mode the HPI pumps recirculate reactor coolant collected in the containment sump and pass it through heat exchangers for heat removal. When MFW or AFW is available, heat removal is assumed to be required only to prevent HPI pump damage; if AFW or MFW is not available, HPR is required to remove decay heat as well. Typically, at Class B and D plants, the LPI pumps are utilized in the HPR mode, taking suction from the containment sump, passing the pumped water through heat exchangers, and providing net positive suction head to the HPI pumps.

The event tree constructed for a small-break LOCA at Class G plants is shown in Figure B.13. The LOCA event tree for Class G plants is similar to that for Class B and D plants except that long-term cooling is provided by the CSR system rather than by the HPR system. The event tree branches and sequences are discussed further below.

1. Initiating event (small-break LOCA) [IE-SLOCA]. The initiating event is a LOCA similar to that described for PWR plant Classes B and D. The following branches have functions and success requirements similar to those following a small-break LOCA at PWRs associated with all of the plant classes defined.
2. Reactor trip [RT].
3. Auxiliary feedwater and main feedwater [AFW and MFW].
4. High-pressure injection and feed and bleed [HPI and F&B].
5. Recovery of secondary-side cooling [SGCOOL].
6. RCS cooldown to RHR initiation pressure and RHR [COOLDOWN and RHR].
7. Containment spray recirculation [CSR]. In the event that normal secondary-side cooling (AFW or MFW) is unavailable following a small-break LOCA, cooling via the CSR system during HPR is required to mitigate the transient.
8. High-pressure recirculation [HPR].

The event tree constructed for a small-break LOCA at PWR Class H plants is shown in Figure B.18. The event tree has been developed assuming that SG depressurization and condensate pumps can provide adequate RCS pressure reduction in the event of an unavailability of AFW and MFW to permit HPI and HPR to function in these plants. The event tree branches and sequences are similar to those following a transient-induced LOCA.

1. Initiating event (small-break LOCA) [IE-SLOCA]. The initiating event is similar to that described above for PWR Classes B, D, and G. The following branches have functions and success requirements similar to those discussed previously for this class.
2. Reactor trip [RT].
3. Auxiliary feedwater, main feedwater, and condensate [AFW, MFW, and COND].
4. High-pressure injection [HPI].
5. RCS cooldown to RHR initiation pressure [COOLDOWN].
6. Residual heat removal [RHR].
7. High-pressure recirculation [HPR].

The event tree constructed for a small LOCA at Class A plants is shown in Figure B.3. The LOCA event tree for Class A plants is similar to that for Classes B and D except that the CSR system is required in conjunction with HPR in some sequences where secondary cooling is not provided.

As with the PWR transient and LOOP sequences, differences between plant classes are driven by the use of CSR on plant Classes A and G and by the use of condensate pumps in lieu of feed and bleed on PWR Class H.

B.5.5 PWR Steam Generator Tube Rupture

The event trees constructed define potential plant response following an SGTR. In the event of an SGTR, the nominal plant response is to provide RCS inventory makeup using the HPI system; detect and then isolate the ruptured SG by closing appropriate AFW, MFW, and main steam isolation valves; and depressurize the RCS to below the SG relief valve reseat pressure using the intact SGs. This allows the relief valves to reseat and terminates flow from the RCS into the failed SG. If the break cannot be isolated, the RCS must be cooled down further and the RHR system must be placed in operation before RWST inventory is depleted. Failure to perform these functions is assumed to result in core damage.

The SGTR event tree constructed for PWR plant Classes B and D, G, and A are shown in Figures B.9, B.14, and B.4, respectively. Descriptions of the branches that are unique to SGTR response follow. Branches on the SGTR event tree that are also included on other event trees are not described further.

1. Initiating event (SGTR) [IE-SGTR]. The initiating event is the failure of one SG tube, with resulting RCS flow from the primary to the secondary side of the SG. Simultaneous rupture of multiple tubes is not addressed.
2. Reactor trip [RT]. Failure to trip the reactor following an SGTR is assumed to result in core damage (this may be conservative).
3. Auxiliary feedwater [AFW-SGTR]. AFW flow to the intact (unimpacted) SGs must be provided to remove decay heat and cool the RCS to reduce its pressure to below the SG relief valve reseat point. Success for this branch requires flow from one or more AFW pumps to at least one intact SG.
4. Main feedwater [MFW]. The MFW system can be used for heat removal if AFW is unavailable. Most MFW systems isolate on safety injection, and subsequent operability is dependent on the type of pump driver; turbine-driven MFW pumps require steam from the nonimpacted SGs once the faulted SG is isolated.
5. High-pressure injection [HPI].
6. RCS cooldown below SG relief valve setpoint [RCS-SG]. Success for this branch requires the use of the ADVs or TBVs to reduce RCS pressure below the SG relief valve reseat pressure.
7. Ruptured SG isolated [SGISOL]. Success requires the ruptured SG to be isolated by closing open valves associated with feed, blowdown, and steam flow. This, in conjunction with RCS cooldown to below the SG relief valve reseat pressure, terminates flow from the tube rupture.
8. RCS cooldown below RHR pressure [RCSCOOL]. If the ruptured SG cannot be isolated, RCS cooldown is continued using the TBVs until RHR can be initiated. On plants with large ADV capacity, RCS cooldown may be accomplished without TBVs. Once on the RHR system, the SGs (which are no longer required for decay heat removal) can be isolated if necessary.
9. Residual heat removal [RHR].

The SGTR event tree constructed for PWR Class H is shown in Figure B.19. With the exception of one branch that addresses the potential use of the condensate system if both AFW and MFW fail, all branches are similar to those on the previous event trees.

1. Initiating event (SGTR) [IE-SGTR].
2. Reactor trip [RT].
3. Auxiliary feedwater [AFW-SGTR].
4. Main feedwater [MFW].
5. Condensate [COND]. In the event that both AFW and MFW are unavailable, the ADVs [or TBVs if the main steam isolation valve (MSIVs) are open] can be used on PWR Class H plants to depressurize the intact SGs to the point that the condensate pumps can be used for SG cooling. Flow from one condensate pump to one SG is assumed to be adequate.
6. High-pressure injection [HPI].
7. RCS cooldown below SG relief valve setpoint [RCS-SG].
8. Ruptured SG isolated [SGISOL].
9. RCS cooldown below RHR pressure [RCSCOOL].
10. Residual heat removal [RHR].

B.5.6 Alternate Recovery Actions

The PWR event trees have been developed on the basis that proceduralized recovery actions will be attempted if primary systems that provide protection from core damage are unavailable. In the event AFW and MFW are unavailable and cannot be recovered in the short term, the use of feed and bleed cooling is modeled in all plants except for Class H, where SG depressurization and use of the condensate pumps is modeled instead.

Alternate equipment and procedures—beyond the systems and functions included in the event trees—may be successful in mitigating the effects of an initiating event, provided the appropriate equipment or procedure is available at a particular plant. This may include:

- the use of supplemental DGs—beyond the normal safety-related units—to power equipment required for continued core cooling and reactor plant instrumentation. A number of plants have added such equipment, often for fire protection.
- depressurization following a small-break LOCA to the initiation pressure of the LPI systems to provide RCS makeup in the event that HPI fails. Procedures to support this action are known to exist at some plants.
- use of electric power cross-ties among adjacent units.

The potential use of these alternate recovery actions was addressed in the analysis of the 1994 precursors when information concerning their plant-specific applicability was available.

B.6 BWR Event Tree Models

The BWR event trees describe the impact of the availability and unavailability of front-line systems in each plant class on core protection following three initiating events: trip, LOOP, and small-break LOCA. The systems modeled in the event trees are those associated with the generic functions required in response to an initiating event. The systems that are assumed capable of providing these functions are:

Function	System
Reactor subcriticality	Reactor scram and standby liquid control (following failure to trip)
Reactor coolant system integrity	Addressed in small-break LOCA models and in trip and LOOP sequences involving failure of primary relief valves to reseat
Reactor coolant inventory	High-pressure injection systems [HPCI or HPCS, RCIC, CRD, FWCI]
	Main feedwater
	Low-pressure injection systems following blowdown [low-pressure coolant injection (LPCI) (BWR Classes B and C), condensate, low-pressure core spray (LPCS), residual heat removal service water (RHRSW) or equivalent]
Short-term core heat removal	Power conversion system (PCS)
	High-pressure injection systems [HPCI, RCIC, CRD, FWCI (BWR Class A)]
	Isolation condenser (BWR Classes A and B)
	Main feedwater
	Low-pressure injection systems following blowdown [LPCI (BWR Classes B and C), LPCS, condensate]
	Note: Short-term core heat removal to the suppression pool (all cases where power conversion system is faulted) requires use of the RHR system or containment venting for heat removal in the long term.

Function	System
Long-term core heat removal	Power conversion system
	Isolation condenser (BWR Class A)
	Residual heat removal [shutdown cooling or suppression pool cooling modes (BWR Class C)]
	Shutdown cooling (BWR Classes A and B)
	Containment cooling (BWR Class A)
	Low-pressure coolant injection [containment cooling (CC) mode (BWR Class B)]
	Containment venting

B.6.1 BWR Nonspecific Reactor Trip

The nonspecific reactor trip event tree constructed for BWR plant Class C is shown in Figures B.35 and 36. The event tree branches and the sequences leading to potential severe core damage follow [event tree branch designations are shown in brackets]. The Class C plants are discussed first because all but a few of the BWRs fit into the Class C category.

1. Initiating event (transient) [IE-T]. The initiating event is a transient or upset event that results in a rapid shutdown of the plant. Transients that are initiated by a LOOP or a small-break LOCA are modeled in separate event trees. Transients initiated by a large-break LOCA or large SLB are not addressed in the event trees described here; trees applicable to such initiators are developed separately if required.

2. Reactor shutdown [RPS]. To achieve reactor subcriticality and thus halt the fission process, the RPS commands rapid insertion of the control rods into the core. Successful scram requires rapid insertion of control rods with no more than two adjacent control rods failing to insert. Failure to scram results in sequences associated with ATWS, which is described later in this section.

3. Power conversion system [PCS]. Upon successful reactor scram, continued operation of the PCS would allow continued heat removal via the main condenser. This is considered successful mitigation of the transient. Continued operation of the PCS requires the MSIVs to remain open and requires the operation of the condenser, the turbine bypass system (TBS), the condensate pumps, the condensate booster pumps, and the feedwater pumps.

4. SRVs close [SRV]. SRVs are assumed to lift following scram. Success for this branch requires the reseating of all but one open SRV once the reactor pressure vessel (RPV) pressure decreases below the relief valve set point. If an SRV sticks open, a transient-induced LOCA is initiated. The response of BWR Class C plants to a single stuck-open SRV is similar to the response when no SRV sticks open and is represented by the upper branch. The failure of two valves to close is represented by the middle branch; plant response is similar to a medium-break LOCA. The lowest branch represents the failure of more than two SRVs to close. This response is similar to a large-break LOCA.

5. Feedwater [MFW]. Given unavailability of the PCS, continued delivery of feedwater to the RPV will keep the core from becoming uncovered. This, in combination with successful long-term decay heat removal, will mitigate the transient, preventing core damage. For plants with turbine-driven feed pumps, the PCS failure with subsequent feedwater success cannot involve MSIV closure or loss of condenser vacuum because this would disable the feed pumps.

6. High-pressure coolant injection (or high-pressure core spray) [HCI]. The primary function of the HPCI or HPCS system is to provide makeup following small-break LOCAs while the reactor is at high pressure (not depressurized). The system is also used for decay heat removal following transients involving a loss of feedwater. Some later Class C plants are equipped with HPCS systems, but the majority are equipped with

HPCI systems. HPCI or HPCS can provide the required makeup and short-term decay heat removal when the condenser and feedwater system are unavailable.

7. Reactor core isolation cooling [RCI]. The RCIC system is designed to provide high-pressure coolant makeup for transients that result in LOFW. Both RCIC and HPCI (or HPCS) initiate when the reactor coolant inventory drops to the low-low level set point, taking suction from the condensate storage tank or the suppression pool. To prevent tripping of HPCI and RCIC pumps on high water level, HPCI is normally secured after HPCI/RCIC initiation when pressure and water level are restored. RCIC must then be operated until the RHR system can be placed in service. The RCIC system is also capable of providing successful makeup following a single stuck-open SRV.

8. Depressurization via manual actuation of the SRVs or the automatic depressurization system [ADS]. In the event that the high-pressure systems have failed to provide adequate flow, the RPV can be depressurized to allow use of the low-pressure, high-capacity injection systems. The ADS will automatically initiate on high drywell pressure and low-low reactor water level, the availability of one train of the LPCI or LPCS systems, and following a time delay (which can be reset by the operator). The SRVs can also be opened by the operators to speed the depressurization process or if ADS fails to automatically actuate.

9. CRD injection [CRD]. In transient-induced sequences where heat removal and minimal core makeup are required (i.e., no more than one SRV sticks open), the CRD pumps can deliver coolant to the RPV.

10. Condensate system [CDS]. Low-pressure injection can be provided by the condensate system if it is available following a loss of feedwater. Condensate is initially drawn from the condenser hotwell.

11. Low-pressure core spray [LCS]. Low-pressure injection can be provided by the LPCS system if required. The LPCS system performs the same functions as the LPCI system (described below) except that the coolant, which is drawn from the suppression pool or the condensate storage tank (CST), is sprayed over the core.

12. Low-pressure coolant injection [LCI]. The LPCI system can provide short-term heat removal and cooling water makeup if the reactor has been depressurized to the operating range of the low-head RHR pumps. At Class C plants, LPCI is a mode of the RHR system; thus, the RHR pumps operate during LPCI. LPCI takes suction from the suppression pool or the CST and discharges into the recirculation loops or directly into the reactor vessel. If LPCI is successful in delivering sufficient flow to the reactor, long-term heat removal success is still required to mitigate core damage.

13. RHR service water or other injection source [SWS]. This is a backup measure for providing water to the reactor to reflood the core and maintain core cooling if other injection sources are unavailable. Typically, the high-pressure SW pumps are aligned to the shell side of the RHR heat exchangers for delivery of water to one of the recirculation loops.

14. Residual heat removal [RHR]. Three modes of RHR are represented by this branch. In the shutdown cooling mode, coolant is circulated from the reactor by the RHR pumps through the RHR heat exchangers and back to the reactor vessel. In the suppression pool cooling mode, the RHR pumps and heat exchangers are aligned to take water from the suppression pool, cool it using the RHR heat exchangers, and return it to the suppression pool. In the containment spray mode, water from the suppression pool is first cooled using the RHR heat exchangers before being sprayed into the containment and returning to the suppression pool. Long-term core cooling success requires that heat transfer to the environment commence within ~12–24 h of the transient. RHR success following successful reactor scram and high- or low-pressure injection of water to the RPV will prevent core damage.

15. Containment venting [CVS]. If RHR fails, decay heat can be removed by venting the suppression pool or drywell. Success for this branch requires alignment of the vent header and initiation of venting prior to exceeding a plant-specific maximum containment pressure. The time to reach this pressure is sequence-specific in many cases.

16. CRD injection following venting [CR1]. The steaming that will occur in the suppression pool following venting is assumed to fail any injection source that draws from the suppression pool. Hence, the feed operation associated with venting must come from an injection system that operates at low pressure and that has a source of water other than the suppression pool. If RPV makeup is from the suppression pool prior to venting, then

another makeup source must be aligned. One potential source of post-venting injection is the CRD system, represented by this branch. Because venting occurs late, only minimal CRD flow (one pump) is required.

17. RHRSW injection following venting [SW1]. If the CRD system is unavailable for post-venting makeup, the RHRSW system can be used instead. This branch represents the success or failure of the RHRSW system for this purpose.

The event tree constructed for a BWR plant Class A nonspecific reactor trip is shown in Figure B.21. The event tree is similar to that constructed for BWR Class C plants with the following exceptions: Class A plants are equipped with ICs and FWCI systems instead of RCIC and HPCI (or HPCS) systems. The isolation condensers can provide long-term core cooling provided no loss of inventory exists. Class A plants do not have LPCI systems, although they are equipped with LPCS; suppression pool cooling is provided by a system independent of the shutdown cooling (SDC) system. The event tree branches different from those for Class C are discussed further below.

1. Initiating event (transient) [IE-T]. The initiating event is a nonspecific reactor trip similar to that described for BWR Class C plants. The following branches have functions and success requirements similar to those following a transient at BWRs associated with Class C.

2. Reactor shutdown[RPS].

3. Power conversion system [PCS].

4. SRVs close [SRV]. The three branches represent conditions in which (1) all open SRVs close, (2) one valve fails to close, and (3) more than one valve fails to close. Following a transient with closure of all SRVs (upper branch), the IC can provide core cooling, as can MFW. If one SRV sticks open, MFW is required for RPV makeup and short-term core cooling, unless the RPV is depressurized so that low-pressure systems can be used. If more than one SRV sticks open, then the low-pressure systems can be utilized without the need for automatic or manual depressurization.

5. Feedwater [MFW]. MFW or FWCI can provide short-term transient mitigation. MFW is required for makeup in transient-induced LOCA sequences and for heat removal in sequences when the IC system would have mitigated the transient but was not available. FWCI is initiated automatically on low reactor level and uses the normal feedwater trains to deliver water to the reactor vessel. When feedwater is successful, long-term decay heat removal is required for complete transient mitigation. (PCS unavailability is assumed prior to MFW demand.)

6. Isolation condenser and isolation condenser makeup [ISO]. If PCS is not available and significant inventory has not been lost via the SRVs, then the IC system can provide decay heat removal and mitigate the transient. The IC system is an essentially passive system that condenses steam produced by the core, rejecting the heat to cooling water and returning the condensate to the reactor. Makeup is provided to the cooling water as needed. The system does not provide makeup to the reactor vessel.

7. Depressurization via SRV or ADS [ADS].

8. CRD injection [CRD].

9. Condensate system [CDS].

10. Low-pressure core spray [LCS].

11. Fire water injection [FWS]. Fire water or other raw water systems can provide a capability similar to that provided by the RHRSW connection on Class C BWRs. As a backup source, if all normal core cooling is unavailable, fire water can be aligned to the LPCS injection line to provide water to the reactor vessel.

12. Shutdown cooling [SDC]. Like the shutdown cooling mode of the RHR system at Class C plants, the SDC system is a closed-loop system that performs the long-term decay heat removal function by circulating primary coolant from the reactor through the system's heat exchangers and back to the reactor vessel. Success requires the operation of at least one SDC loop.

13. Containment cooling [CSS]. If the SDC system fails to provide long-term decay heat removal, the CC system can remove decay heat. The system utilizes dedicated pumps, drawing suction from the suppression pool,

passing it through heat exchangers where heat is rejected to the service water system, and then either returning it directly to the suppression pool or spraying it into the dry well.

14. Containment venting [CVS].
15. CRD injection following venting [CR1].
16. Firewater injection following venting [FW1]. This branch is equivalent to RHRSW injection following venting in BWR Class C.

The event tree constructed for a BWR plant Class B nonspecific reactor trip is shown in Figures B.25 through B.28. The event tree is most similar to that constructed for BWR Class A plants. In fact, the branches are the same except that Class B plants are equipped with HPCI systems instead of FWCI systems, and they are equipped with an LPCI system that represents an additional capability for providing low-pressure injection. Also, at Class B BWRs, the containment system considered in the event tree utilizes the LPCI pumps rather than having its own dedicated pumps.

B.6.2 Anticipated Transient Without Scram

The event trees constructed define potential plant response following an ATWS. Following a failure to automatically and manually scram or insert rods, the fission process is terminated by tripping the recirculation pumps and injecting soluble boron into the RPV. Availability of the PCS at this point terminates the transient. If PCS is unavailable, the operators further control power by lowering the RPV level to the top of the active fuel and using HPCI or HPCS for makeup. Failing this, RPV pressure is lowered to allow the low-pressure systems to provide makeup.

Similar event trees are used for each BWR class (differences exist in the systems used for makeup, consistent with the systems available at each plant class). The event trees are shown in Figures B.34, B.40, and B.32, respectively, for classes A, B, and C. Descriptions of the event tree branches that are unique to ATWS follow. Branches on the ATWS trees that are also included on the transient event trees are not discussed further.

1. Initiating event (reactor shutdown) [RPS]. The initiating event is an effective transfer from the transient event tree for sequences involving failure to scram (sequence 80 for BWR Class C).
2. Recirculation pump trip [RRS]. Success for this branch requires the automatic or manual trip of the recirculation pumps to reduce power.
3. Standby liquid control [SLC]. The operators manually start the standby liquid control system to borate the RPV. This system is initiated immediately following a failure to scram since it takes some time to be effective.
4. ADS inhibited and level controlled [AD1]. Failing to shut down the reactor manually or by alternate means, the operators must attempt to control power using RPV level. The major actions are as follows. First, inhibit ADS. This both protects the containment (by avoiding a major transfer of hot RPV water to the suppression pool) and prevents the automatic actuation of LPCS and LPCI. Second, terminate injection. This excludes standby liquid control system (SLCS) injection and CRD flow. RPV level is deliberately lowered to the top of the active fuel (TAF). Level lowering reduces reactivity and power. Third, restore injection. If water level were to fall below TAF, there would be no assurance that core damage would be prevented. Hence, level is reinstated.
5. High-pressure coolant injection [HCI].
6. Manual reactor depressurization [DEP]. If the high-pressure systems are unavailable, the operators lower RPV pressure to allow the use of the low-pressure systems for RPV makeup. This must be done carefully to prevent flushing boron from the core region.
7. Condensate, LPCS, LPCI (if available) [CDS, LCS, LCI].
8. Residual heat removal or shutdown cooling and containment cooling [RHR or SDC and CSS]. Only the suppression pool cooling made of RHR is viable because of the time periods and RPV pressures involved.
9. Containment venting [CVS].

B.6.3 BWR Loss-of-Offsite Power

The event trees constructed define responses of BWRs to a LOOP in terms of sequences representing success and failure of plant systems. Only LOOPs that challenge the EPS and result in scram are addressed in the ASP Program.

The event tree constructed for a LOOP at BWR Class C plants is shown in Figures B.37 and B.38. The event tree branches associated with sequences leading to core damage are described below (branches that are identical to those for a BWR Class C transient are not further described).

1. Initiating event (LOOP) [IE-L]. The initiating event for a LOOP corresponds to any situation in which power from both the auxiliary and startup transformers is lost and scram occurs. This situation could result from grid disturbances or onsite faults.
2. Reactor shutdown [RP1]. Given a load rejection, a scram signal is generated. Successful scram is the same as for the transient trees: a rapid insertion of control rods with no more than two adjacent control rods failing to insert. The scram can be automatically or manually initiated. Failure to scram following a LOOP is assumed to result in core damage (this may be conservative).
3. Emergency power [EPS]. Emergency power is provided by DGs at almost all plants. The DGs receive an initiation signal when an undervoltage condition is detected. Emergency power success requires the starting and loading of a sufficient number of DGs to support safety-related loads in systems required to mitigate the transient and maintain the plant in a safe shutdown condition.
4. LOOP recovery (long-term) [OEP]. Success for this branch requires recovery of offsite power or diesel-backed ac power before the station batteries are depleted, typically 2 to 4 h.
5. SRVs close [SRV].
6. HPCI (or HPCS) or RCIC [HCI and RCI]. Success requirements for these branches are identical to those following a transient at Class C BWRs. Either RCIC or HPCI (or HPCS) can provide the makeup and short-term core cooling required following most transients, including failure of the EPS. HPCI and RCIC only require dc power and sufficient steam to operate the pump turbines. HPCS systems utilize a motor-driven pump but are diesel-backed and utilize dedicated SW cooling.
7. Depressurization via SRV or the ADS [ADS].
8. CRD injection [CRDL]. Given availability of emergency power to the CRD pumps, success requirements for this branch following a LOOP are identical to those following a transient. Manual restart of the CRD pumps is required following the LOOP.
9. LPCS, LPCI, and RHR service water injection [LCSL, LCIL, and SWSL]. Given availability of emergency power, success requirements for these branches following a LOOP are identical to those following a transient.
10. Residual heat removal [RHRL]. Given the availability of emergency power, the success requirements for this branch are similar to those following a nonspecific reactor trip transient at Class C BWRs. Success for any one of the three modes associated with RHR can provide the long-term decay heat removal required for transient mitigation. If emergency power fails, it must be recovered to power long-term decay heat removal equipment. However, long-term decay heat removal is not required until ~12–24 h after the LOOP (well beyond the time at which emergency power must be recovered to avoid battery depletion).
11. Containment venting, CRD injection following venting, and RHRSW injection following venting [CVS, CR1L, and SW1L].

The event tree constructed for a LOOP at BWR Class A plants is shown in Figure B.22. The event tree is similar to that constructed for BWR Class C plants with the major exception that Class A plants are equipped with ICs and FWCI systems instead of RCIC and HPCI (or HPCS) systems. However, given a LOOP, FWCI would be unavailable because it is not backed by emergency power. Also, additional long-term core cooling is not required with IC success, as long as no transient-induced LOCA exists. In the emergency power failure sequences, the IC system is the only system that can provide core cooling because FWCI would be without power. The event tree branches that are different from those for a BWR Class A transient and a BWR Class C LOOP (LOOP-related branches only) are further discussed below.

1. Initiating event (LOOP) [IE-L]. The initiating event is a LOOP similar to that described for Class C BWRs.
2. Reactor shutdown [RP1].
3. Emergency power [EPS].
4. LOOP recovery (long-term) [OEP].
5. SRVs close [SRV].
6. Feedwater [MFW]. The feedwater system can provide short-term core cooling and makeup for transient mitigation. However, MFW success requires normal power supplies on most plants. If emergency power can be supplied to the MFW pumps (from a gas turbine, for example), then MFW can provide short-term core cooling and makeup.
7. Isolation condenser and isolation condenser makeup [ISO].
8. Depressurization via SRV or ADS [ADS].
9. CRD injection [CRDL]. Given availability of emergency power to the CRD pumps, success requirements for this branch following a LOOP are identical to those following a transient. Manual restart of the CRD pumps is required following the LOOP.
10. LPCS and fire water injection [LCSL and FWS]. Success requirements for these branches are similar to those following a nonspecific reactor trip at Class A BWRs. With interim high-pressure cooling unavailable, either LPCS or, as a last resort, fire water or another water source can be used to provide low-pressure water for core makeup and cooling. LPCS pumps and valves require emergency power to operate. Plants typically have one engine-driven fire pump that can run during a LOOP without emergency power.
11. SDC and containment cooling [SDCL and CSSL]. Given the availability of emergency power or recovery of offsite power, success requirements fcr these branches are similar to those following a nonspecific reactor trip transient at Class A BWRs.
12. Containment venting, CRD injection following venting, and firewater injection following venting [CVS, CR1L, FW1].

The event tree constructed for a BWR plant Class B LOOP is shown in Figures B.29 through B.32. The event tree is most similar to that constructed for BWR Class A plants. The branches are the same, except that Class B plants are equipped with HPCI systems instead of FWCI systems and are equipped with a LPCI system, which represents an additional capability for providing low-pressure injection. At Class B BWRs, the containment cooling system utilizes the LPCI pumps rather than having its own dedicated pumps. In emergency power failure sequences, either the IC or HPCI system can provide the required core cooling for short-term transient mitigation. However, if an SRV sticks open (transient-induced LOCA), then the IC cannot provide the makeup needed, and HPCI is required. The IC can also provide long-term cooling, but when only HPCI is operable, recovery of emergency power is necessary to power SDC-related loads.

B.6.4 BWR Loss-of-Coolant Accident

The event trees constructed define the response of BWRs to a LOCA in terms of sequences representing success and failure of plant systems. The LOCA chosen for consideration is a small-break LOCA that would require a reactor scram and continued operation of high-pressure systems. A large-break LOCA would require operation of the high-volume/low-pressure systems and is not addressed in the models.

The LOCA event tree constructed for BWR Class C plants is shown in Figure B.39. The event tree branches associated with core damage sequences follow (only branches that are different from BWR Class C transient sequences are described).

1. Initiating event (small LOCA) [IE-SL]. Any breach in the RCS on the reactor side of the MSIVs that results in coolant loss in excess of the capacity of one CRD pump and a reactor scram is considered to be a LOCA.

A small-break LOCA is considered to be one in which losses are not great enough to reduce the system pressure to the operating range of the low-pressure systems.

2. Reactor shutdown [RPS].
3. MFW, HPCI or HPCS, and RCIC [MFW, HCI and RCI].
4. Depressurization via SRV or ADS [ADS].
5. Control rod drive injection [CRD].
6. Condensate, LPCS, LPCI, or RHR service water [CDS, LCS, LCI, and SWS].
7. Residual heat removal [RHR].
8. Containment venting, CRD injection followinp venting, and RHRSW injection following injection [CVS, CR1, SW1].

The small-break LOCA event tree constructed for BWR Class A plants is shown in Figure B.23. The event tree branches associated with sequences leading to core damage follow (only branches that are different from BWR Class A transient branches are described).

1. Initiating event (small-break LOCA) [IE-S]. The initiating event is a small-break LOCA similar to that described for BWR Class C plants.
2. Reactor shutdown [RPS].
3. Feedwater [MFW].
4. Depressurization via SRV or ADS [ADS].
5. CRD injection [CRD].
6. Condensate, low-pressure core spray, and fire water injection [CDS, LPCS, and FWS].
7. Shutdown cooling and containment cooling [SDC and CSS].
8. Containment venting, CRD injection following injection, and firewater injection following venting [CVS, CR1, and FW1].

The small-break LOCA event tree constructed for BWR Class B plants is shown in Figure B.33. The event tree is most similar to that constructed for BWR Class A plants. In fact, the branches are the same, except that (1) some Class B plants are equipped with HPCI systems instead of FWCI systems and (2) Class B BWRs have a LPCI system, which provides an additional capability for low-pressure injection. At Class B BWRs, the containment cooling system uses the LPCI pumps rather than having its own dedicated pumps.

B.6.5 Alternate Recovery Actions

The BWR event trees have been developed on the basis that proceduralized recovery actions will be attempted if primary systems that provide protection against core damage are unavailable. If feedwater, HPCI, and RCIC are unavailable (FWCI and ICs on BWR Classes A and B) and cannot be recovered in the short term, the use of ADS (to depressurize below the operating pressure of low-pressure systems) and the CRD pumps is modeled. In addition, the potential for short-term recovery of a faulted system is also included in the appropriate branch model.

Alternate equipment and procedures, beyond the systems and functions included in the event tree, may be successful in mitigating the effects of an initiating event, provided the appropriate equipment or procedure is available at a particular plant. This may include:

- the use of supplemental diesel generators, beyond the normal safety-related units, to power equipment required for continued core cooling and reactor plant instrumentation. A number of plants have added such equipment, often for fire protection.

the use of electric power cross-ties among adjacent units. The potential use of these alternate recovery actions was addressed in the analysis of the 1994 precursors when information concerning their plant-specific applicability was available.

B.7 Fault Tree Models

Fault tree models were developed for each branch included in the accident sequences represented on the plant-class event trees. While a single fault tree could be used to model the failure logic for some systems, others required multiple models to represent the different success criteria applicable to different sequences.

The system fault tree models consider (1) failures of active components that must start and run or change position when a system is demanded and (2) components such as manual valves that must remain in a preset condition. The common cause failure of redundant components that can directly result in system failure (a subset of all potential common cause failures) is also included. Operator actions required to actuate a manually actuated system are also addressed, as are actions to recover an initially failed system.

Each fault tree was developed using "supercomponent" basic events that include grouped failures associated with a major component such as a pump or a train of a system. The use of supercomponents provides the same logic structure as a model developed with individual component basic events but facilitates computer solution of the logic models. As an example of a supercomponent, consider a train of a system that includes a motor-operated valve that must open, two manual valves that must remain open, a check valve that must open, and a pump that must start and run. If none of these components and failure modes are included elsewhere in any other fault tree, except perhaps in the same grouping, then they can be combined into a single supercomponent. The supercomponent, which should have engineering meaning, is then used as a single basic event representing the potential failure of the five components.

Basic event failure probabilities for each supercomponent are developed using individual component failure probabilities, primarily from the ASP data base,[6] earlier ASP program data, and NUREG-1032.[7] A 24-h mission time is used for most components with hourly failure rates, such as a pump failing to run (one exception was the mission time for emergency diesel generators, which is based on the 90th percentile LOOP recovery time).

In the example supercomponent, probabilities for failure of the motor-operated valve to open (3.0×10^{-3}), failure of both manual values to remain open (2×10^{-4}), failure of the pump to start and run for its mission time [3×10^{-3} (start) + 24 h × $3 \times 10\text{-}^{5}$/h (run)], and failure of the check valve to open (1×10^{-4}) would be added to estimate the supercomponent failure probability (7.0×10^{-3}).

Common cause failure probabilities are quantified using the Multiple Greek Letter (MGL) method with data from *Procedures for Analysis of Common Cause Failures in Probabilistic Safety Analysis*, NUREG/CR-5801.[8]

At the present time, the only support system failures that are modeled are emergency ac power failures following a LOOP. The models may be expanded in the future to include other support system failures, such as those in the service water system.

An example ASP fault tree is included in Figure B.41. Additional information concerning the development of the fault tree models is provided in Ref. 9.

B.8 References

1. *Systems Analysis Programs for Hands-On Integrated Reliability Evaluations (SAPHIRE)*, Version 5.0, NUREG/CR-6116, Vols. 1-10.

2. *PRA Procedures Guide,* NUREG/CR-2300, January 1983, Section 6.3.2.4.

3. *Precursors to Potential Severe Core Damage Accidents: 1992, A Status Report*, NUREG/CR-4674, Vol. 17, Appendix A, December 1993.

4. M. Modarres, E. Lois, and P. Amico, Martin Marietta Energy Systems, Inc., Oak Ridge National Laboratory, *LWR Categorization Report,* University of Maryland, College Park, MD, November 13, 1984.

5. E. Lois, *A Class-Specific Approach to Nuclear Power Plant Safety Studies with Applications*, PhD Dissertation, University of Maryland, College Park, MD, 1985.

6. *Analysis of Core Damage Frequency: Internal Events Methodology*, NUREG/CR-4550, Vol. 1, Rev. 1, January 1990.

7. P. W. Baranowsky, *Evaluation of Blackout Accidents at Nuclear Power Plants*, NUREG-1032, June 1988.

8. A. Mosleh, *Procedures for Analysis of Common Cause Failures in Probabilistic Safety Analysis,* NUREG/CR-5801, April 1993.

9. M. Sattison et al., "SAPHIRE Models and Software for ASP Evaluations," *Proceedings of the U.S. Nuclear Regulatory Commission's Twenty-Second Water Reactor Safety Information Meeting,* NUREG/CP-0140, Vol. 1, October 1994.

Table B.1. ASP Reactor Plant Classes

Plant name	Plant class
ANO - Unit 1	PWR Class D
ANO - Unit 2	PWR Class G
Beaver Valley 1	PWR Class A
Beaver Valley 2	PWR Class A
Browns Ferry 1	BWR Class C
Browns Ferry 2	BWR Class C
Browns Ferry 3	BWR Class C
Braidwood 1	PWR Class B
Braidwood 2	PWR Class B
Brunswick 1	BWR Class C
Brunswick 2	BWR Class C
Byron 1	PWR Class B
Byron 2	PWR Class B
Callaway 1	PWR Class B
Calvert Cliffs 1	PWR Class G
Calvert Cliffs 2	PWR Class G
Catawba 1	PWR Class B
Catawba 2	PWR Class B
Clinton 1	BWR Class C
Comanche Peak	PWR Class B
Cook 1	PWR Class B
Cook 2	PWR Class B
Cooper Station	BWR Class C
Crystal River 3	PWR Class D
Davis-Besse	PWR Class B
Diablo Canyon 1	PWR Class B
Diablo Canyon 2	PWR Class B
Dresden 2	BWR Class B
Dresden 3	BWR Class B
Duane Arnold	BWR Class C
Farley 1	PWR Class B
Farley 2	PWR Class B
Fermi 2	BWR Class C
Fitzpatrick	BWR Class C
Fort Calhoun	PWR Class G
Ginna	PWR Class B

Table B.1. ASP Reactor Plant Classes (cont.)

Plant name	Plant class
Grand Gulf 1	BWR Class C
Haddam Neck	PWR Class B
Harris 1	PWR Class B
Hatch 1	BWR Class C
Hatch 2	BWR Class C
Hope Creek 1	BWR Class C
Indian Point 2	PWR Class B
Indian Point 3	PWR Class B
Kewaunee	PWR Class B
LaSalle 1	BWR Class C
LaSalle 2	BWR Class C
Limerick 1	BWR Class C
Limerick 2	BWR Class C
Maine Yankee	PWR Class B
McGuire 1	PWR Class B
McGuire 2	PWR Class B
Millstone 1	BWR Class A
Millstone 2	PWR Class G
Millstone 3	PWR Class A
Monticello	BWR Class C
Nine Mile Point 1	BWR Class A
Nine Mile Point 2	BWR Class C
North Anna 1	PWR Class A
North Anna 2	PWR Class A
Oconee 1	PWR Class D
Oconee 2	PWR Class D
Oconee 3	PWR Class D
Oyster Creek	BWR Class A
Palisades	PWR Class G
Palo Verde 1	PWR Class H
Palo Verde 2	PWR Class H
Palo Verde 3	PWR Class H
Peach Bottom 2	BWR Class C
Peach Bottom 3	BWR Class C
Perry 1	BWR Class C
Pilgrim 1	BWR Class C

Table B.1. ASP Reactor Plant Classes (cont.)

Plant name	Plant class
Point Beach 1	PWR Class B
Point Beach 2	PWR Class B
Prairie Island 1	PWR Class B
Prairie Island 2	PWR Class B
Quad Cities 1	BWR Class C
Quad Cities 2	BWR Class C
River Bend 1	BWR Class C
Robinson 2	PWR Class B
Salem 1	PWR Class B
Salem 2	PWR Class B
San Onofre 2	PWR Class H
San Onofre 3	PWR Class H
Seabrook 1	PWR Class B
Sequoyah 1	PWR Class B
Sequoyah 2	PWR Class B
South Texas 1	PWR Class B
St. Lucie 1	PWR Class G
St. Lucie 2	PWR Class G
Summer 1	PWR Class B
Surry 1	PWR Class A
Surry 2	PWR Class A
Susquehanna 1	BWR Class C
Susquehanna 2	BWR Class C
Three Mile Island 1	PWR Class D
Turkey Point 3	PWR Class B
Turkey Point 4	PWR Class B
Vermont Yankee	BWR Class C
Vogtle 1	PWR Class B
Vogtle 2	PWR Class B
WNP 2	BWR Class C
Waterford 3	PWR Class H
Wolf Creek 1	PWR Class B
Yankee Rowe	PWR Class B
Zion 1	PWR Class B
Zion 2	PWR Class B

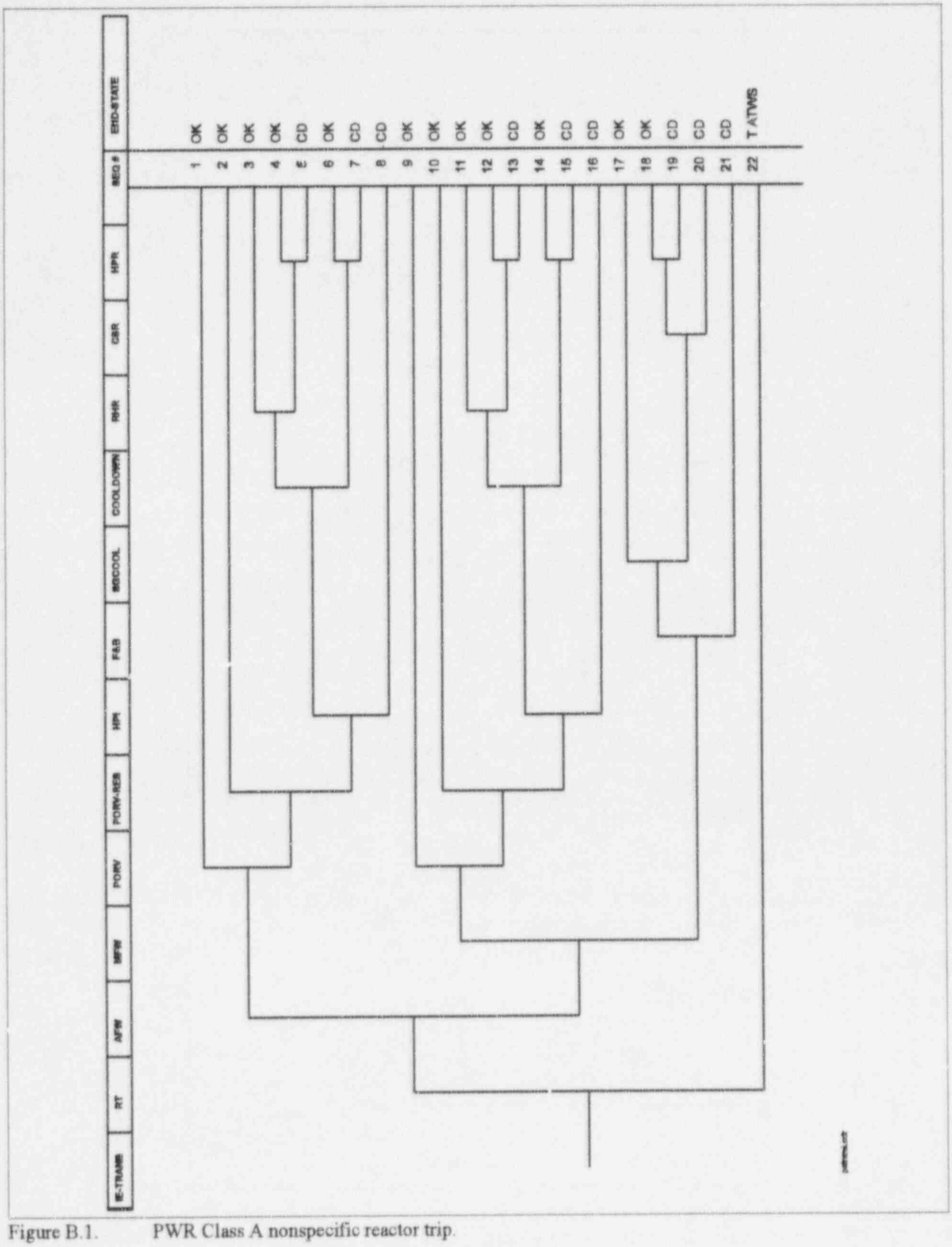


Figure B.1. PWR Class A nonspecific reactor trip.

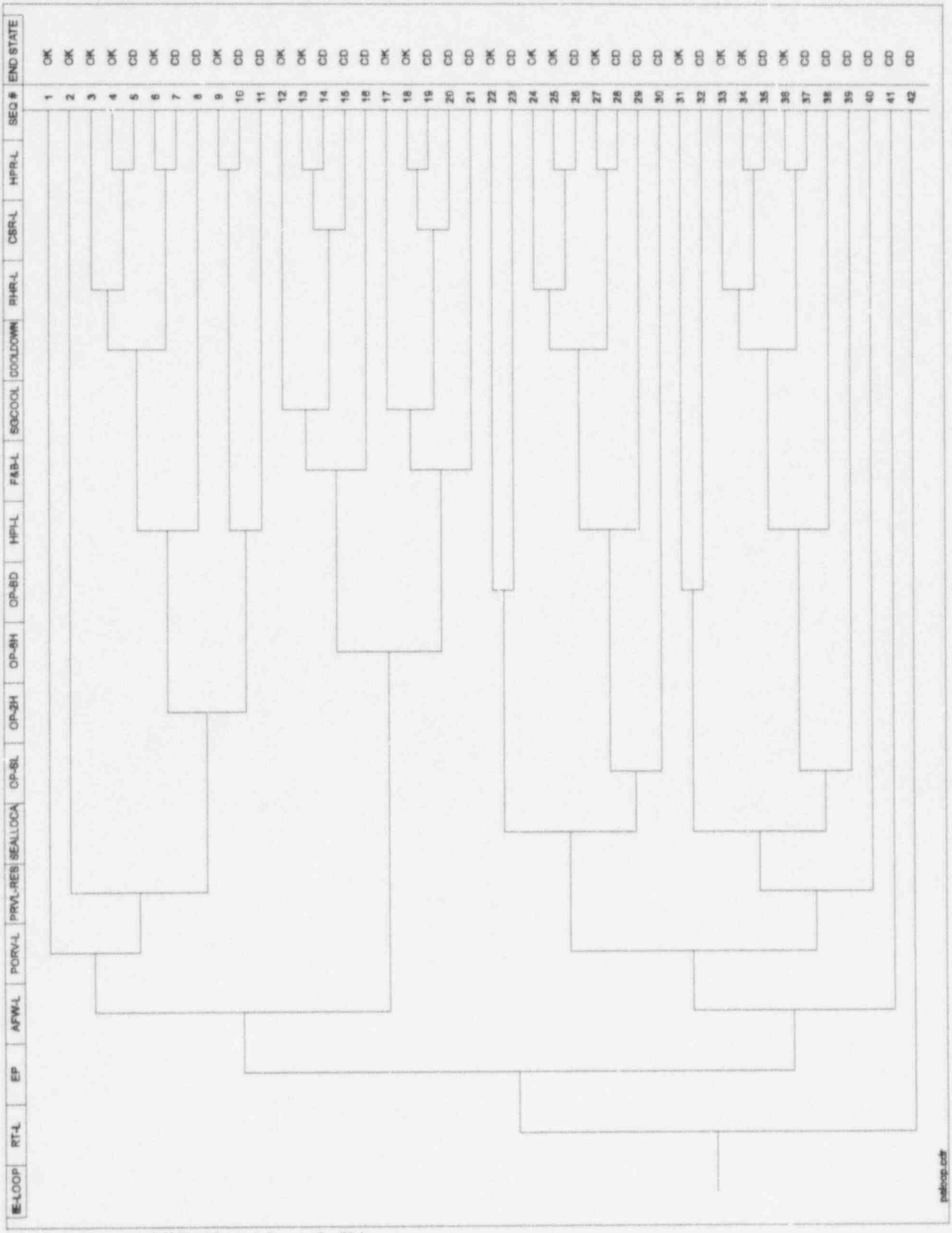


Figure B.2. PWR Class A loss-of-offsite power.

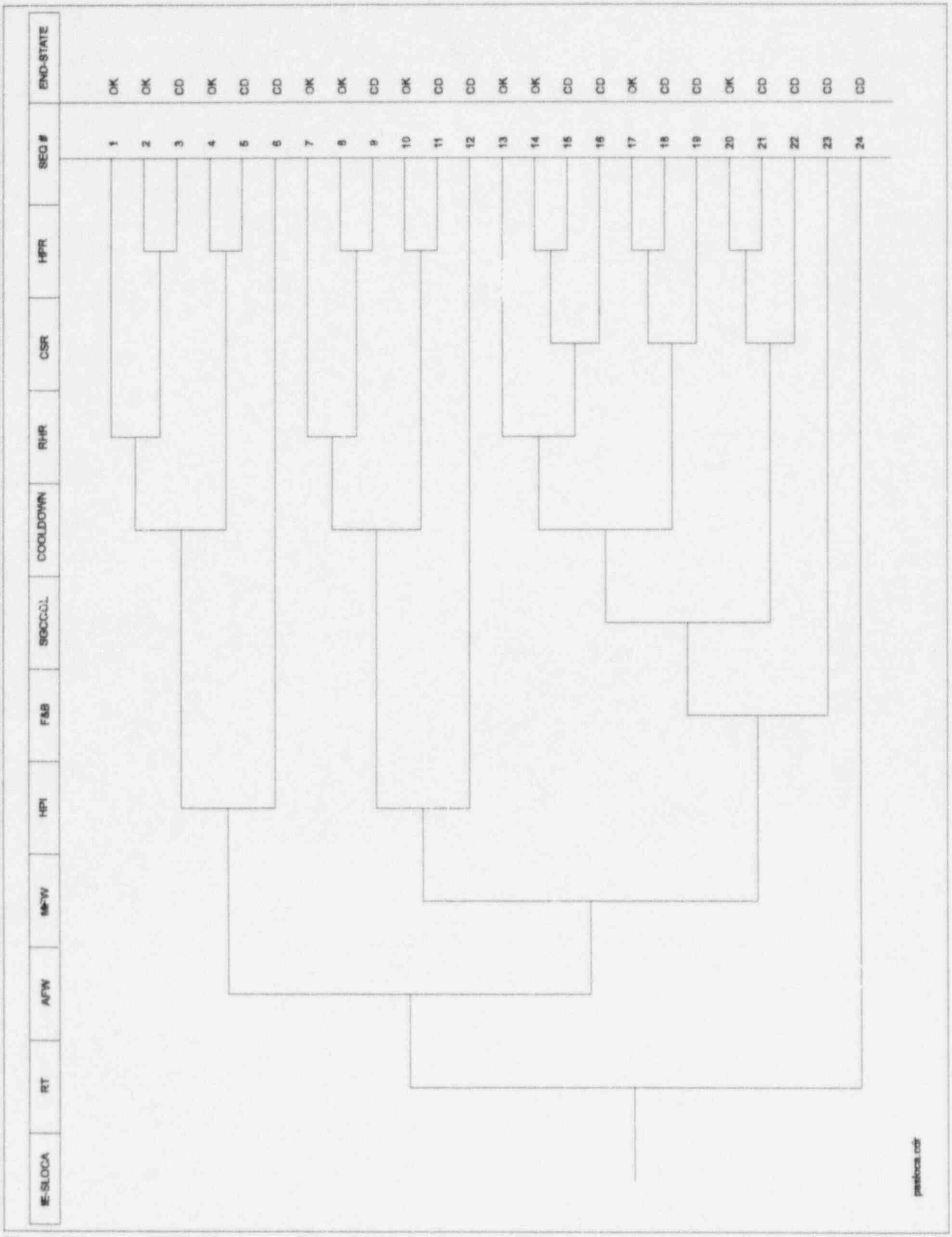


Figure B.3. PWR Class A small-break loss-of-coolant accident.

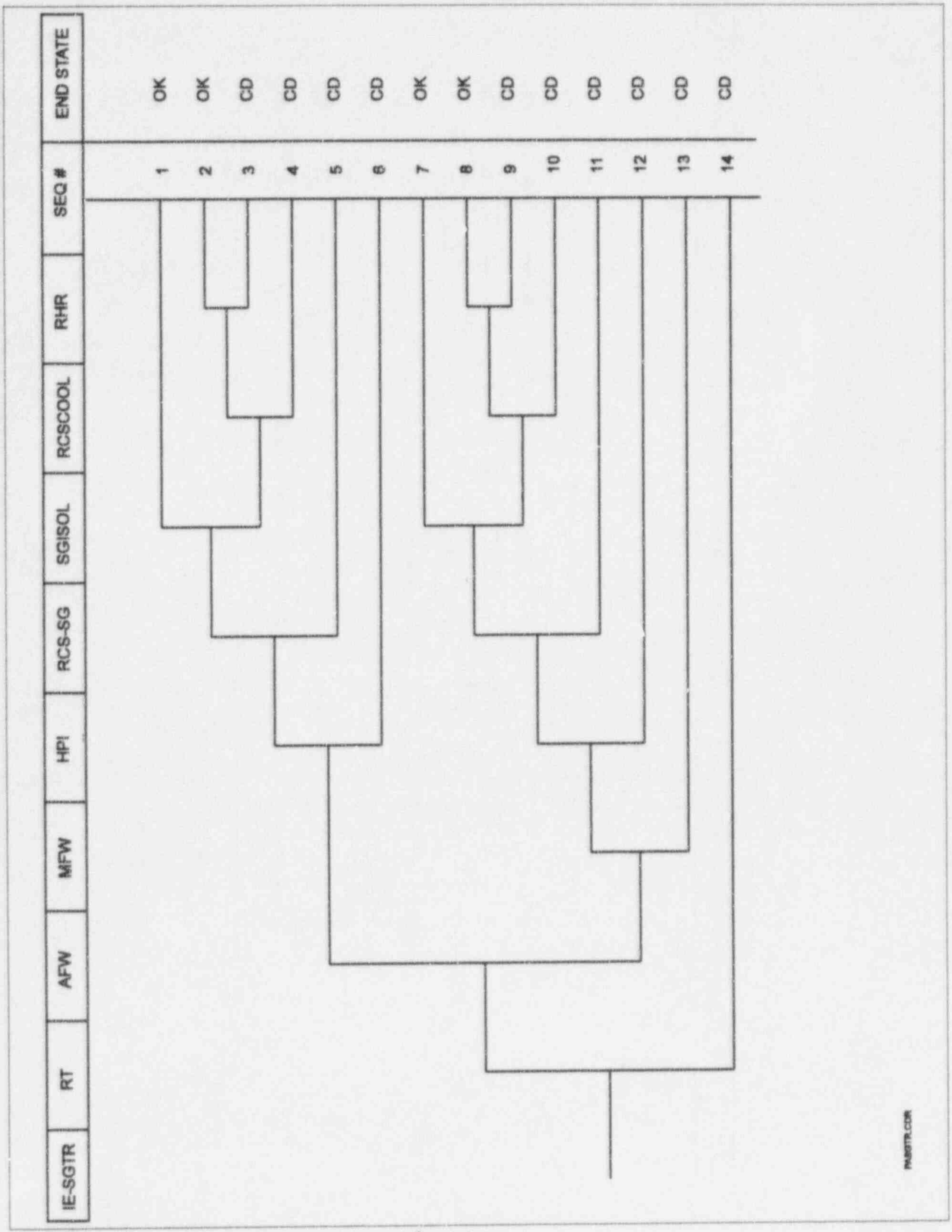


Figure B.4. PWR Class A steam generator tube rupture.

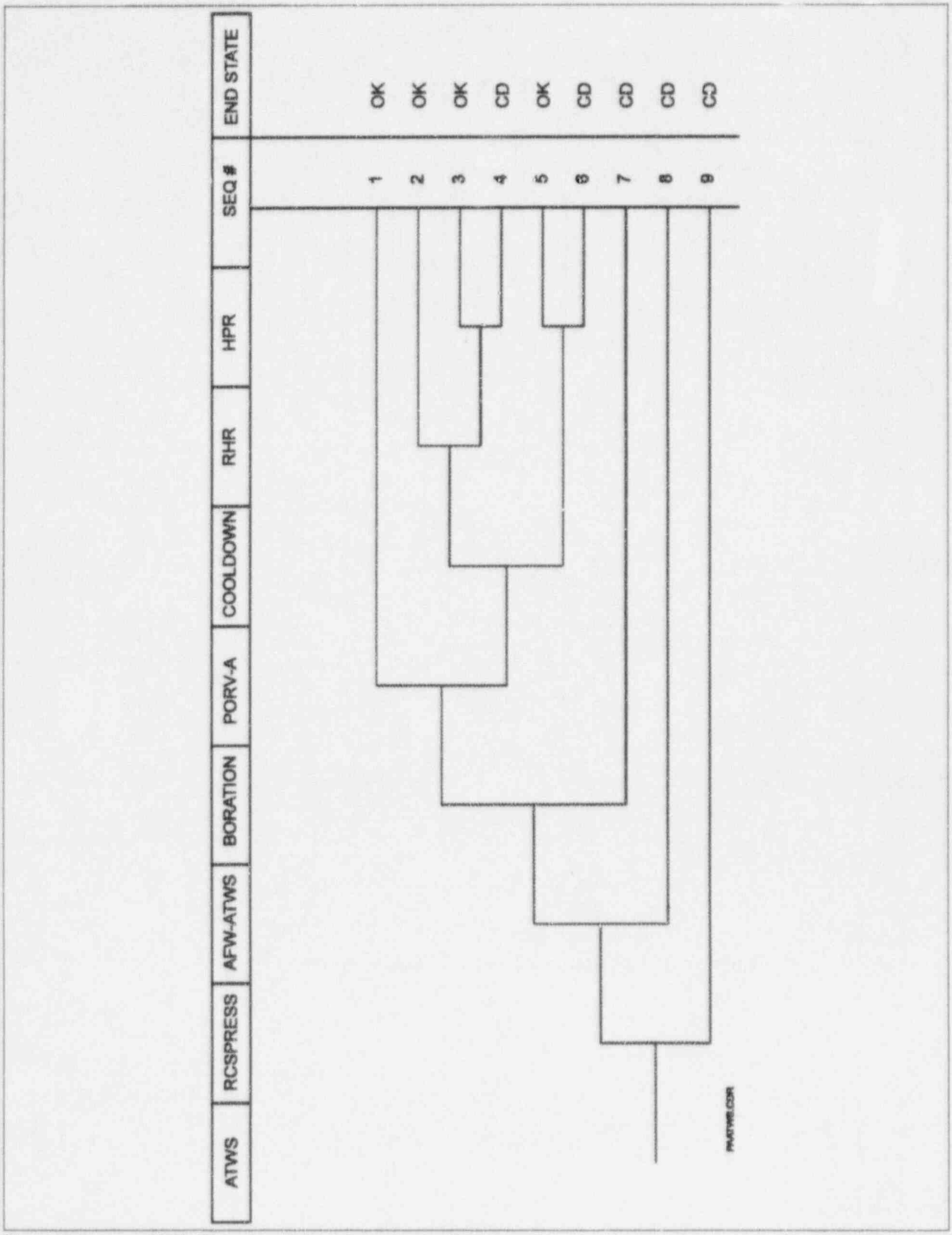


Figure B.5. PWR Class A anticipated transient without scram.

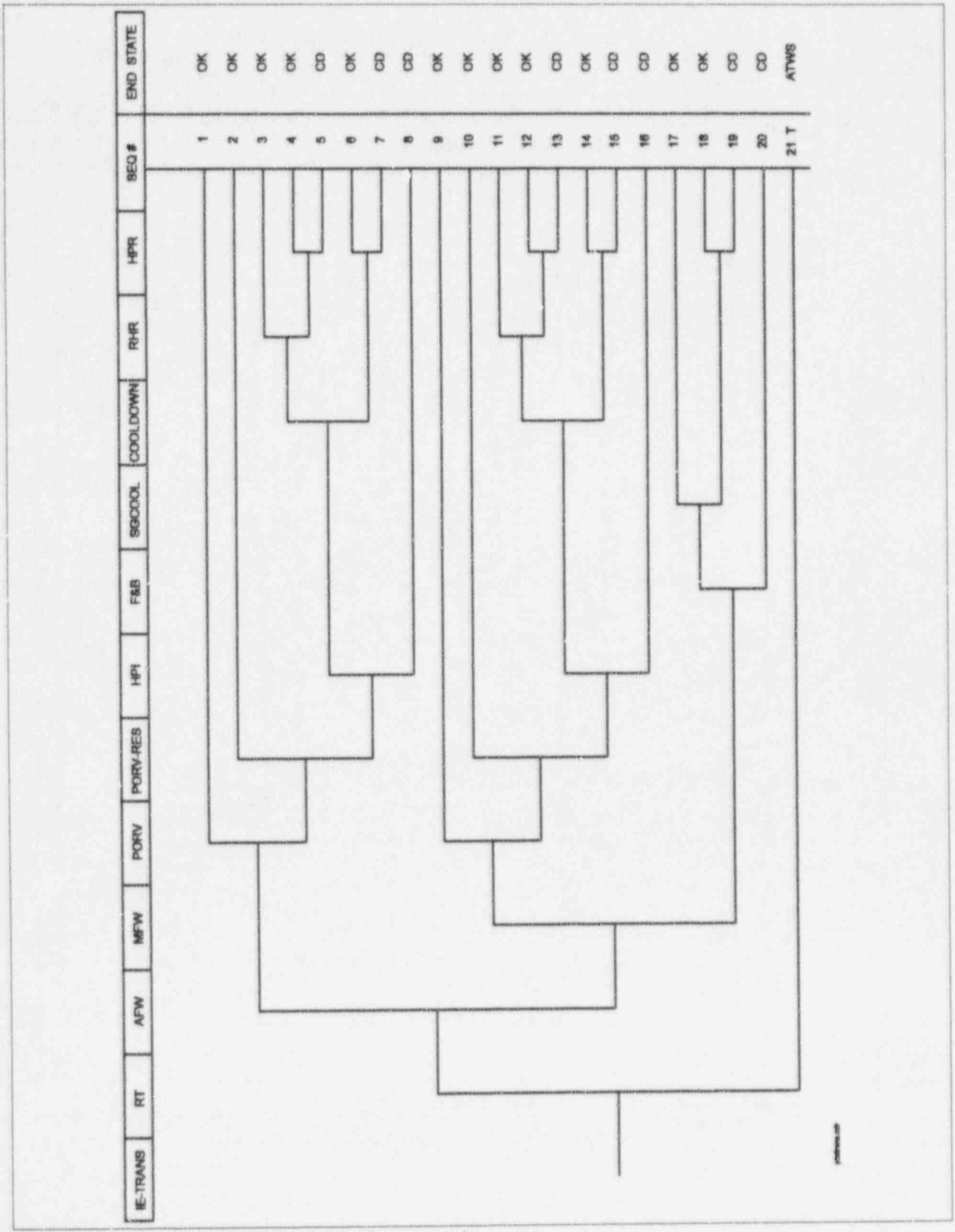


Figure B.6. Classes B and D nonspecific reactor trip.

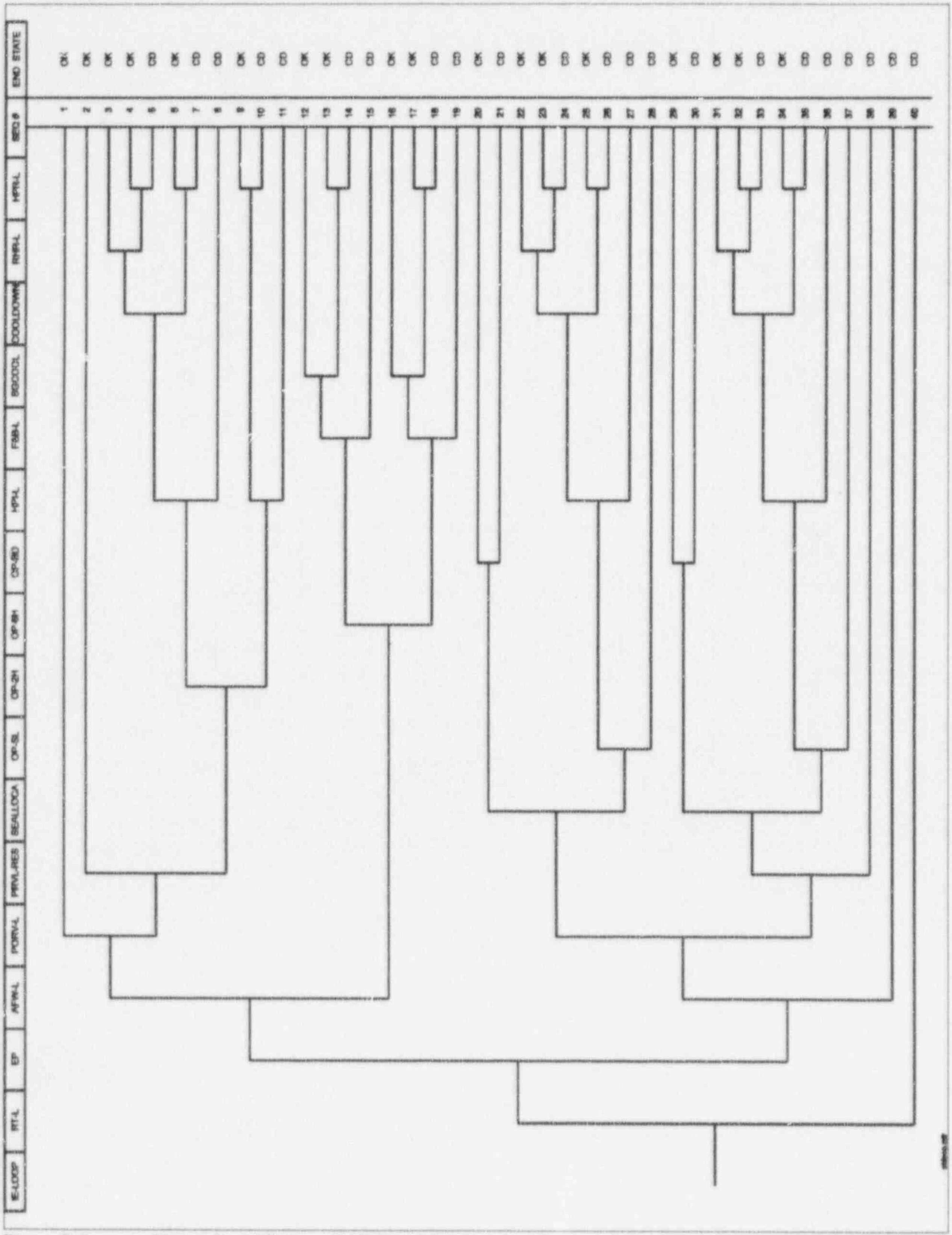


Figure B.7. Classes B and D loss-of-offsite power.

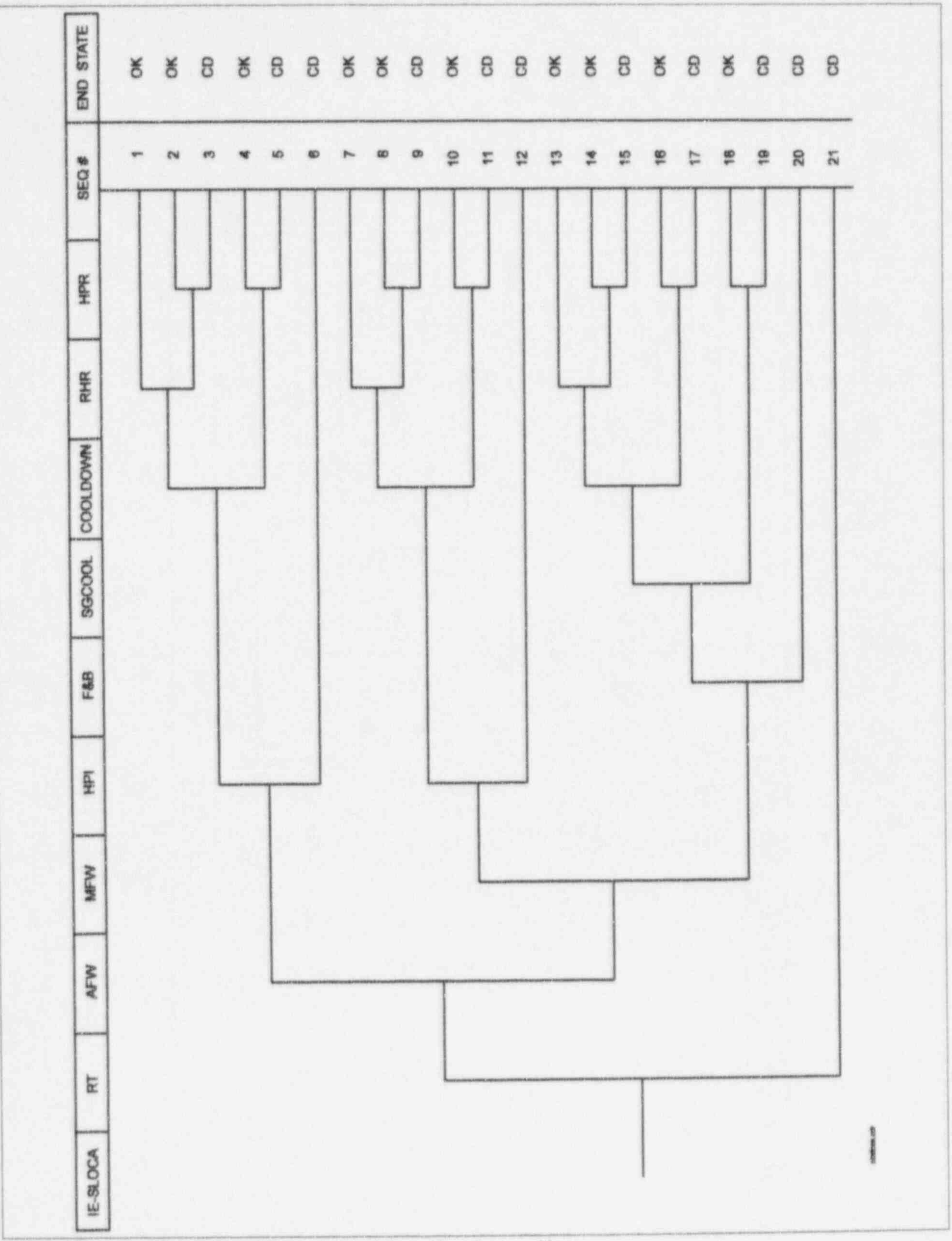


Figure B.8. Classes B and D small-break loss-of-coolant accident.

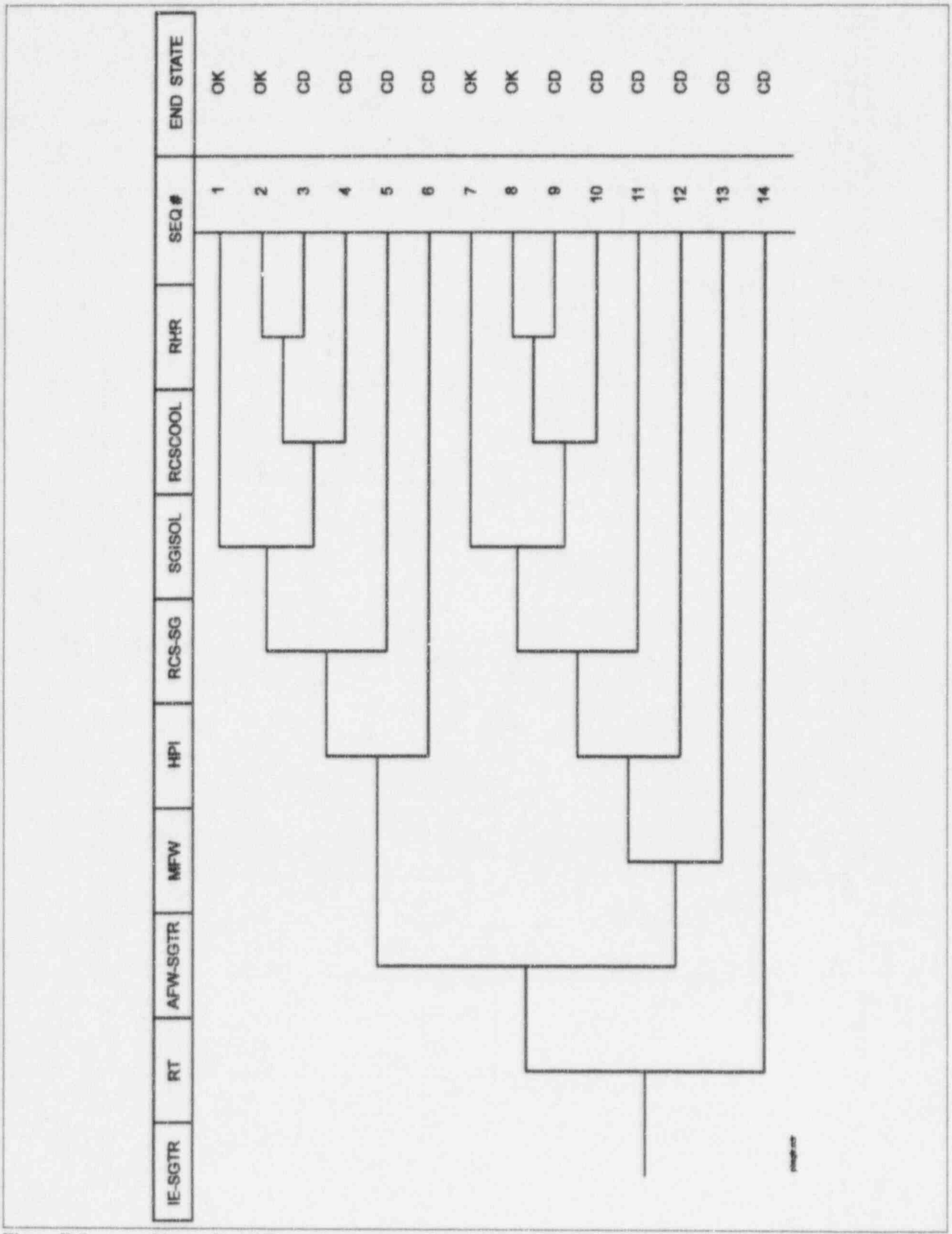


Figure B.9. Classes B and D steam generator tube rupture.

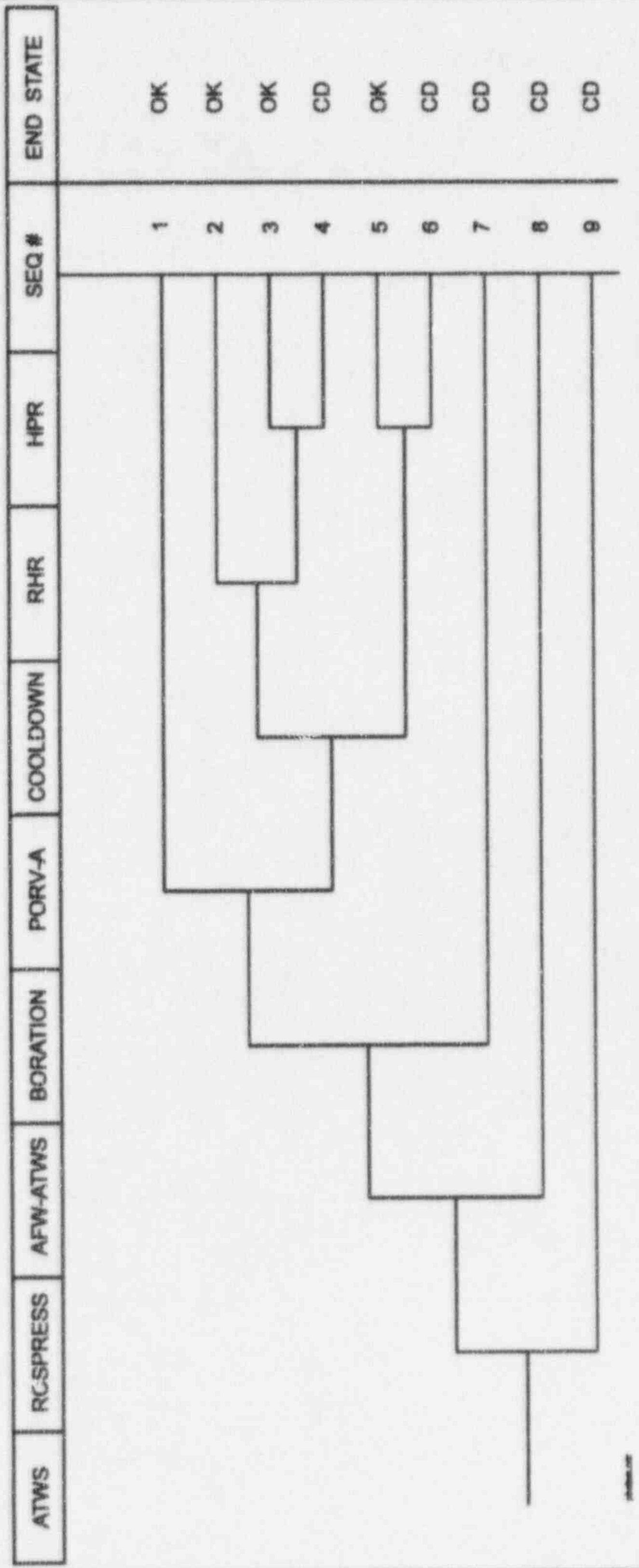


Figure B.10. Classes B and D anticipated transient without scram.

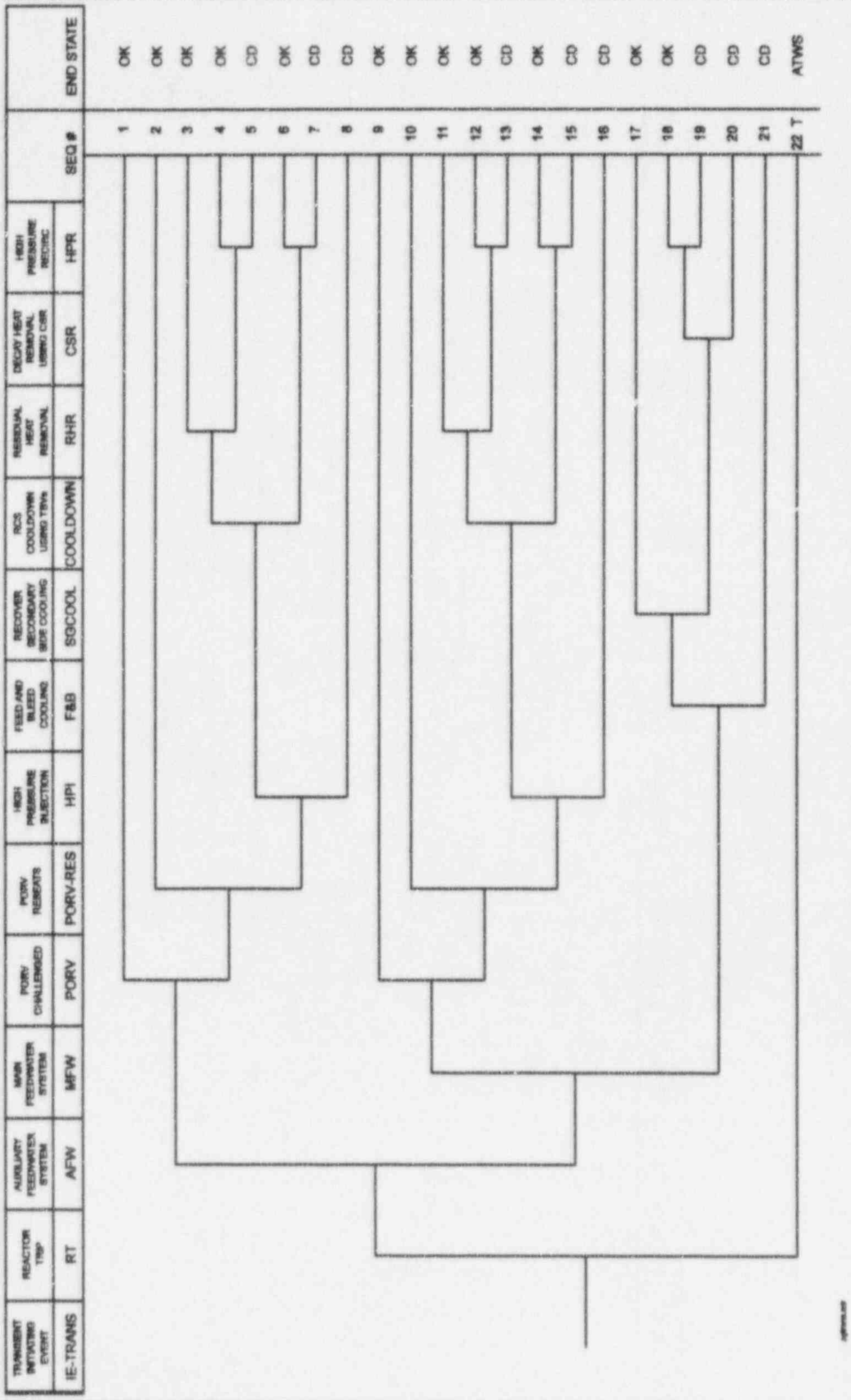


Figure B.11. PWR Class G nonspecific reactor trip.

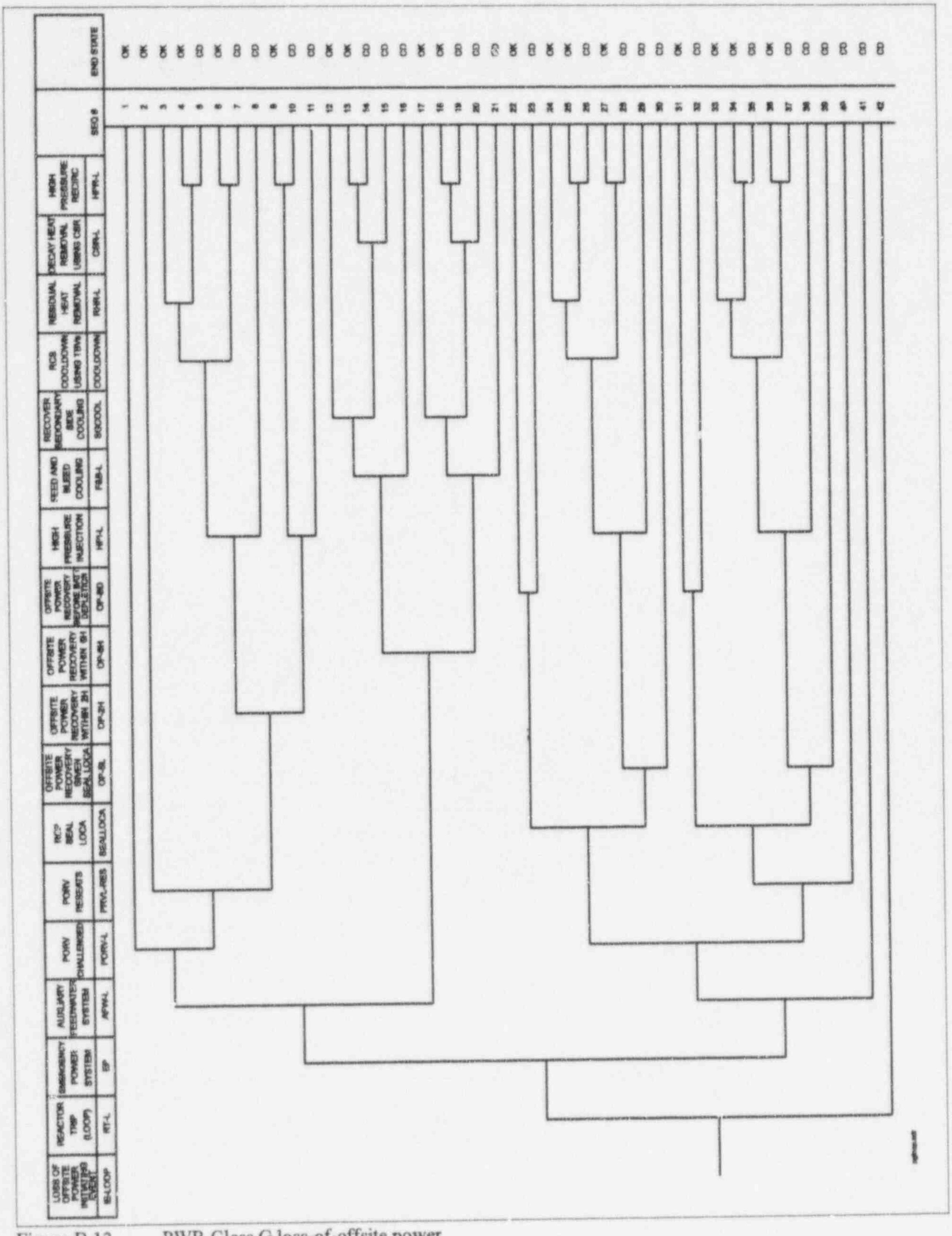


Figure B.12. PWR Class G loss-of-offsite power.

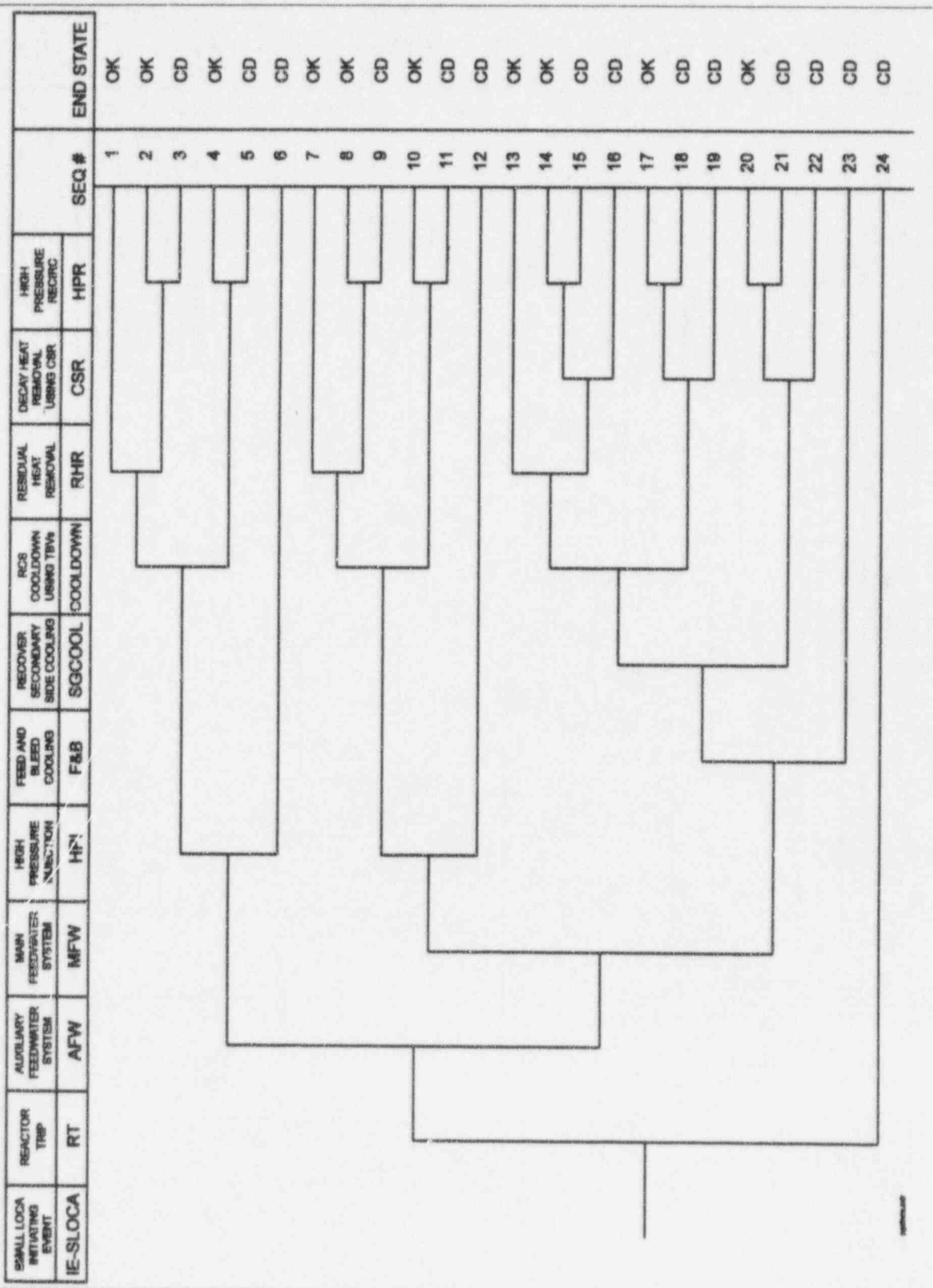


Figure B.13. PWR Class G small-break loss-of-coolant accident.

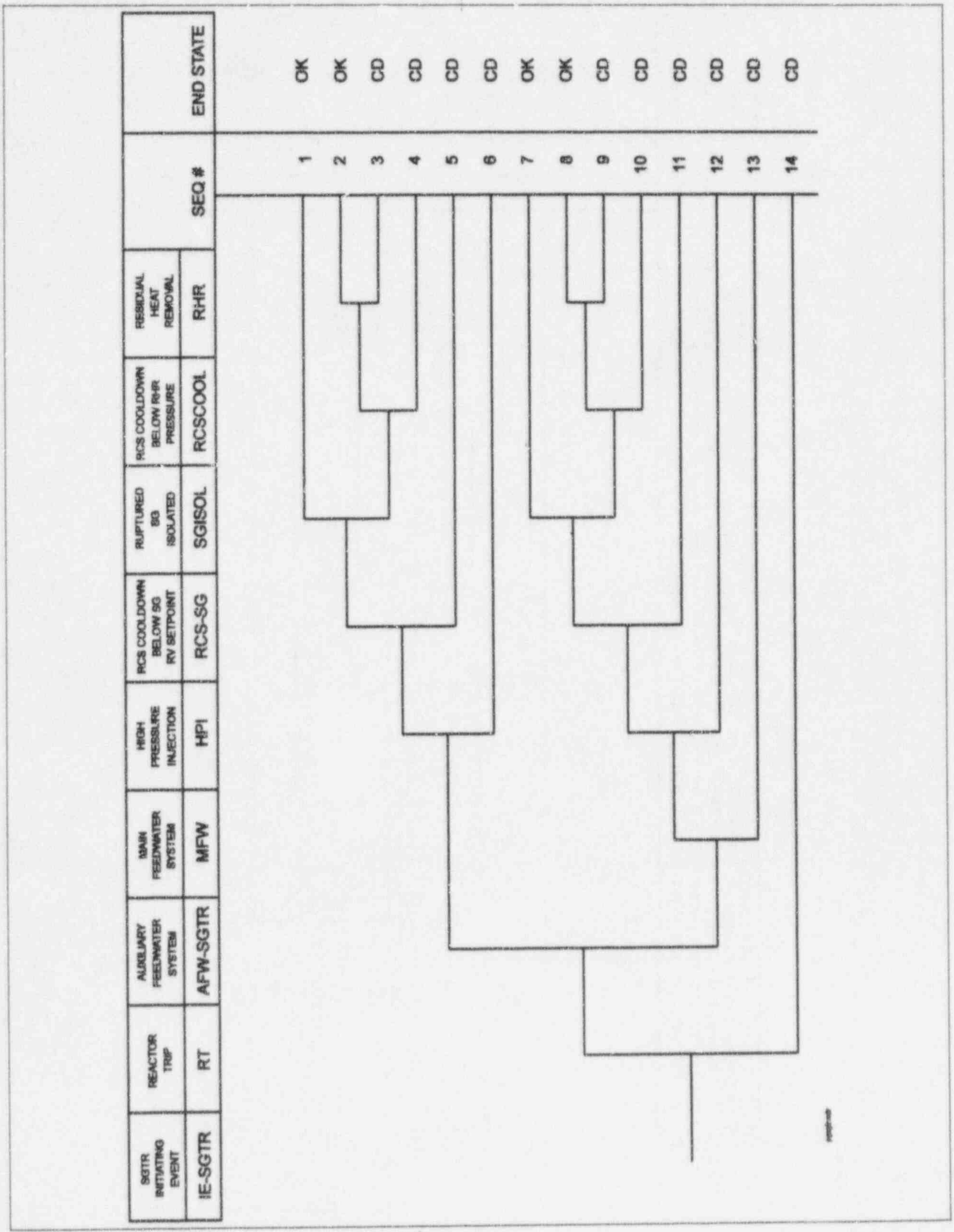


Figure B.14. PWR Class G steam generator tube rupture.

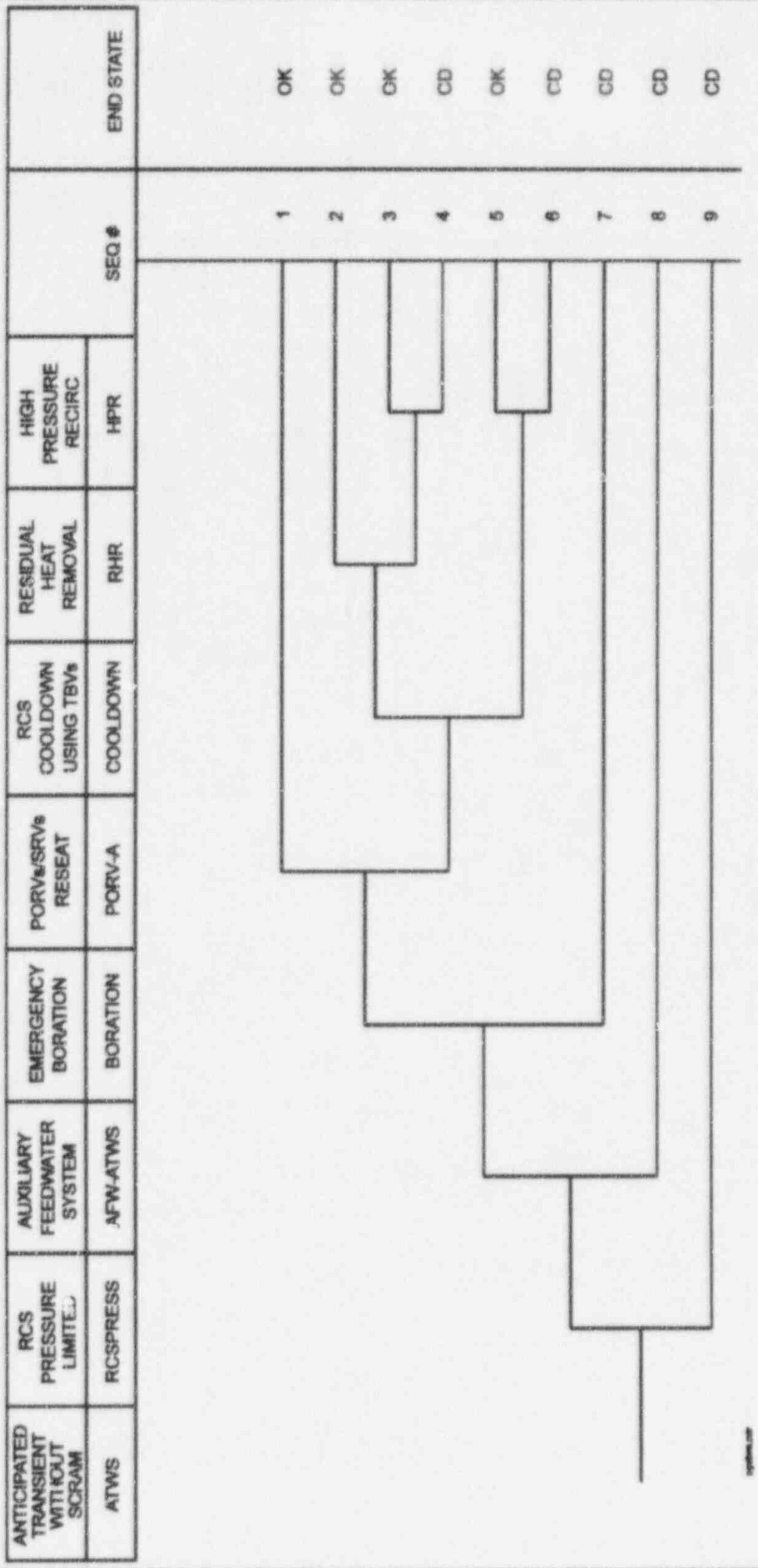


Figure B.15. PWR Class G anticipated transient without scram.

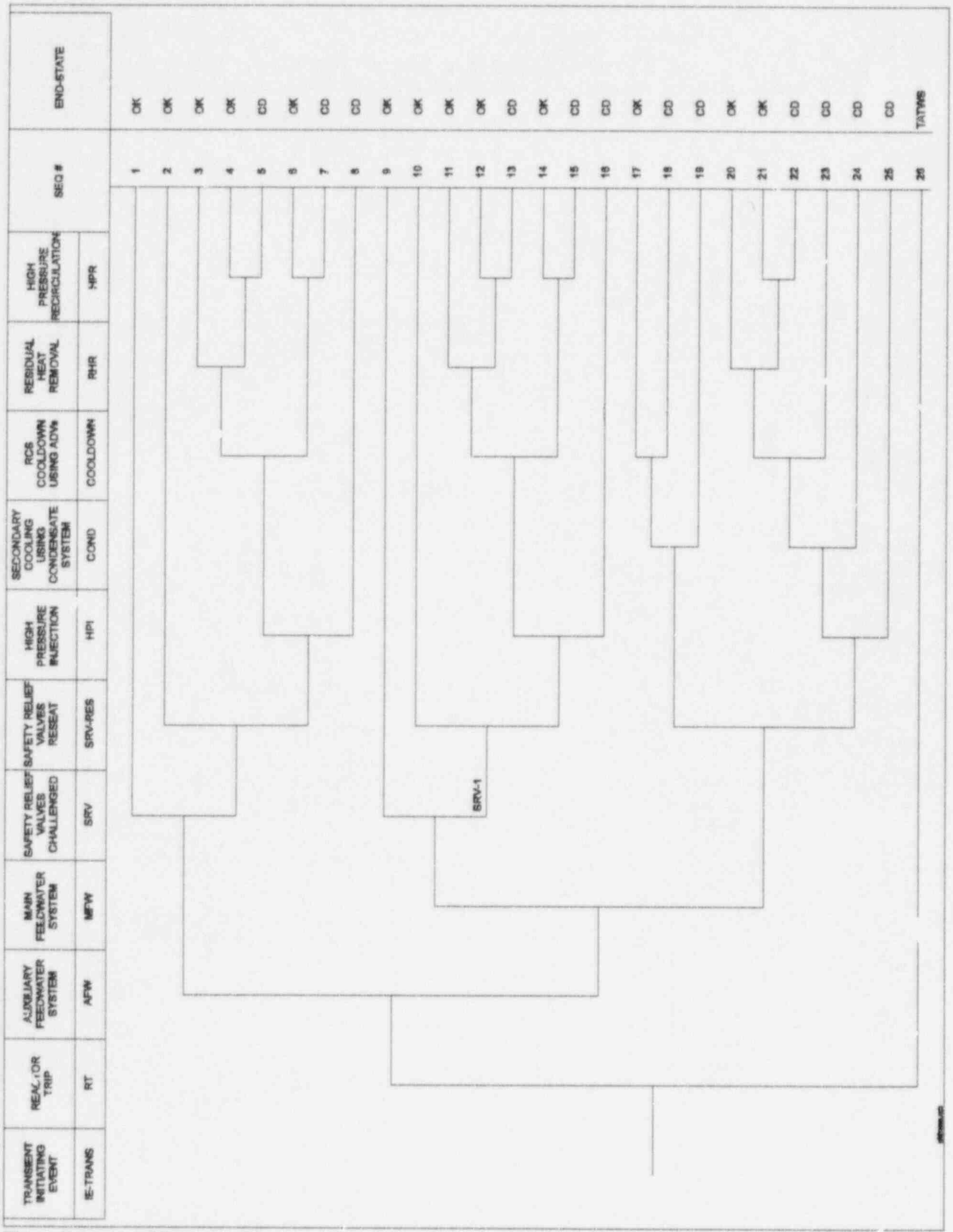


Figure B.16. PWR Class H nonspecific reactor trip.

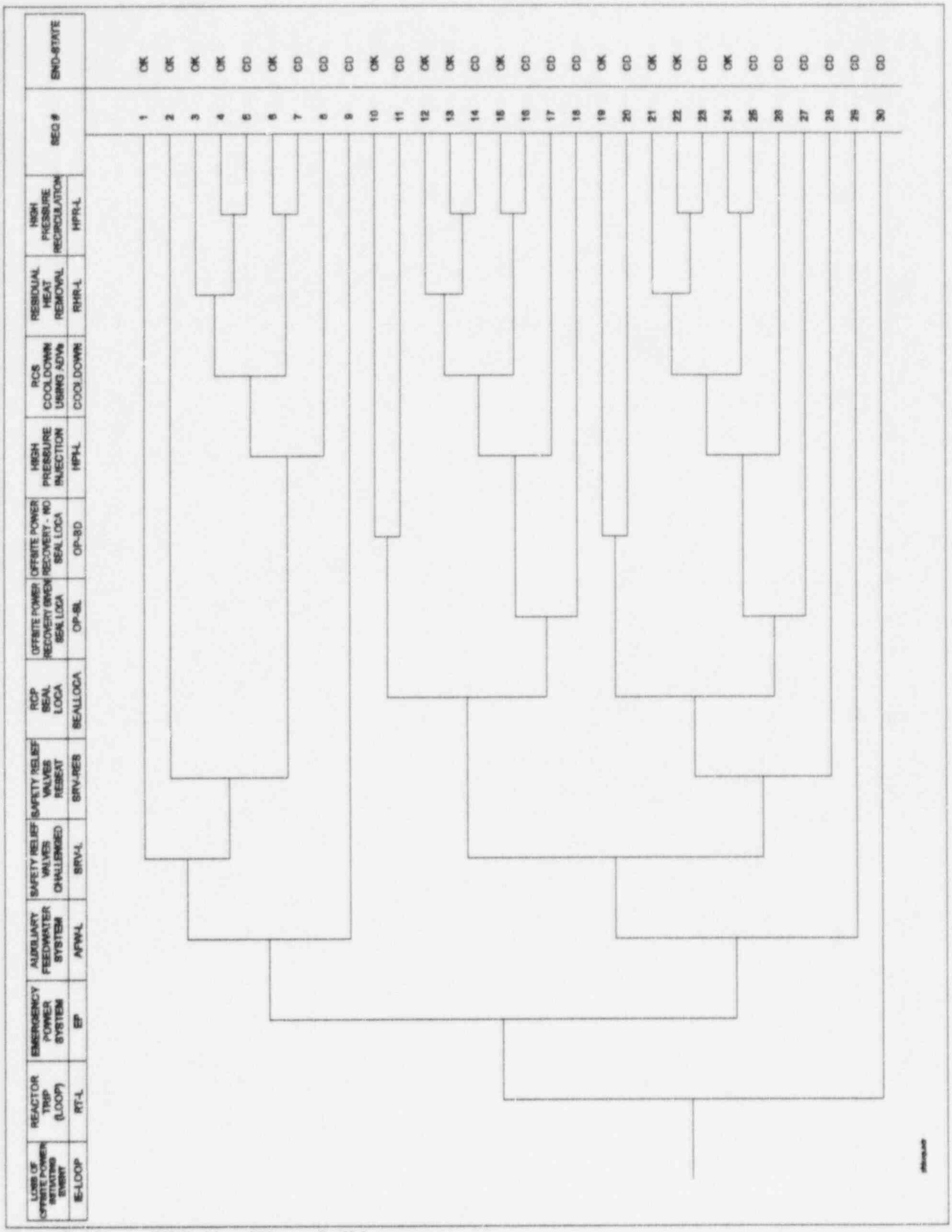


Figure B.17. PWR Class H loss-of-offsite power.

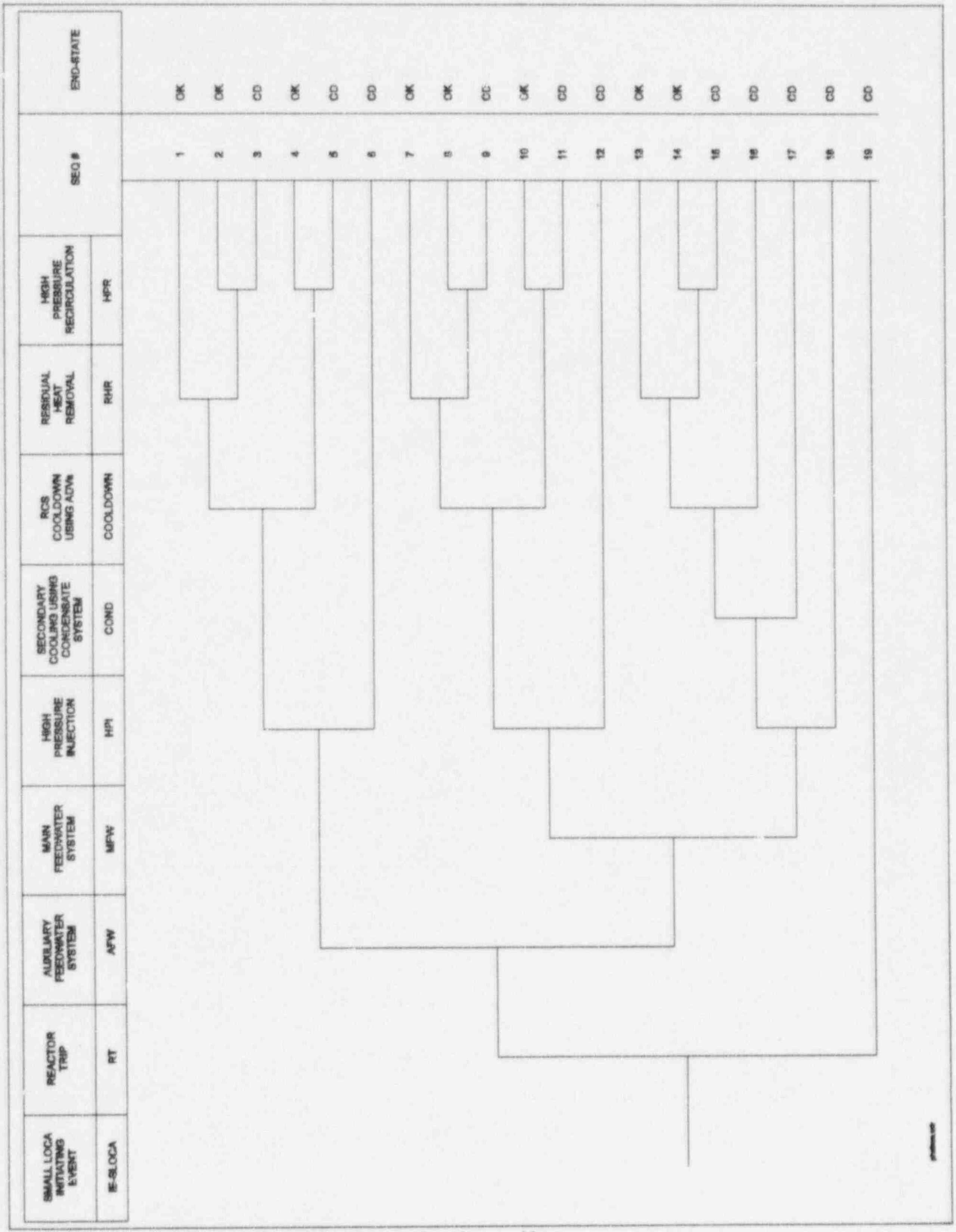


Figure B.18. PWR Class H small-break loss-of-coolant accident.

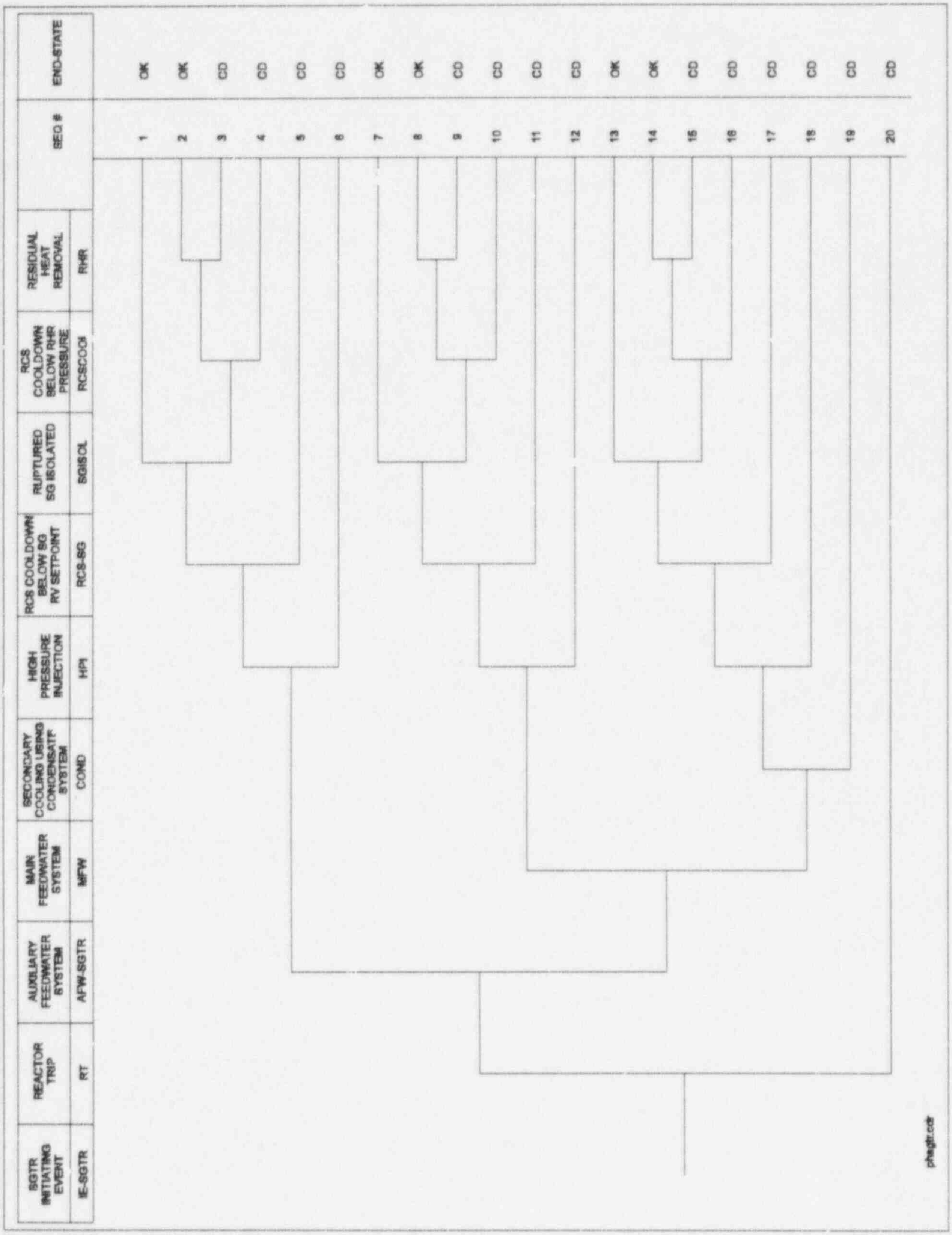


Figure B.19. PWR Class H steam generator tube rupture.

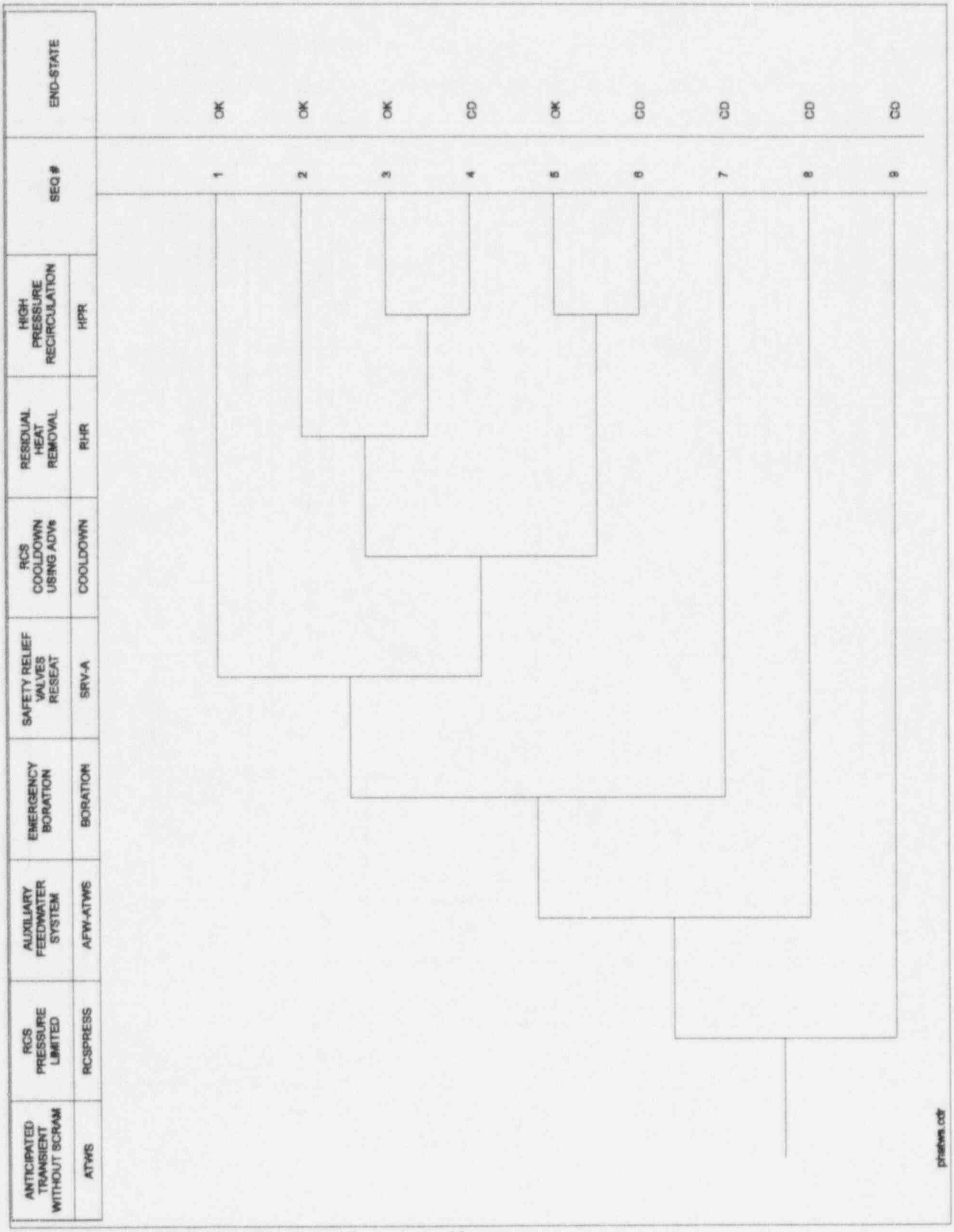


Figure B.20. PWR Class H anticipated transient without scram.

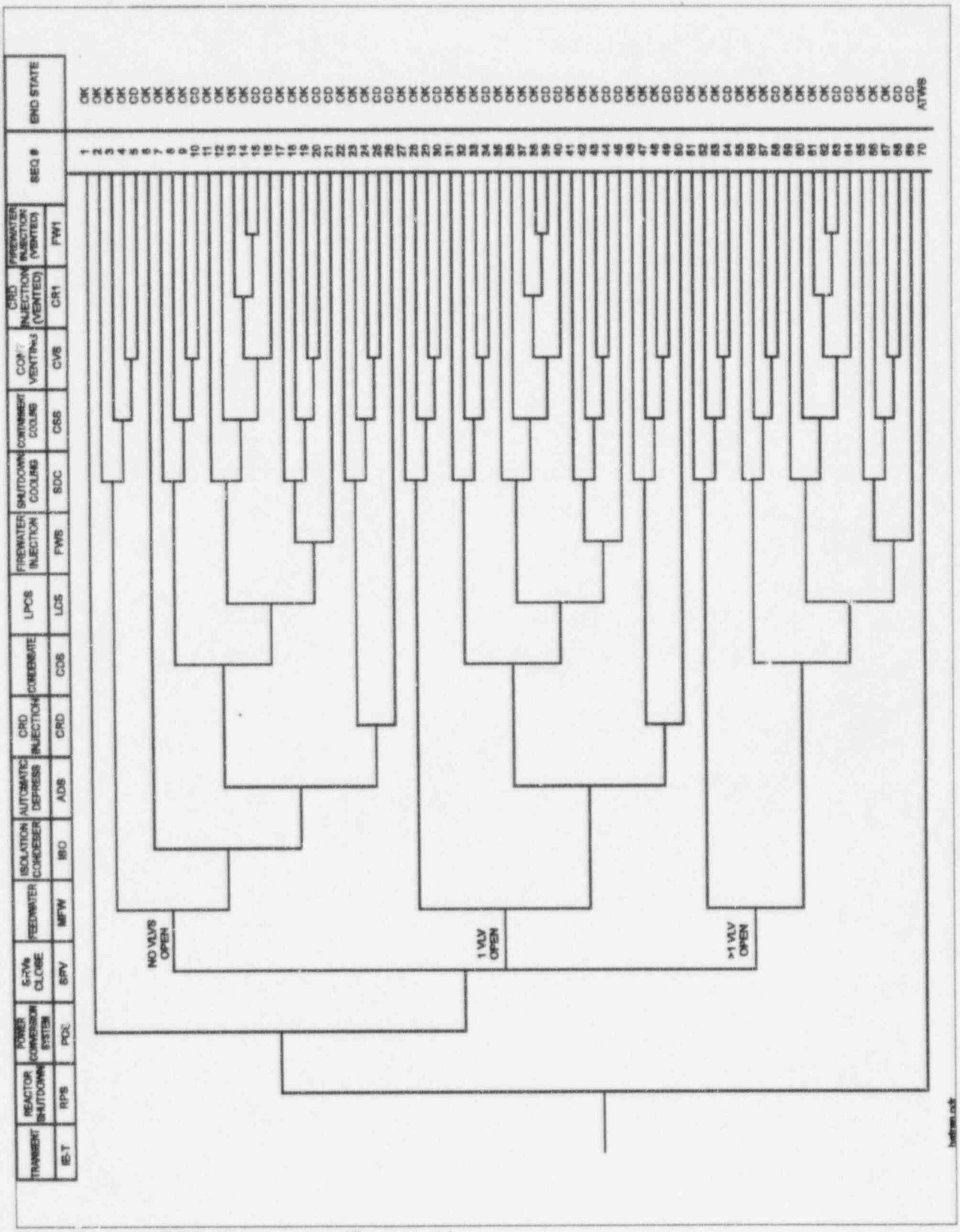


Figure B.21. BWR Class A nonspecific reactor trip.

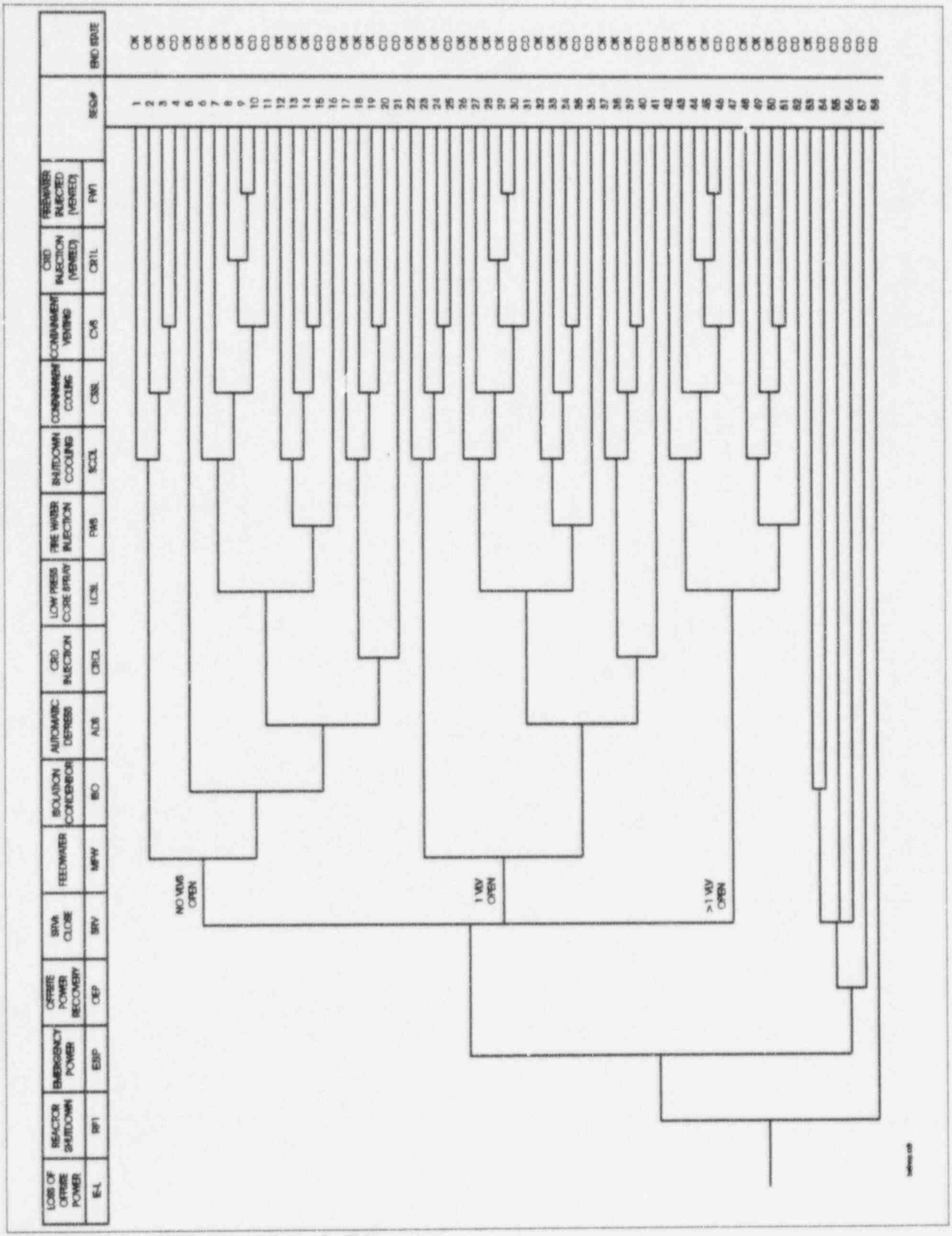


Figure B.22. BWR Class A loss-of-offsite power.

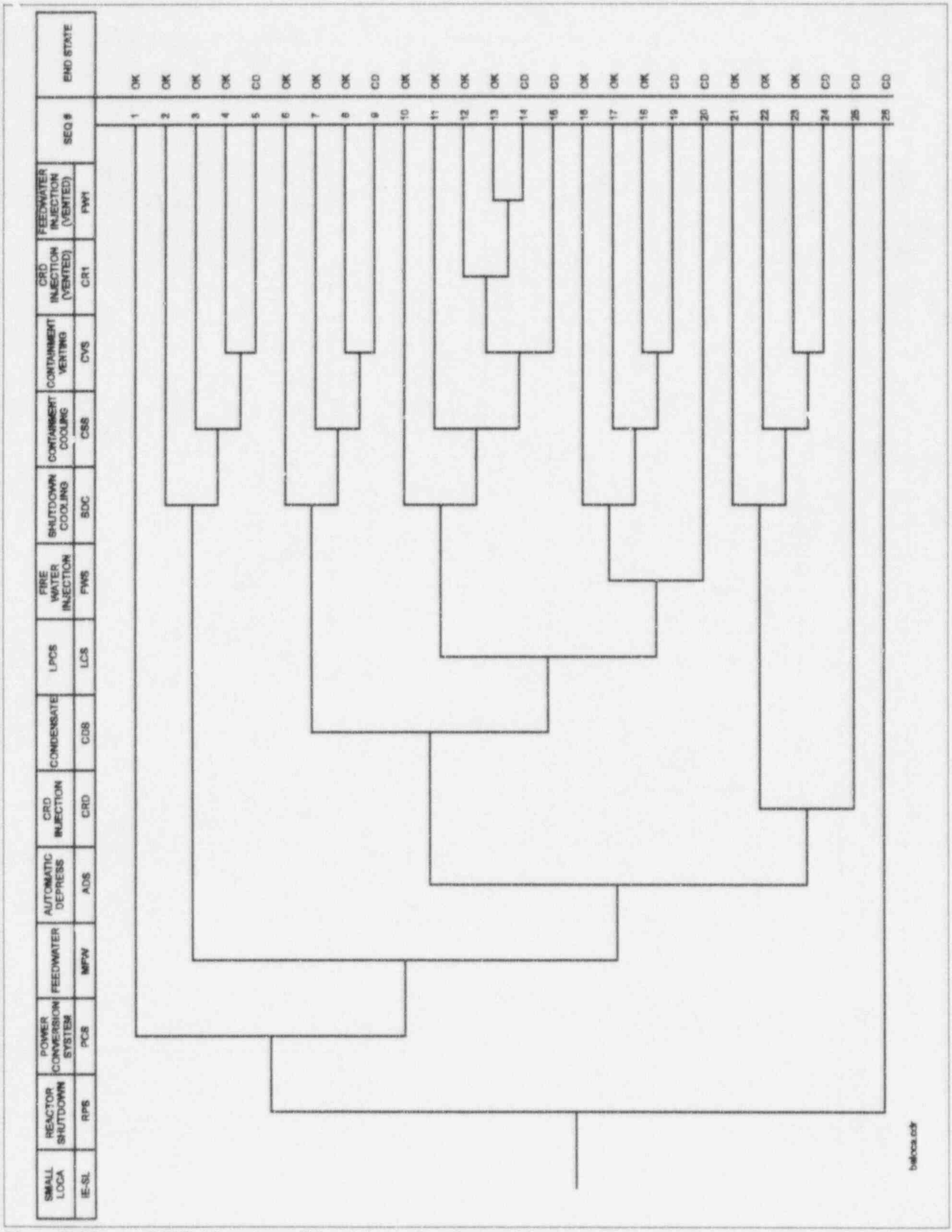


Figure B.23. BWR Class A small-break loss-of-coolant accident.

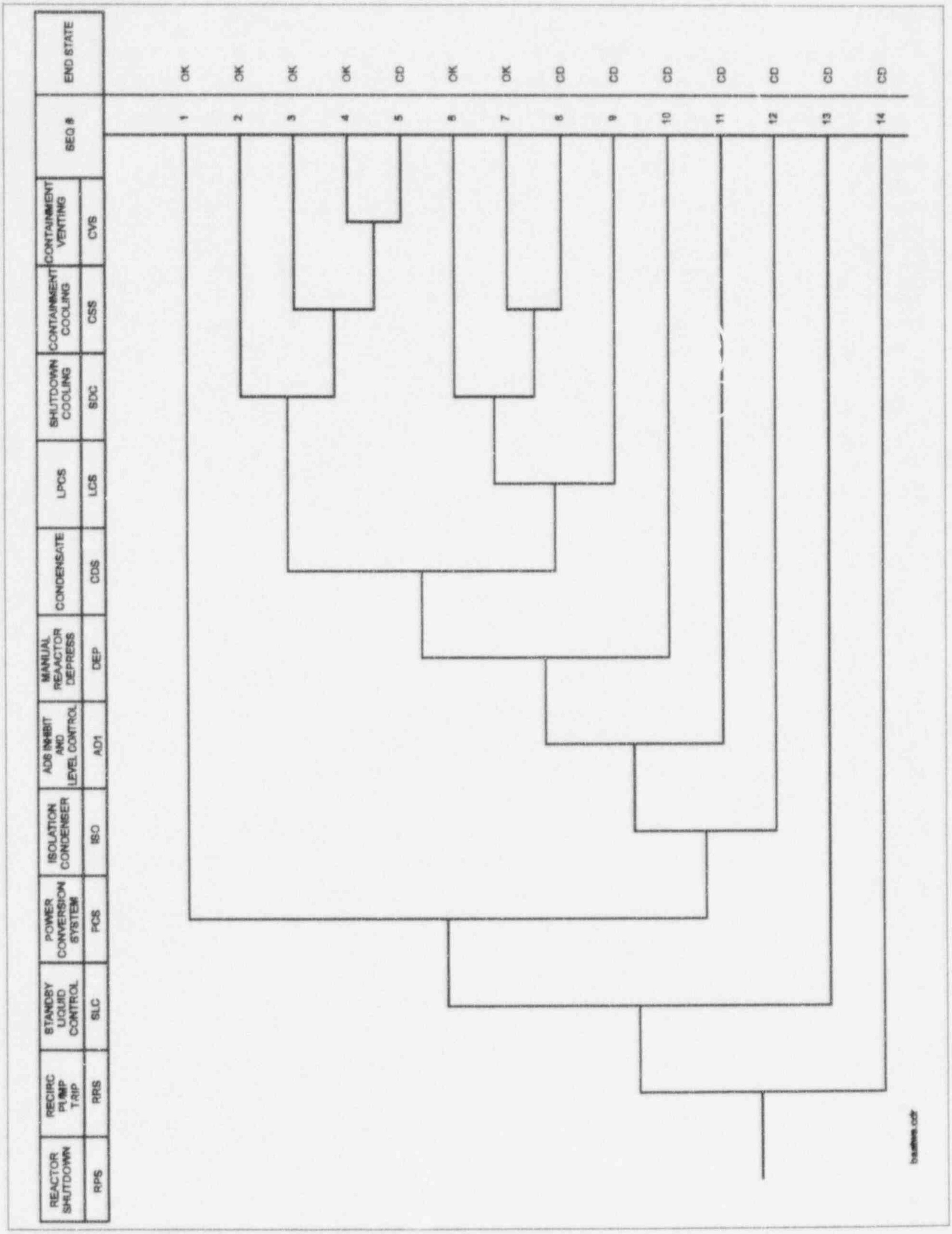


Figure B.24. BWR Class A anticipated transient without scram.

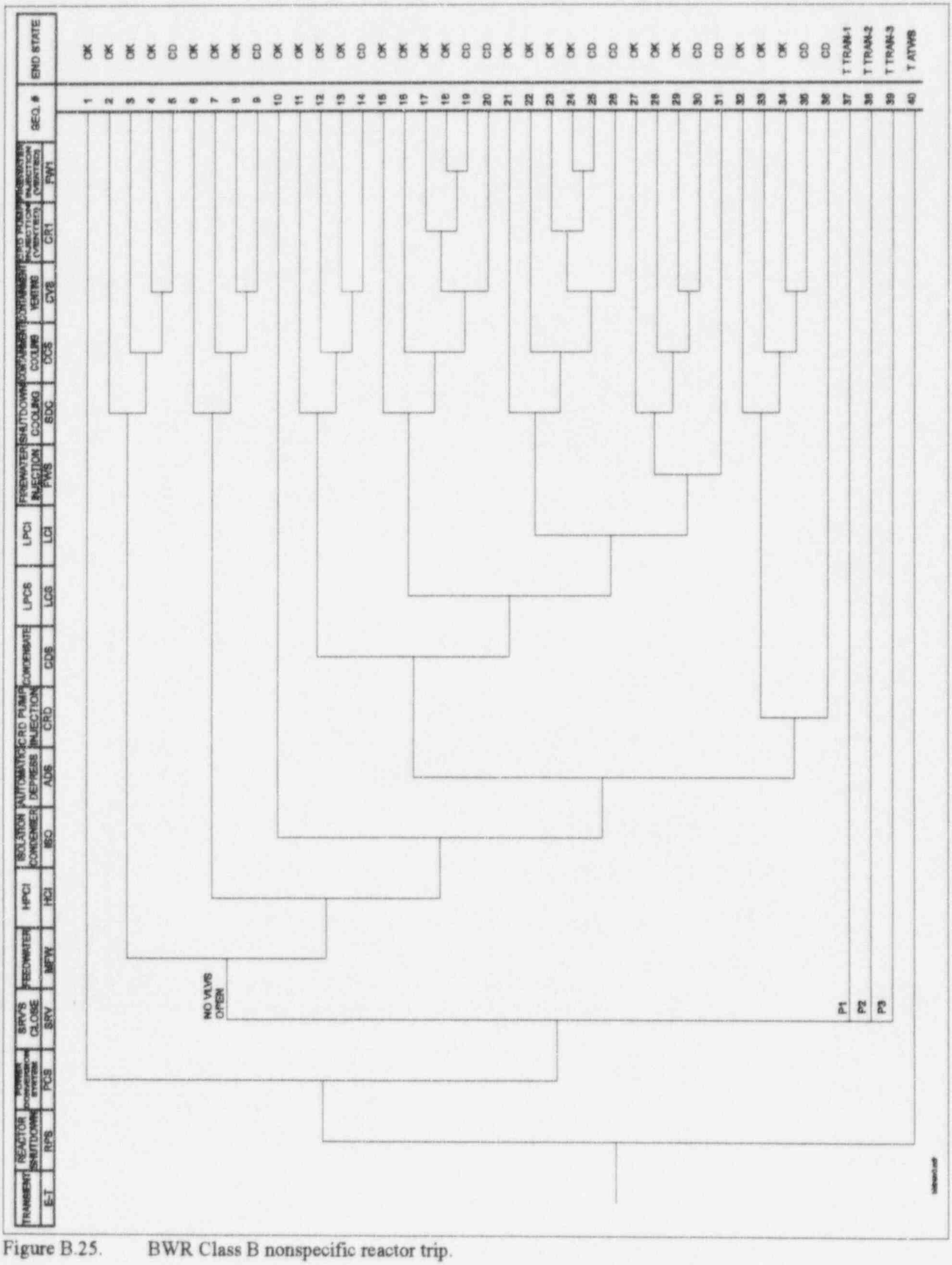


Figure B.25. BWR Class B nonspecific reactor trip.

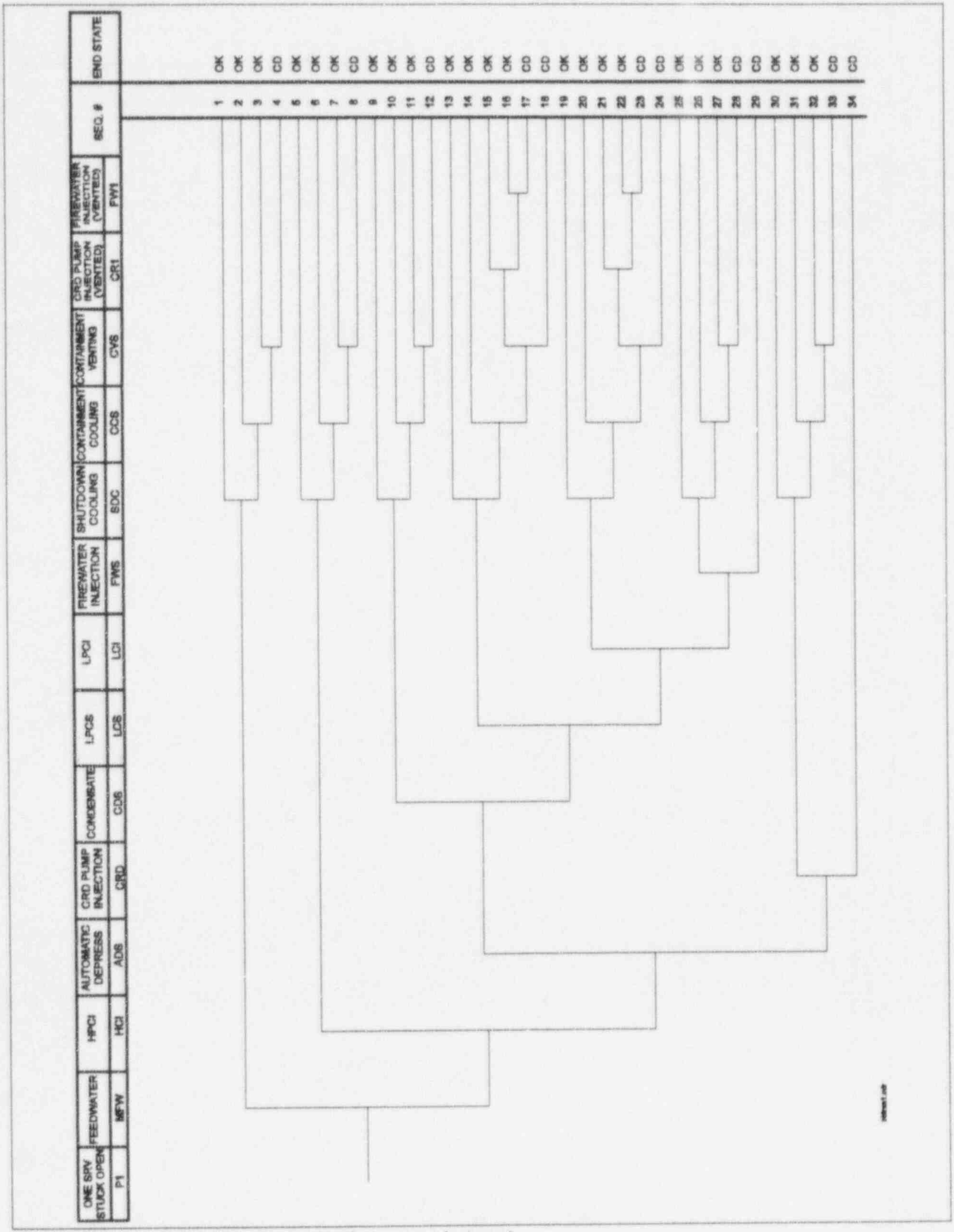


Figure B.26. BWR Class B nonspecific reactor trip (cont.).

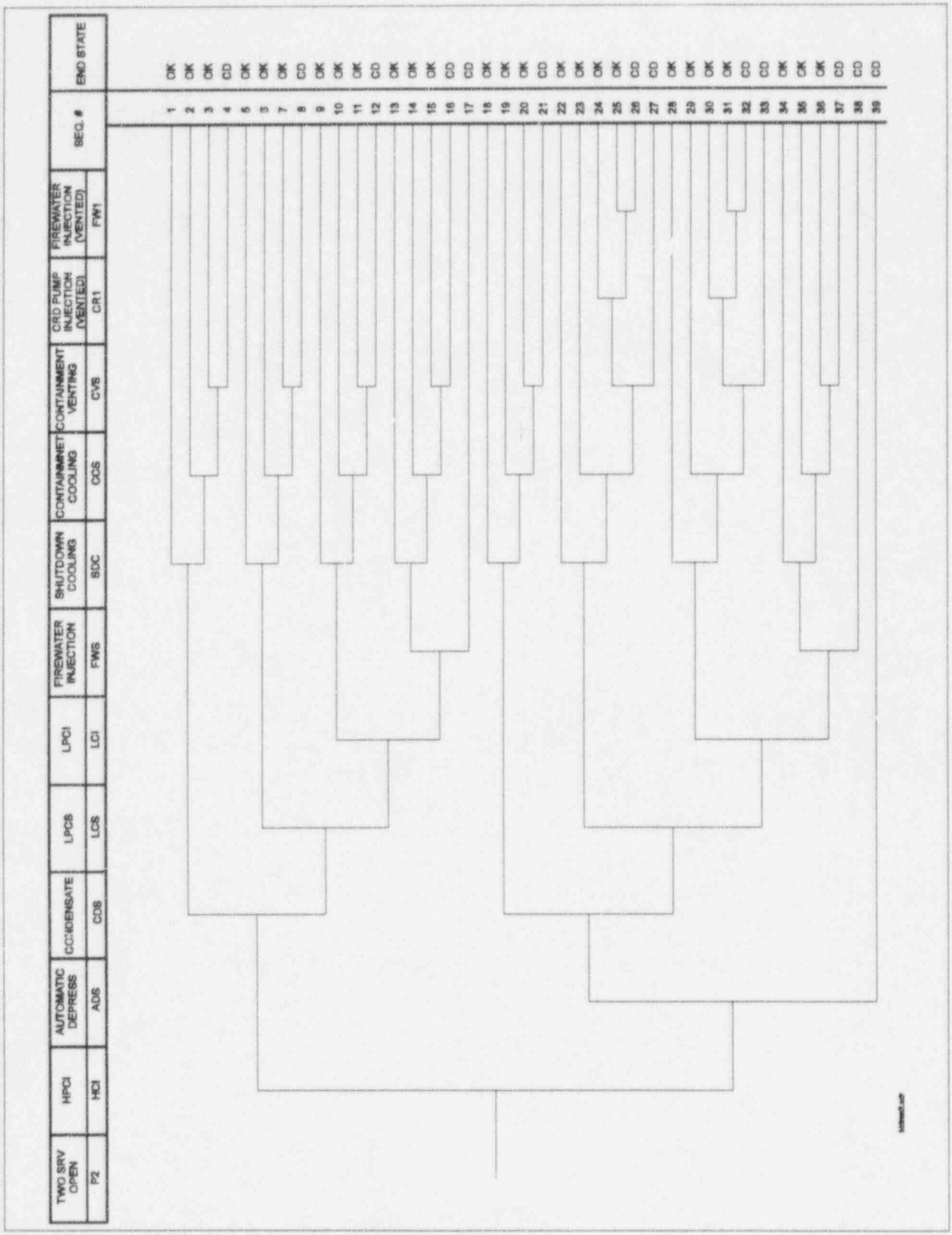


Figure B.27. BWR Class B nonspecific reactor trip (cont.).

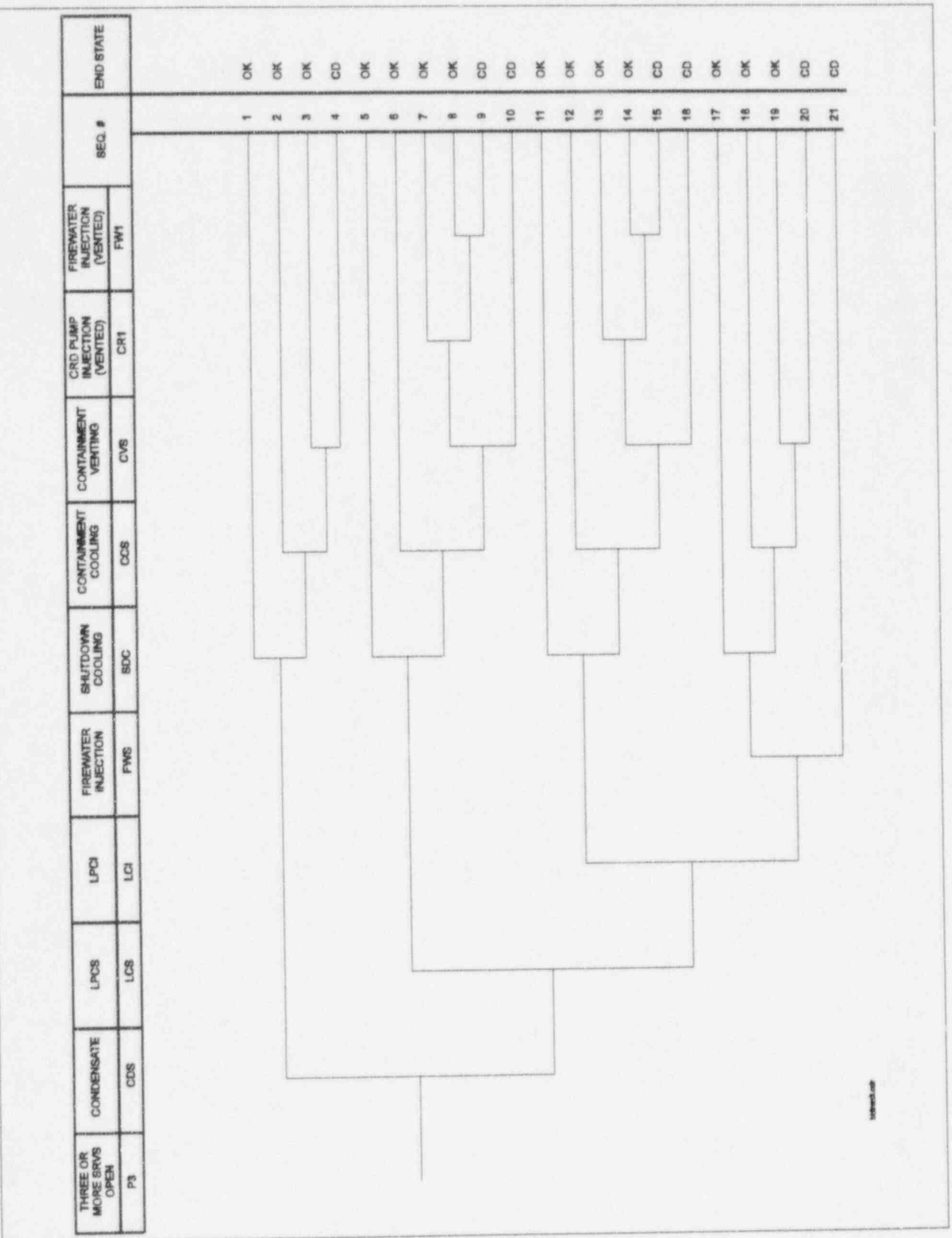


Figure B.28. BWR Class B nonspecific reactor trip (cont.).

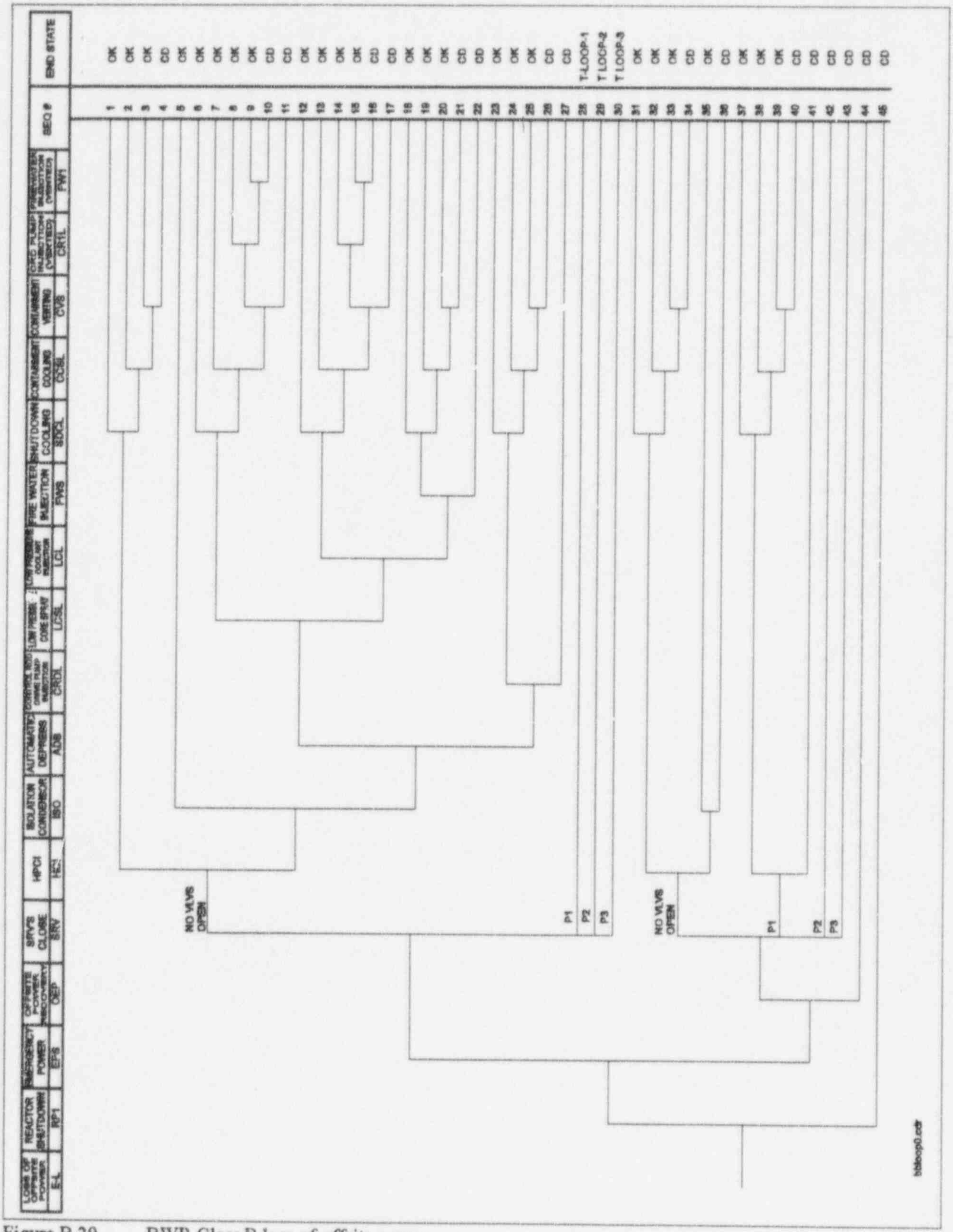


Figure B.29. BWR Class B loss-of-offsite power.

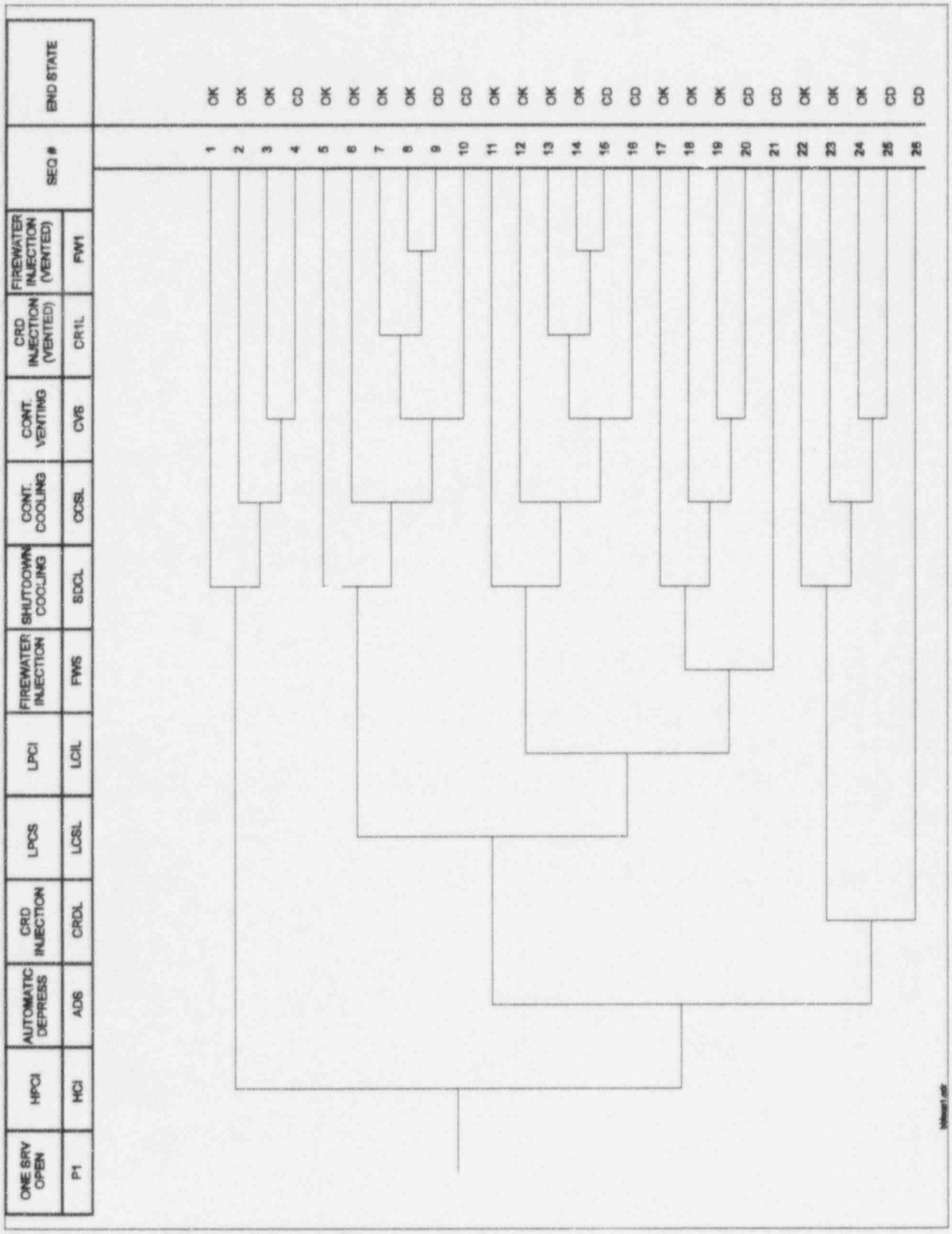


Figure B.30. BWR Class B loss-of-offsite power (cont.).

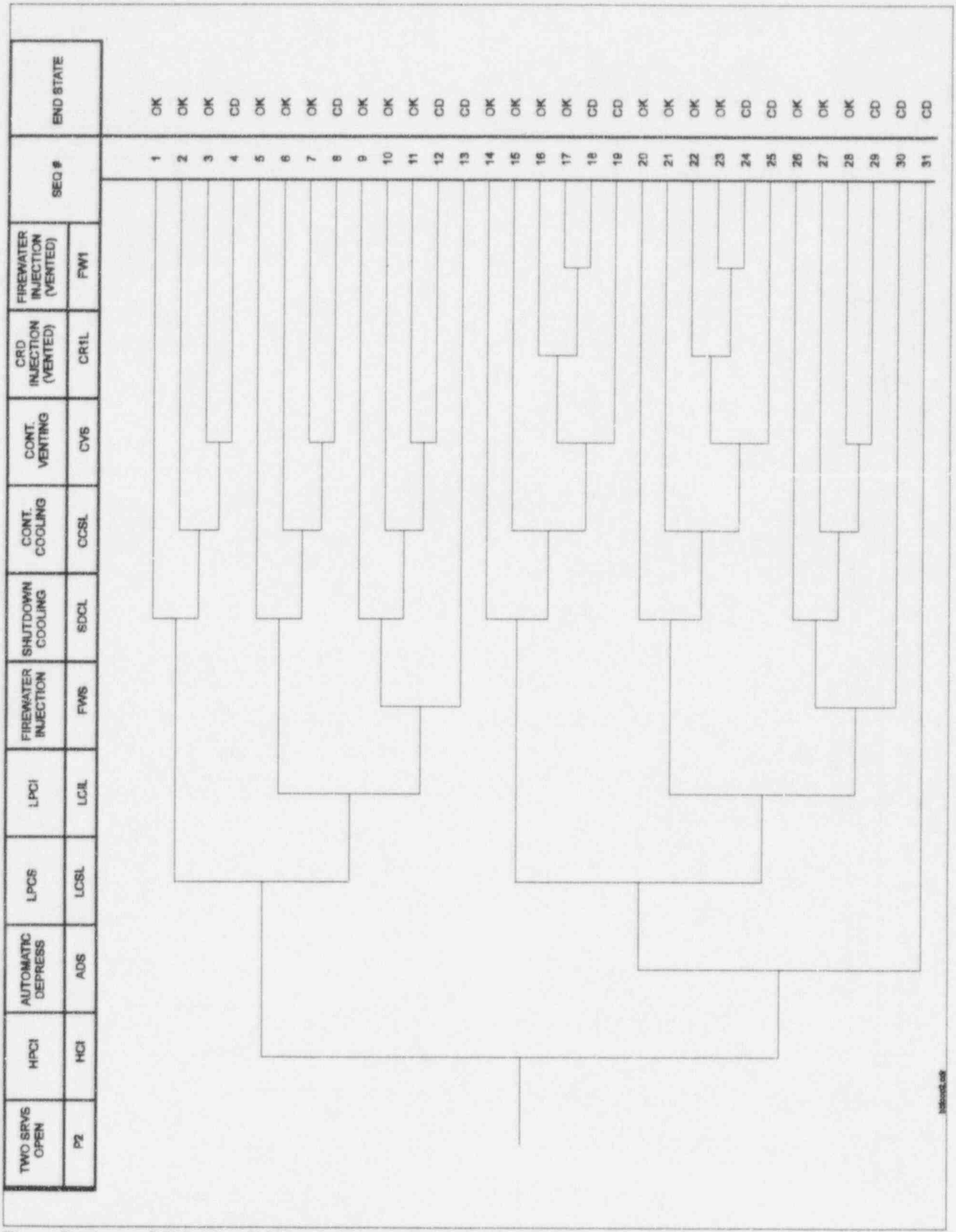


Figure B.31. BWR Class B loss-of-offsite power (cont.).

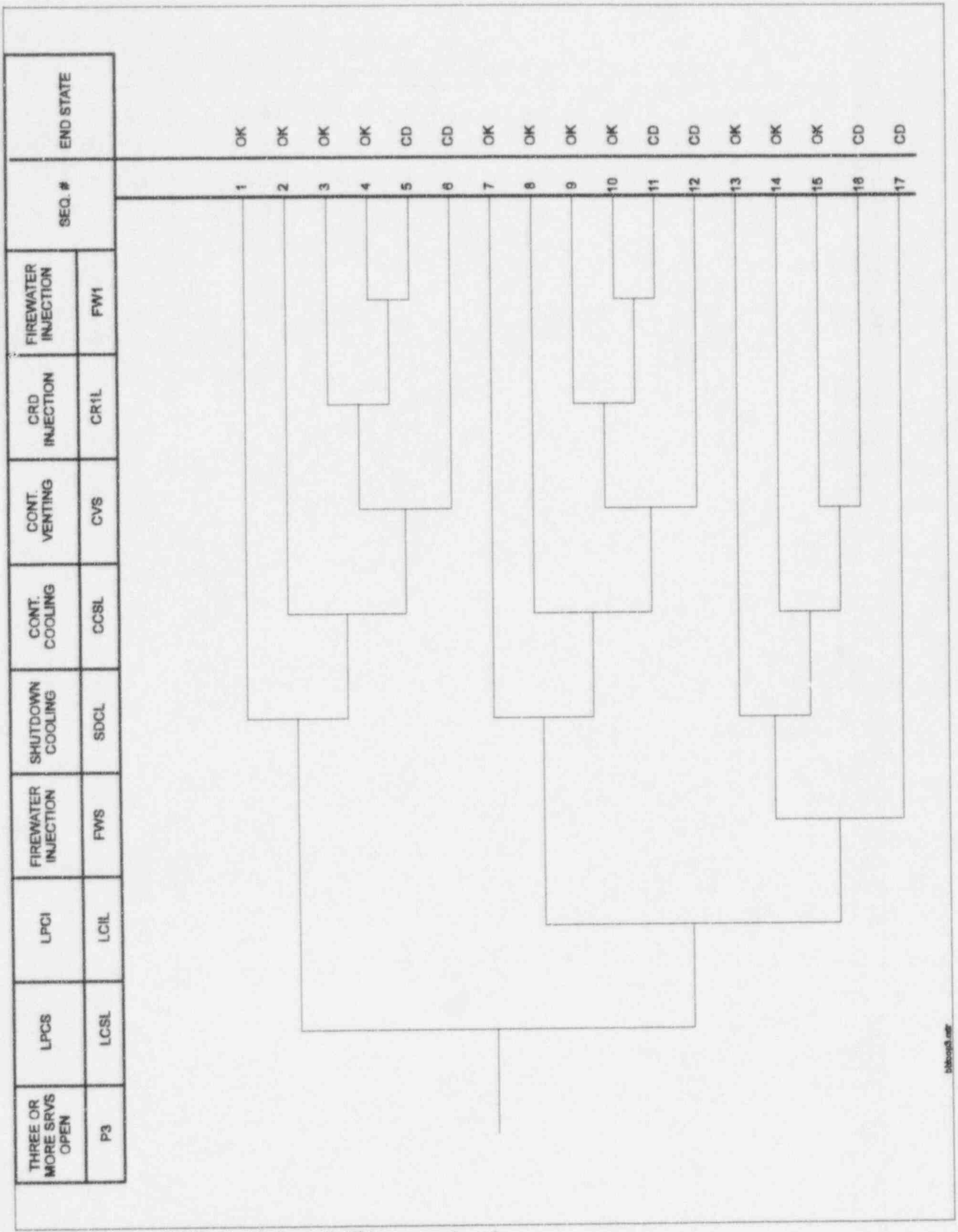


Figure B.32. BWR Class B loss-of-offsite power (cont.).

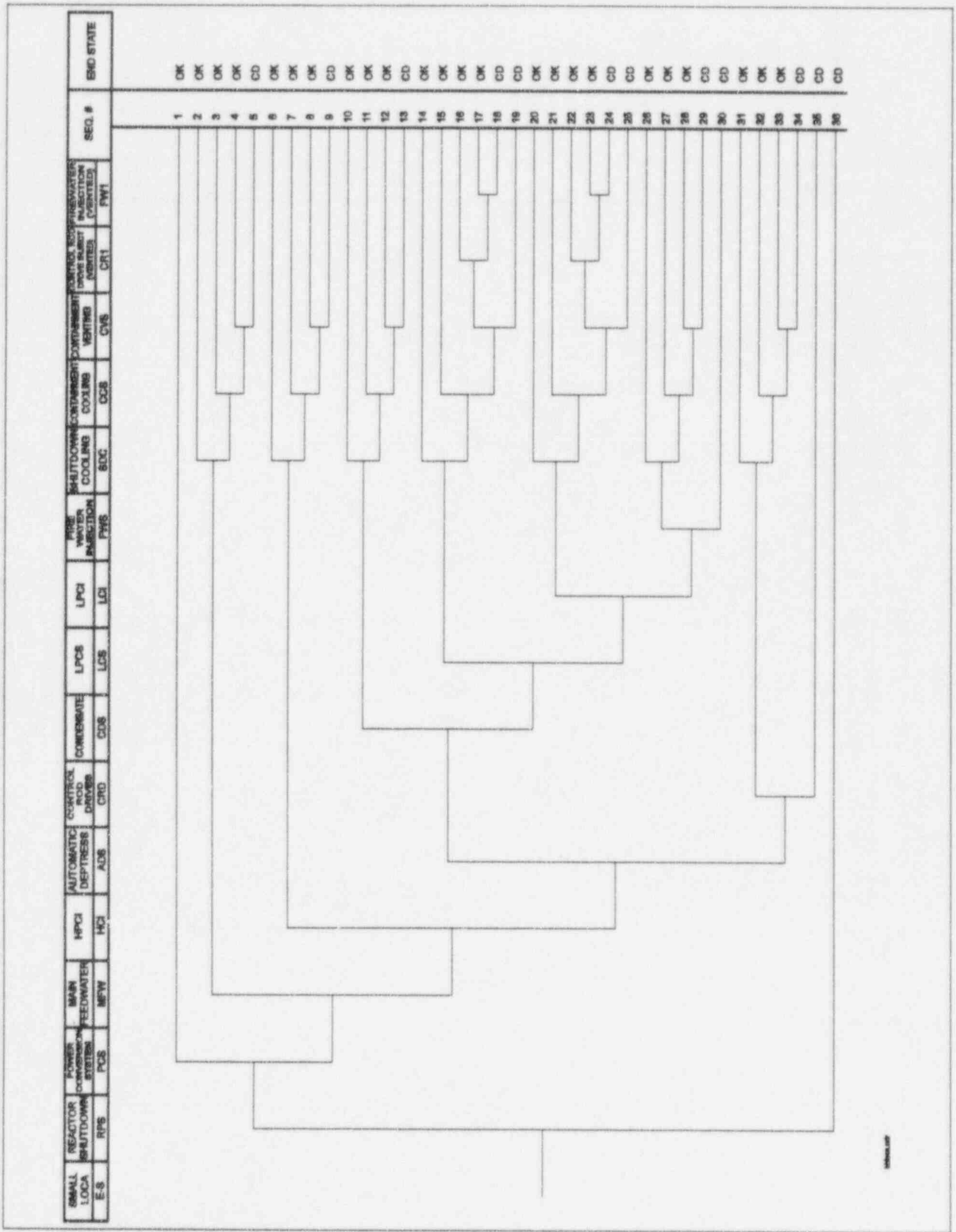


Figure B.33. BWR Class B small-break loss-of-coolant accident.

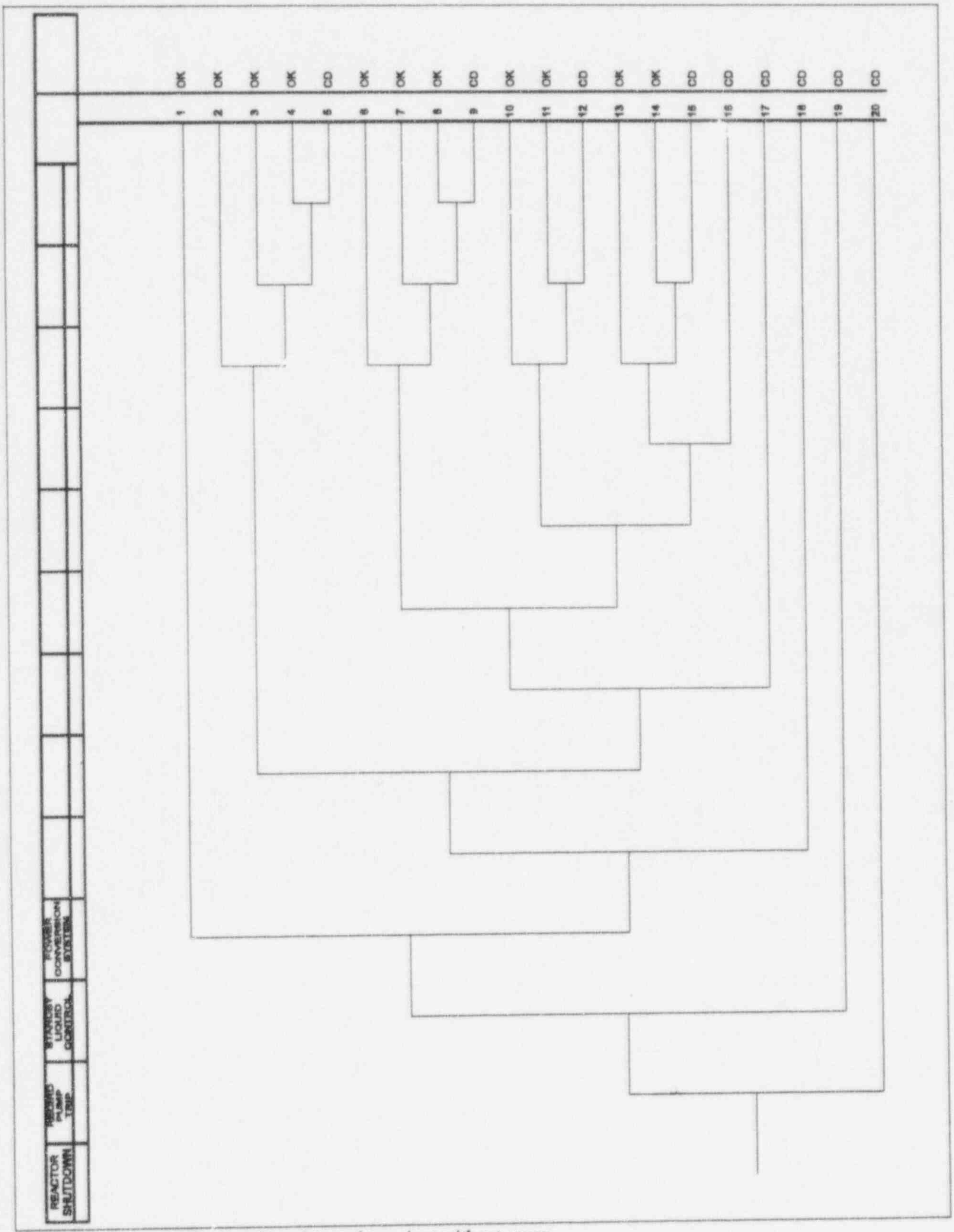


Figure B.34. BWR Class B anticipated transient without scram.

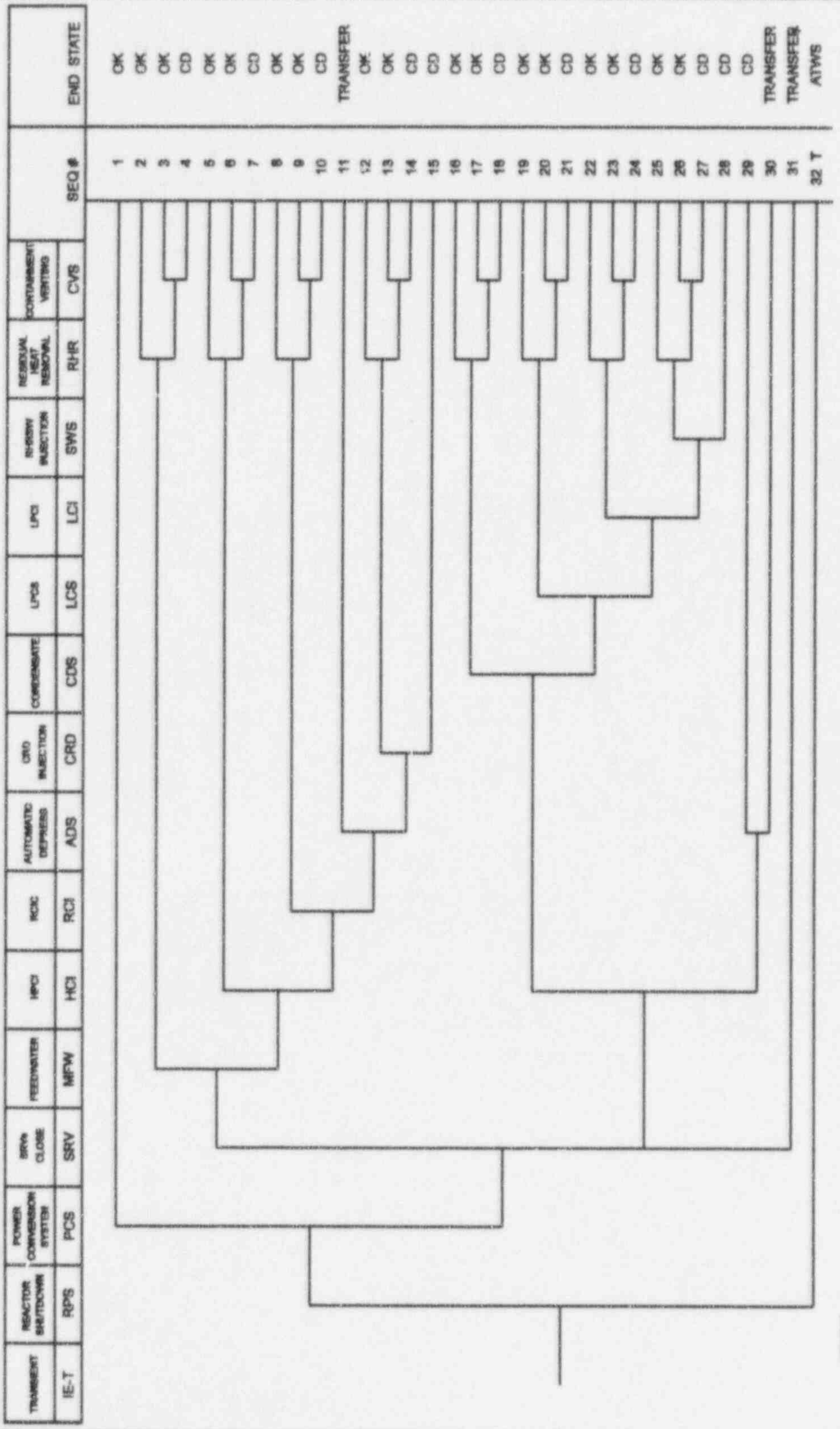


Figure B.35. BWR Class C nonspecific reactor trip.

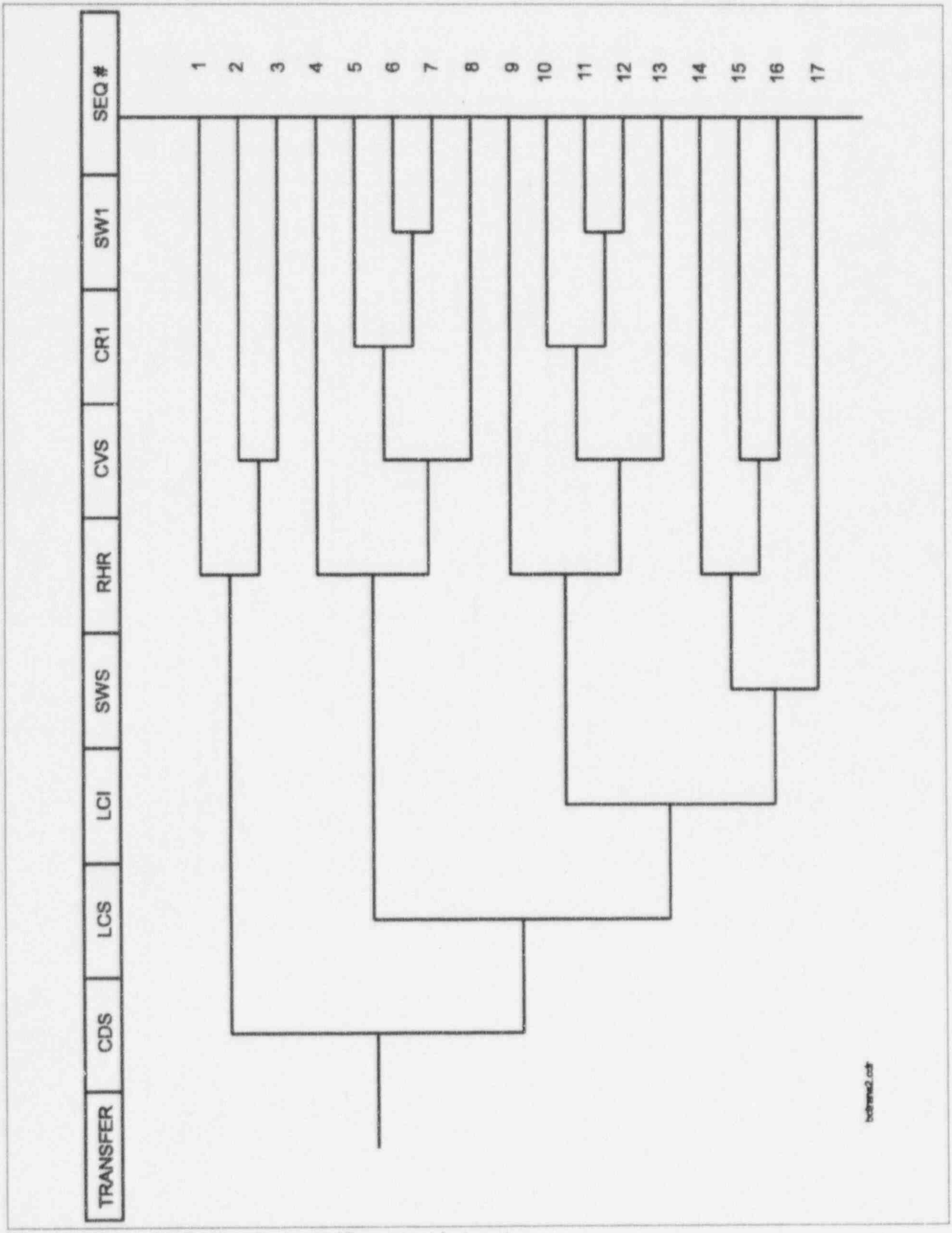


Figure B.36. BWR Class C nonspecific reactor trip (cont.).

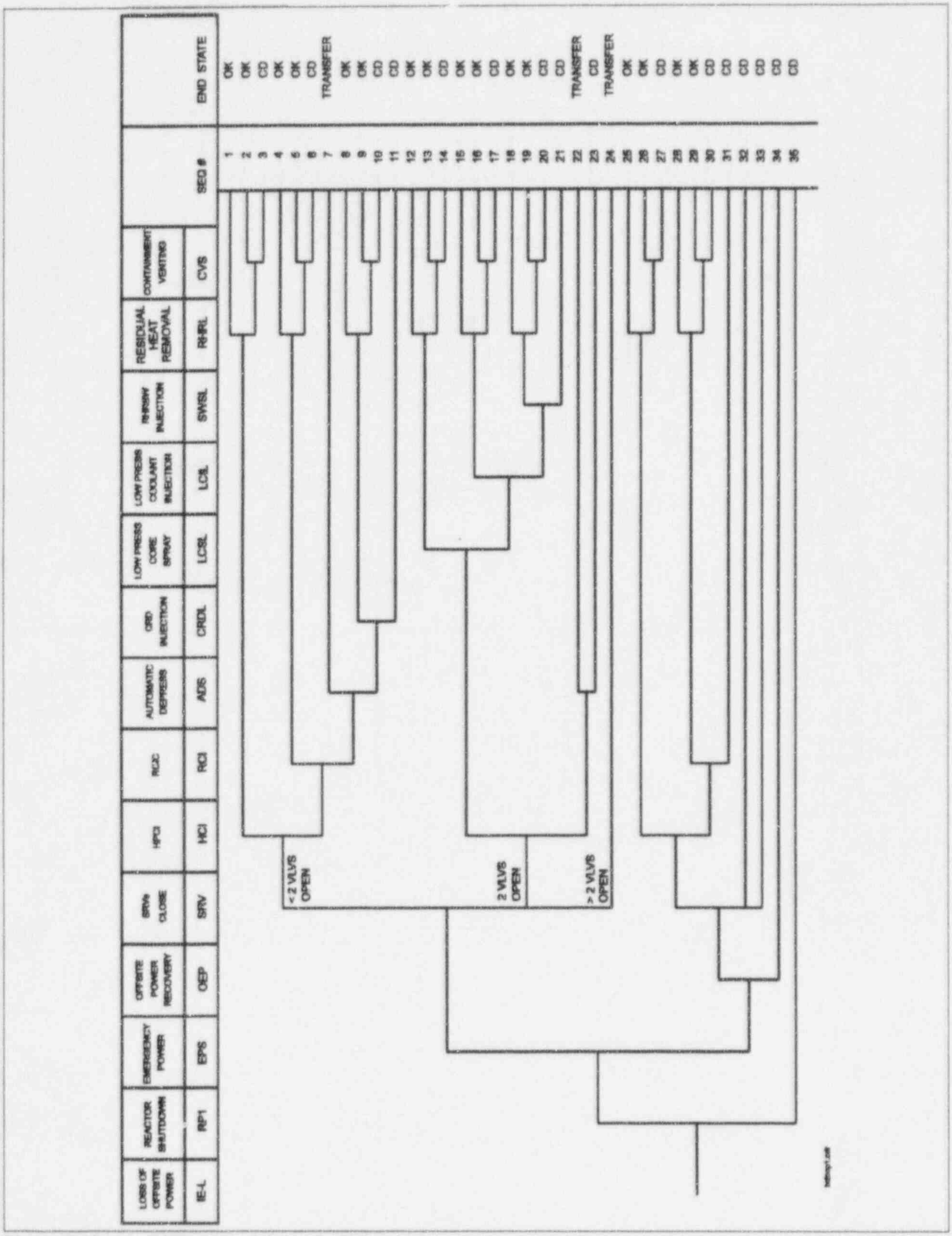


Figure B.37. BWR Class C loss-of-offsite power.

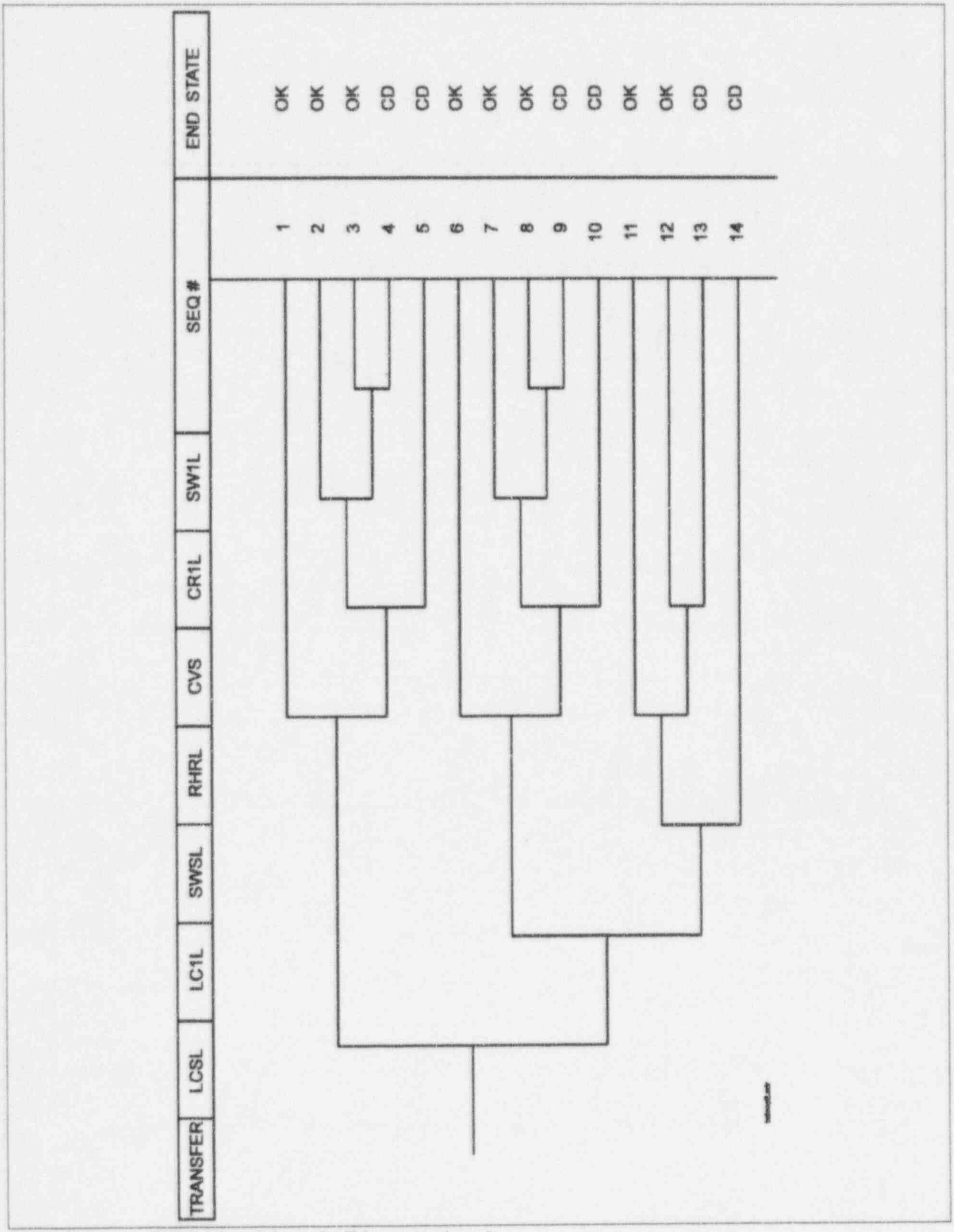


Figure B.38. BWR Class C loss-of-offsite power (cont.).

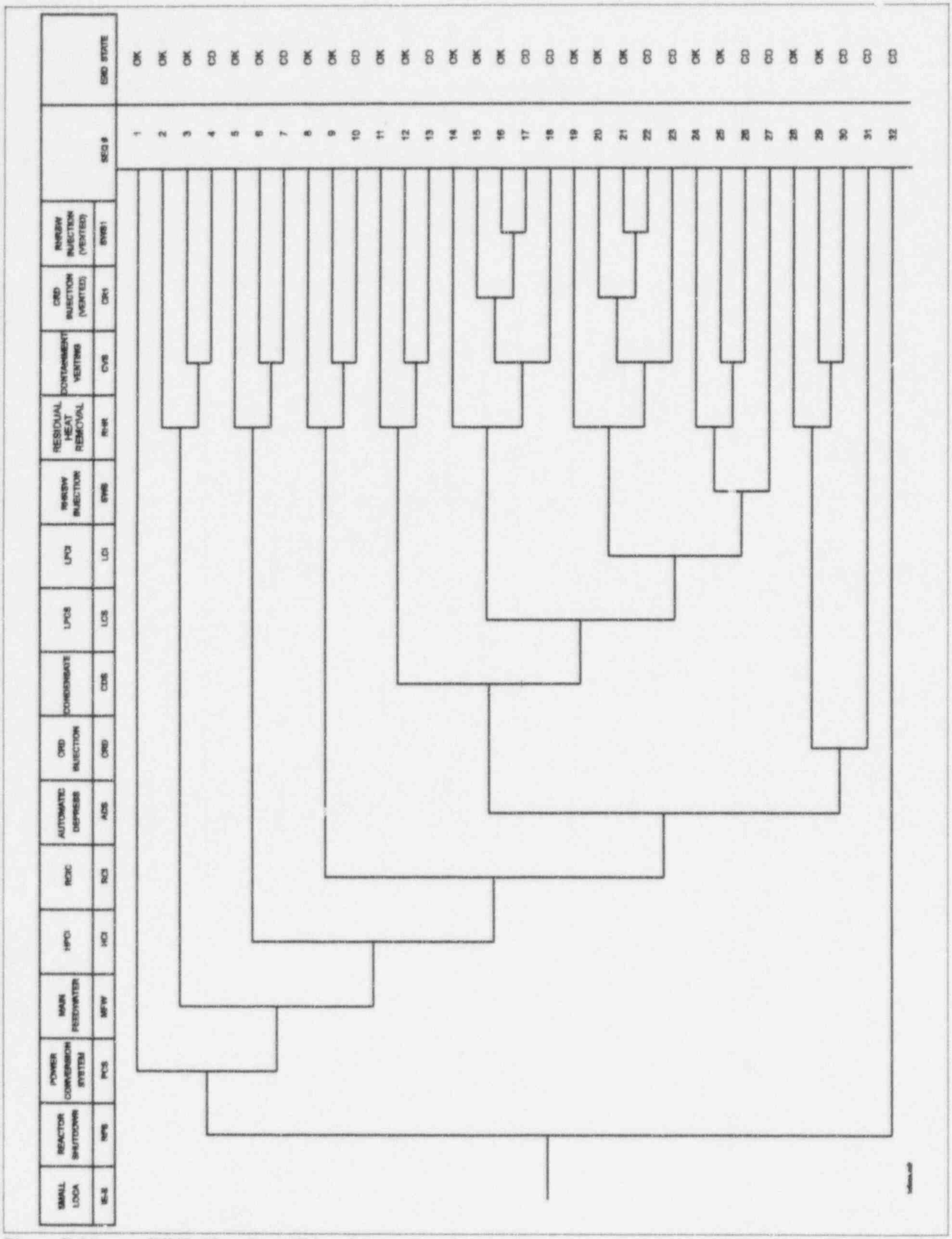


Figure B.39. BWR Class C small-break loss-of-coolant accident

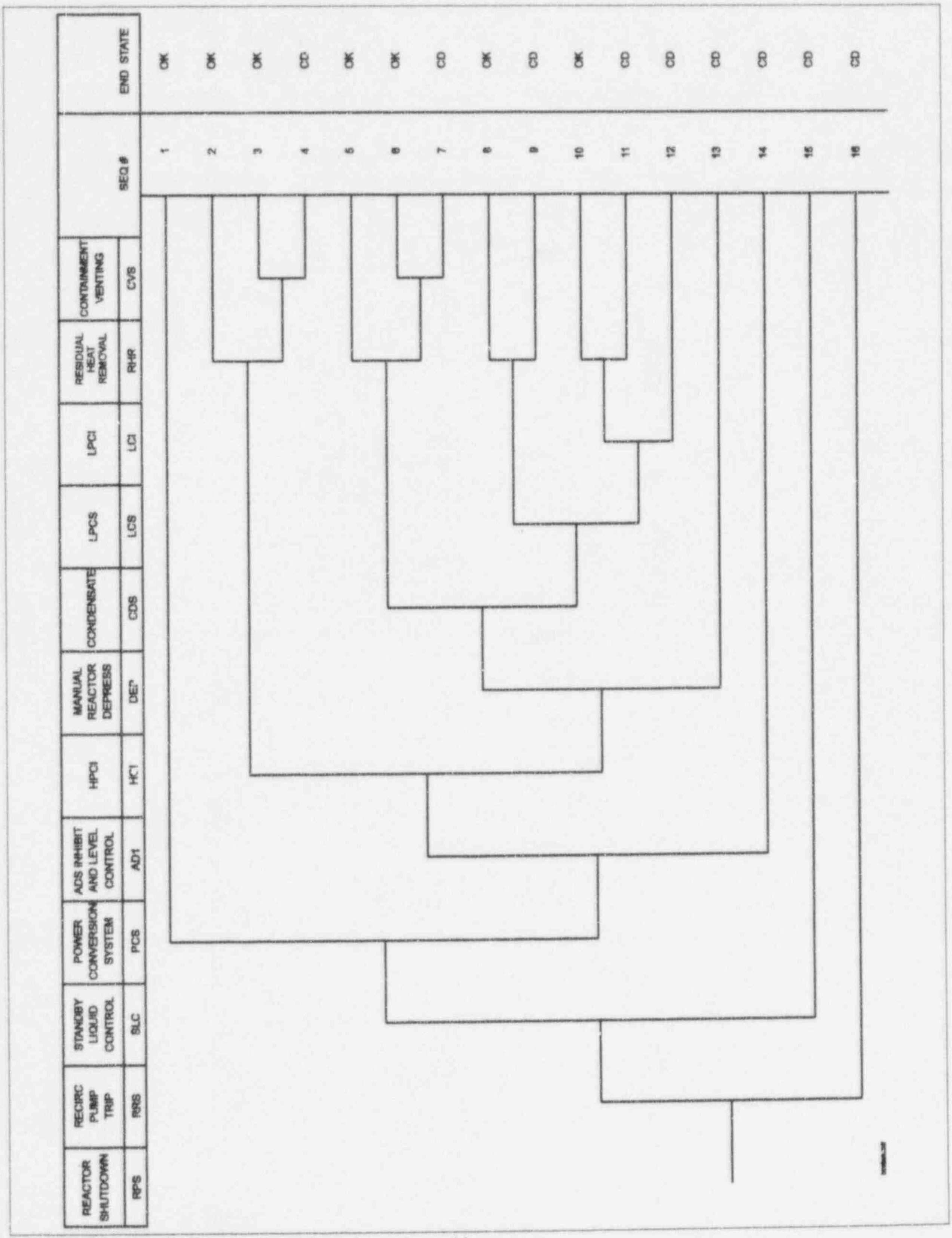


Figure B.40. BWR Class C anticipated transient without scram.

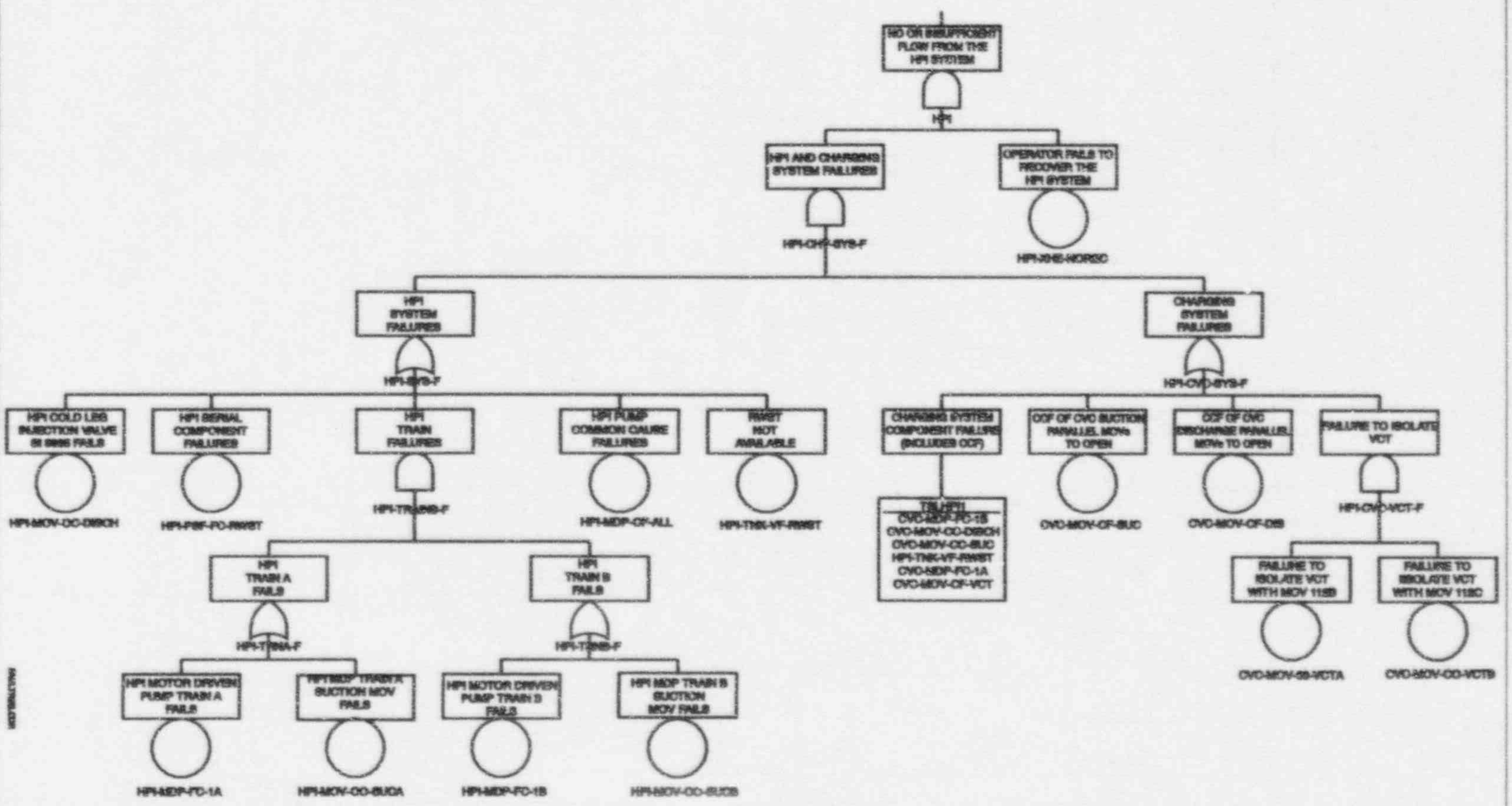

NO OR INSUFFICIENT FLOW FROM THE HPI SYSTEM
HPI
HPI AND CHARGING SYSTEM FAILURES
HPI-CHG-SYS-F
OPERATOR FAILS TO RECOVER THE HPI SYSTEM
HPI-XHE-NOREC
HPI SYSTEM FAILURES
HPI-SYS-F
CHARGING SYSTEM FAILURES
HPI-CVC-SYS-F
HPI COLD LEG INJECTION VALVE SI 8886 FAILS
HPI-MOV-OC-DISCH
HPI SERIAL COMPONENT FAILURES
HPI-PSF-FC-RWST
HPI TRAIN FAILURES
HPI-TRAINS-F
HPI PUMP COMMON CAUSE FAILURES
HPI-MDP-CF-ALL
RWST NOT AVAILABLE
HPI-TNK-VF-RWST
CHARGING SYSTEM COMPONENT FAILURE (INCLUDES CCF)
TSLHPI1
CVC-MDP-FC-1B
CVC-MOV-OC-DISCH
CVC-MOV-OC-SUC
HPI-TNK-VF-RWST
CVC-MDP-FC-1A
CVC-MOV-CF-VCT
CCF OF CVC SUCTION PARALLEL MOVs TO OPEN
CVC-MOV-CF-SUC
CCF OF CVC DISCHARGE PARALLEL MOVs TO OPEN
CVC-MOV-CF-DIS
FAILURE TO ISOLATE VCT
HPI-CVC-VCT-F
FAILURE TO ISOLATE VCT WITH MOV 115B
CVC-MOV-OO-VCTA
FAILURE TO ISOLATE VCT WITH MOV 115C
CVC-MOV-OO-VCTB
HPI TRAIN A FAILS
HPI-TRNA-F
HPI TRAIN B FAILS
HPI-TRNB-F
HPI MOTOR DRIVEN PUMP TRAIN A FAILS
HPI-MDP-FC-1A
HPI MDP TRAIN A SUCTION MOV FAILS
HPI-MOV-OO-SUCA
HPI MOTOR DRIVEN PUMP TRAIN B FAILS
HPI-MDP-FC-1B
HPI MDP TRAIN B SUCTION MOV FAILS
HPI-MOV-OO-SUCB
FAULTREE.CDR

Figure B.41. Representative ASP fault tree.

Appendix C

At-Power Precursors

C.1 At-Power Precursors

C.1.1 Accident Sequence Precursor Program Event Analyses for 1994

This appendix documents 1994 operational events selected as accident sequence precursors that are analyzed with the plant in an at-power condition.

Licensee Event Reports (LERs) and other event documentation describing operational events at commercial nuclear power plants were reviewed for potential precursors if

1. the LER was identified as requiring review based on a computerized search of the Sequence Coding and Search System dr˙a base maintained at Oak Ridge National Laboratory, or
2. the LER or other event documentation was identified as requiring review by the Nuclear Regulatory Commission's Office for Analysis and Evaluation of Operational Data.

Details of the precursor review, analysis, and documentation process are provided in Section 2 and Appendix A of this report.

C.1.2 Precursors Identified

Eight at-power precursors were identified among the 1994 events reviewed at the Nuclear Operations Analysis Center. Events were identified as precursors if they met one of the following precursor selection criteria and the conditional core damage probability estimated for the event was at least 10^{-6}:

1. the event involved the total failure of a system required to mitigate effects of a core damage initiator,
2. the event involved the degradation of two or more systems required to mitigate effects of a core damage initiator,
3. the event involved a core damage initiator such as a loss of offsite power or small-break loss-of-coolant accident, or
4. the event involved a reactor trip or loss of feedwater with a degraded safety system.

The at-power precursors identified are listed in Table C.1.

Table C.1. List of at-power precursors

Event No.	Plant	Event description	Page
LERs 213/94-004, -005, -007, -013; IR 213/94-03	Haddam Neck	Power Operated Relief Valves and Vital 480-V ac Bus Degraded	C.2-1
LER 237/94-018	Dresden 2	Motor Control Center Trips Due to Improper Breaker Settings	C.3-1
LER 237/94-021	Dresden 2	Long-Term Unavailability of High Pressure Coolant Injection	C.4-1
LER 250/94-005	Turkey Point 3 and 4	Load Sequencers Periodically Inoperable	C.5-1
LER 266/94-002	Point Beach 1 and 2	Both Diesel Generators Inoperable	C.6-1
LER 304/94-002	Zion 2	Unavailability of Turbine-Driven Auxiliary Feedwater Pump and Emergency Diesel Generator	C.7-1
LER 318/94-001	Calvert Cliffs 2	Trip, Loss of 13.8-kV Bus and Short-Term Salt Water Cooling System Unavailability	C.8-1
LER 458/94-023	River Bend	Scram, Main Turbine-Generator Fails to Trip, Reactor Core Cooling Isolation Cooling and Control Rod Drive System Unavailable	C.9-1

C.1.3 Event Documentation

Analysis documentation and precursor calculation information for each precursor are attached. The precursors are in docket/LER number order.

For each precursor, an event analysis sheet is included. This provides a description of the operational event, event-related plant design information, and the assumptions and approach used to model the event, analysis results, and references.

A figure is included that highlights the dominant core damage sequence associated with the event. Conditional core damage calculation information is also provided,including the following tables:

- Probabilities for selected basic events,
- Sequence logic, sequence probabilities and importances and system names for higher probability sequences, and
- Higher probability cut sets for higher probability sequences.

C.2 LER Nos. 213/94-004, -005, -007, -013; IR 213/94-03

Event Description: Power-Operated Relief Valves and Vital 480-V ac Bus Degraded

Date of Event: February 16 and 19, 1994

Plant: Haddam Neck

C.2.1 Event Summary

On February 16, 1994, testing revealed that one of two feeds to motor control center-5 (MCC-5) could jam and fail to close when demanded. MCC-5 supplies power to a number of vital components in both safety system trains. During testing on February 19, 1994, it was discovered that air operators for the pressurizer power-operated relief valves (PORVs) were experiencing control air leaks and that the PORVs could not be operated properly from their safety-grade control air supply. Investigation revealed that repairs to fix a prior PORV failure were made incorrectly during the previous refueling outage. The PORV diaphragms were not seated correctly and were coated with a lubricant rather than a required sealant. Substantial air leaks resulted, and the PORVs could not be opened more than 50%. The combined conditional core damage probability estimated for these events is 1.4×10^{-4}.

C.2.2 Event Description

During a maintenance outage, an operability surveillance test was performed on the pressurizer PORVs on February 19, 1994. This test revealed that both PORV air operators had leaking diaphragms (LER 213/94-005). The PORV diaphragms had been replaced during the 1993 refueling outage following a diaphragm leak in one of the two PORVs (LER 213/93-007).

Surveillance testing of the PORVs in May 1993 revealed that one valve was experiencing leakage from its diaphragm assembly (LER 213/93-007). This leak, in conjunction with failure of the associated air pressure regulator, resulted in excessive air consumption. Had the system been demanded, operator action to isolate the leaking PORV would have been required to ensure an adequate long-term supply of control air to the other PORV. Repairs to the system, including replacement of the PORV diaphragms, were completed prior to the end of the 1993 refueling outage.

The design of the new diaphragms varied somewhat from the original ones, which may have contributed to the difficulties experienced during the replacement process. Errors were made during the replacement, including the use of a lubricant instead of a sealant around the diaphragm's bolt circle. This allowed the diaphragm to extrude out between the sections of its housing, creating a pathway for air leakage. An NRC inspection team report related to this event (50-213/94-03, April 7, 1994) indicates that both valves could only be opened about 50% during testing. The LER for the event indicates that two safety functions were potentially compromised by the PORV failures: feed-and-bleed cooling and high-pressure safety injection (HPSI) makeup during certain small-break loss-of-coolant accidents (LOCAs).

The HPSI pumps at Haddam Neck do not develop sufficient discharge head to force adequate flow for feed-and-bleed cooling through the pressurizer safety valves. Accordingly, the operators must be able to open a PORV for feed-and-bleed cooling to succeed. Air is supplied to the PORVs from the containment air compressors. The containment air compressors, which are located within the containment building, are not rated for the environmental conditions that could occur during feed-and-bleed cooling, and the compressors could be expected to fail under such conditions. The PORVs are provided with safety-related control air accumulators that maintain a reserve supply of control air in the event of compressor failure, but these accumulators were inadequate to operate the PORVs during the time that the air-operator diaphragms were damaged. LER 213/94-005 reported that air leakage would have resulted in the eventual loss of air and closure of the PORVs for feed-and-bleed conditions. As a result of their incorrect installation, the PORV air-operator diaphragms were damaged and subject to leakage from some unknown time after they were were replaced during the 1993 refueling outage until the condition was discovered on February 19, 1994.

LER 213/94-005 also identified a concern related to the provision of HPSI minimum flow protection by the PORVs. During small-break LOCA sequences, the HPSI minimum flow recirculation line to the refueling water storage tank is isolated, and minimum flow protection is provided by opening the PORVs. With the PORVs inoperable, this protection would not be provided, and the HPSI pumps would be subject to damage if reactor coolant system (RCS) pressure remained above the HPSI pump shutoff head. The LER indicates that an alternate strategy of using charging flow would be successful in maintaining the RCS filled for small break sizes that would not be large enough to ensure minimum necessary HPSI flow.

LER 213/94-004 reports that, during a period of time overlapping the PORV unavailability, the automatic bus transfer (ABT) circuit for MCC-5 failed when tested. At the time of the event, MCC-5 supplied many pieces of important equipment in both trains, including equipment that may have been required for successful operation of HPSI, low-pressure safety injection (LPSI), recirculation, long-term cooling, containment spray, RCS loop isolation, one PORV block valve, emergency boration, feedwater isolation, reactor coolant pump (RCP) seal cooling, service water, control air, and the closed cooling water system. Subsequent to this event, modifications were made to reduce the dependency upon MCC-5.

MCC-5 can be supplied from either 480-V ac bus 5 (emergency train A) or bus 6 (emergency train B). Normally, the alignment is aligned such that bus 5 is the preferred supply and bus 6 is the alternate supply. At the time of the event, if the preferred supply was lost, the ABT system aligned MCC-5 to the alternate bus. If power was restored to the preferred bus, the ABT would realign back to the preferred bus. During a test of the ABT system, bus 5 was deenergized. As designed, the breaker supplying MCC-5 from bus 5 opened, and the supply breaker from bus 6 automatically closed to restore power. When bus 5 was reenergized, MCC-5 automatically realigned itself to bus 5. During the second part of the test, the preferred power source selector switch (PPSSS) for the ABT was moved to make bus 6 the preferred power supply and bus 5 the alternate. When the PPSSS was moved to the bus 6 position, the bus 5 supply breaker opened as expected, but the bus 6 supply breaker failed to automatically close, deenergizing MCC-5.

Subsequent investigation revealed that a mechanical defect in the MCC-5 feeder breaker from bus 6 prevented it from closing. With bus 6 still energized and selected as the preferred power source to MCC-5, the bus 5 supply to MCC-5 was prevented from closing by the ABT system logic. NRC inspection report 50-213/94-03 indicated that the likely cause of the failure of breaker 11C, the feeder from bus 6, was mispositioning of a breaker component ("snap ring") during maintenance. The snap ring being improperly located would cause the 11C breaker to have intermittent failures. Vibrations of the breaker would cause the trip to occur at times and not to occur at other times. This condition would result in intermittent failures of the MCC-5 ABT. The fraction of time that the breaker may have operated is unknown.

LER 213/94-013 reported the failure of a HPSI common header relief valve discovered during testing on May 5, 1994. While the actual lift pressure for the valve was not stated, it was reported that it did not lift during operation of the A pump, which developed a discharge pressure of about 1460 psig; but the valve did lift prematurely during operation of the B pump, which developed about 1510 psig. Leakage flow back to the refueling water storage tank (RWST) through this valve was limited to a maximum of 35 gpm. The condition is reported to have existed from the time that the B pump was overhauled in 1993 until discovery on May 5, 1994.

LER 213/94-007 reported the discovery that the chemical volume and control system (CVCS) pump common header discharge relief valve minimum lift set point was 2653 psig. The maximum charging pump discharge pressure under accident conditions was estimated to be about 2658 psig. Maximum flow through this relief valve is 30 gpm, which would be directed to radwaste drain tanks. Since CVCS is utilized to provide high-pressure recirculation, this represents a potential diversionary flow path from the CVCS during recirculation.

C.2.3 Additional Event-Related Information

The description of this event and the modeling assumptions are based on the plant status at the time of the event. Subsequent design changes have been made to reduce the likelihood and risk of future failures, such as elimination of the PPSSS MCC-5 ABT. Some plant modifications initiated after the June 1993 MCC-5 bus transfer failure that were complete at the time of this event included shifting the power supply from MCC-5 to MCC-12 for one residual heat removal (RHR) to charging pump suction valve, the A charging pump main lube oil pump, and one PORV block valve. The power supply to PORV PR-AOV-570 was also shifted to another source.

C.2.4 Modeling Assumptions

C.2.4.1 General Modeling Issues

The NRC inspection report related to this event (Ref. 5) indicates that the PORVs are required to remain operable for 30 h and provide a total of four valve strokes during feed-and-bleed scenarios. The measured control air leak rate was such that, during an actual event involving loss of the containment control air compressors and PORV demand, the PORV control air accumulators would have been depleted within minutes. Although the valves were able to partially open during testing, the valves would not be able to stay open for the required duration. Further, the containment air compressors are not rated for the containment environment that is expected after initiation of feed-and-bleed cooling. Therefore, the event was modeled as an unavailability of the PORVs for feed-and-bleed cooling. The PORVs would still be functional for overpressure protection of the reactor coolant system.

LER 213/94-005 indicates that the last successful operation of the PORVs was during an outage in May and June of 1993 following installation of the new diaphragms. It further indicates that the likely cause of the PORV failure was incorrect installation of the air-operator diaphragms during the 1993 outage. It was, therefore, assumed that the PORVs were inoperable for feed-and-bleed cooling from July 1993 until the leakage was discovered on February 19, 1994. This was modeled by setting the PORVs as failed for feed-and-bleed conditions at the appropriate places in the model.

The defect, which led to the intermittent failure of the bus 6 feeder breaker, was presumed to have existed from the time of the previous failure during the June 1993 refueling outage until the time of this event in February 1994. The interval analyzed was the period from July 21, 1993, until February 19, 1994, a period of 234 days (4728 h). Although the failure mechanism was intermittent, the fraction of time the component would have operated is unknown. It was assumed the breaker was failed throughout the period of interest. This is a conservative assumption.

The potential loss of HPSI minimum flow protection was not modeled because alternate means, such as the charging system, were available for RCS makeup in event of a small-small-break LOCA.

The potential failure of the HPSI relief valve during operation of train B in recirculation mode after a small-break LOCA was not modeled because, according to information from the LER, it would probably reseat following initiation of sump recirculation with secondary side cooling available. In any event, the maximum potential loss estimated for this pathway during a 24-h demand would be about 50,000 gal, which would still leave adequate sump inventory.

Potential failure of the CVCS relief valve was not modeled because LER 213/94-007 indicated that expected losses would be much less than the maximum relief valve flow rate of 30 gpm. The potential total diversion within a 24-h mission time is less than for the HPSI relief valve and would not affect system operability.

This analysis is structured similarly to the analysis of LER 213/93-007 and Augmented Inspection Team (AIT) Report 213/93-80 provided in the 1993 Accident Sequence Precursor (ASP) Program Annual Report (NUREG/CR-4674, ORNL/NOAC-232, Vols. 19 and 20). That analysis also dealt with failures of PORV control air system components coincident with inoperability of the MCC-5 ABT. Minor modifications to the 1993 analysis were required to adapt the approach to the current event. Those modifications are noted.

Challenge Rate for Pressurizer PORVs and Safety Relief Valves (SRVs)

The PORV block valves are maintained in a closed position at Haddam Neck, and at least one is dependent on MCC-5. Further, the PORVs are assumed failed in this analysis due to the diaphragm air leaks. Therefore, the PORV/SRV challenge rate applies solely to the SRVs after a loss-of-offsite power (LOOP) with MCC-5 unavailable. Since the PORV block valves are normally closed, it was assumed that the lift rate for SRVs is the same as when both the PORVs and SRVs are available. Therefore, this value was not modified.

PORV/SRV Reseat of Challenged Pressurizer PORVs and SRVs

It was assumed that the failure to reseat probability for the SRVs is the same as for the PORVs. The nonrecovery value was set to 1.0 because the safety valves do not have block valves.

Feed-and-Bleed

Feed-and-bleed requires the operation of HPI or the charging pumps, the high-pressure recirculation system (HPR), and the pressurizer PORVs. One HPI or charging pump and one PORV are required for success. Because the PORVs would not remain open for the required duration, feed-and-bleed was assumed inoperable.

C.2.4.2 Transient and Small-Break LOCA Sequences

Two cases were used to model the effects of the failed PORVs during transient and small-break LOCA conditions.

In the first case (IRRAS case 1A), the transient initiating probability was set to 1.0 (true), and the PORVs were failed (set to true). All other initiator probabilities were set to 0 (ignore).

The probability of a transient during the vulnerability period was calculated as follows:

$$1 - \exp(-\lambda t) = 1 - \exp\left[-(1.85 \times 10^{-4}/\mathrm{h}) \times (4728\ \mathrm{h})\right] = 0.58\ .$$

In the second case (IRRAS case 1B), the small-break LOCA initiating probability was set to 1.0 (true), and the PORVs were failed (set to true). All other initiator probabilities were set to 0 (ignore).

The probability of a small-break LOCA during the vulnerability period was calculated as follows:

$$1 - \exp(-\lambda t) = 1 - \exp\left[-(1.0 \times 10^{-6}/\mathrm{h}) \times (4728\ \mathrm{h})\right] = 4.7 \times 10^{-3}\ .$$

The initiating event probabilities and IRRAS case conditional probabilities were used to calculate the core damage probabilities from these initiators (see Table C.2.3 on p. C.2-11).

C.2.4.3 LOOP Sequences

To address the potential loss of MCC-5 and the failed PORVs following a postulated LOOP, a conditioning event tree was used. This event tree characterized potential plant conditions involving emergency diesel generator (EDG) success and failure, short-term (30-min) LOOP recovery, and short-term MCC-5 recovery. The event tree, shown in Figure C.2.1, includes the conditioning sequences shown in Table C.2.1.

Table C.2.1. Sequences for conditioning event tree in Figure C.2.1

Sequence	Description
1	Initial emergency power (EP) success with short-term recovery of offsite power and MCC-5 following the postulated LOOP. This is similar to a loss of feedwater but with a higher probability of a transient-induced LOCA, because the SRVs would lift (if necessary) as a result of the inoperable PORVs. Feed-and-bleed is failed in IRRAS Case 2.1 because of the inoperable PORVs.
2	Initial EP success and short-term recovery of offsite power but with MCC-5 not recovered at 30 min. This is similar to sequence 1, but with the potential for an RCP seal LOCA if MCC-5 is not recovered at 1 h. HPI is assumed unavailable if MCC-5 is not recovered ~0.5 h following a seal LOCA. HPI following a stuck-open SRV and feed-and-bleed are also assumed to be unavailable in IRRAS Case 2.2 since MCC-5 is unavailable at 30 min.
3	LOOP with EP initially successful, MCC-5 recovered, and feed-and-bleed unavailable (IRRAS Case 2.1). Higher probability of a transient-induced LOCA.
4	LOOP with EP initially successful but neither MCC-5 nor offsite power recovered at 30 min. There is a higher potential for an RCP seal LOCA if MCC-5 is not recovered. There is also a higher probability of a transient-induced LOCA. HPI following a stuck-open relief valve and feed-and-bleed are also assumed to be unavailable (IRRAS Case 2.2) since MCC-5 is unavailable at 30 min.
5	Station blackout.
6	Anticipated transient without scram.

LOOP Initiating Event Probability

The probability of a LOOP during the vulnerability period was calculated as follows:

$$1 - \exp(-\lambda t) = 1 - \exp\left[-(1.6 \times 10^{-5}/\mathrm{h}) \times (4728\ \mathrm{h})\right] = 7.3 \times 10^{-2}\ .$$

The vulnerability period was estimated at 4728 h. This is the operational time between plant restart in 1993 and discovery of the PORV problem in February 1994.

Failure to Trip Probability

The failure to trip probability was not modified for this event. The value from the IRRAS model for Haddam Neck is 2×10^{-5}. This includes RPS hardware failures and subsequent operator recovery of the system.

Emergency Power

The probability for emergency power failure was not modified. This probability (2.3×10^{-3}) includes operator recovery following postulated EDG failures.

LOOP Recovery in the First 30 min

The probability for failure to recover the LOOP in the first 30 min was based on LOOP recovery models described in *Revised LOOP Recovery and PWR Seal LOCA Models*, ORNL/NRC/LTR-89/11. These models are based on the results of the data contained in NUREG-1032, *Evaluation of Station Blackout Accidents at Nuclear Power Plants*.

MCC-5 Failure and Restoration

Based on the condition of breaker 11C (feeder from bus 6 to MCC-5) and the unpredictability of its observed failures, breaker 11C was assumed to be failed in this analysis. In addition to the failure of breaker 11C, one additional failure must occur for MCC-5 to lose power. Either breaker 9C (feeder from bus 5) must fail to reclose, or EDG A must fail to start and run.

After a LOOP with the PPSSS in the bus 5 (normal) position, power would be lost to buses 5 and 6. Two cases could 'hen occur.

- Bus 5 is re-energized before bus 6. In this case, breaker 9C will attempt to reclose. If 9C fails to close, the ABT will automatically try to close breaker 11C once bus 6 is energized. However, since breaker 11C is assumed to be failed, manual operator action is required to restore power to MCC-5.
- Bus 6 is re-energized before bus 5. In this case, breaker 11C will attempt to close. Assuming 11C fails to close, the ABT will attempt to automatically reclose breaker 9C after power is restored to bus 5. If breaker 9C fails to reclose, manual operator action is required to restore power to MCC-5. Data collected by the licensee on EDG performance indicate that the time to rated speed and voltage for both of the EDGs was essentially the same. This would mean that bus 6 would reach rated voltage first about 50% of the time. (Circuit timing delays may affect this value somewhat but would have little impact on the analysis results.) Assuming that breaker 11C will fail to close on demand, and a beta factor of 0.1 for breaker 9C since it was subject to the same maintenance procedures as the failed 11C breaker, the probability of failure of the ABT given a LOOP is:

$$[p(5\text{before}6)\times p(9C|11C)]+[p(\overline{5\text{before}6})\times\{p(\text{EDG A})\quad p(9C|11C)\}]=$$

$$[p(5\text{before}6)\times p(9C|11C)]+p(\overline{5\text{before}6})\times p(\text{EDG A})+p(\overline{5\text{before}6})\times p(9C|11C)=$$

$$p(9C|11C)+[p(\overline{5\text{before}6})\times p(\text{EDG A})]=0.1+(0.5\times 0.05)=0.125.\,^*$$

The licensee performed a detailed analysis of MCC-5 failure probabilities. Their assessment indicates that the probability that MCC-5 fails to supply power is 0.059 for LOOP events. However, this assumed a nominal failure rate for breaker 11C.

To recover MCC-5 following a failure of the ABT, an operator must proceed to MCC-5, diagnose the situation, and manually close one of the MCC-5 feeder breakers. During the June 1993 event, an operator took 4 min to complete this action. However, the operator was already stationed at the selector switch, was immediately aware of the ABT failure, and had a minimum of other distractions and stresses. Similarly, during one of two ABT test failures on February 16, 1994, operators took approximately 3 min to repower MCC-5 from bus 5. The time required to repower MCC-5 during the second event is not known.

Following a postulated LOOP with the failure of MCC-5, additional delays would be introduced, including detection time, delays for the control room to contact an auxiliary operator and describe the problem, and operator transit time. Unavailability of power on MCC-5 is not directly addressed in procedure E-0, "Reactor Trip or Safety Injection," until step 16. A median value was used in the analysis; this assumes 6 min for diagnosis and transit time and the observed ~4 min for recovery at the equipment. A 6-min diagnosis and transit time is considered possible because of the proximity of MCC-5 to the control room. [The 10-min median value is somewhat longer than the licensee's estimate of 5 to 6 min (2- to 3-min diagnostic time, 1-min transit, and 2 min to operate breakers) and somewhat shorter than a 16-min value that can be estimated based on a distribution of transit times in response to a faulted EDG (another important component) included in "Electric Power Recovery Models," J. W. Reed and K. N. Fleming, *Proceedings of the International Topical Meeting on Probabilistic Safety Assessment*, PSA'93, January 26–29, 1993.]

The probability of not recovering MCC-5 was estimated by assuming that the 10-min period was the median of a lognormal distribution with an error factor of 3.2 (see Dougherty and Fragola, *Human Reliability Analysis*, John Wiley

* For situations where offsite power is recovered within 30 min, the probability for MCC-5 failure is 0.1.

and Sons, New York, 1988, Chap. 10). This is the error factor for time-reliability correlations (TRCs) for actions without hesitancy, which is considered appropriate based on the recognized importance of MCC-5. Three primary time intervals for MCC-5 recovery were considered in this analysis. These intervals and the associated MCC-5 nonrecovery probabilities are shown in Table C.2.2.

Table C.2.2. MCC-5 nonrecovery values

Time interval (h)	p(MCC-5 not recovered)
0.5	6.0×10^{-2}
1.0	5.6×10^{-3}
1.5	9.5×10^{-4}

For the conditioning event tree, the probabilities of MCC-5 failure followed by failure to recover MCC-5 were determined as follows:

$$p(\text{MCC-5 failed and not recovered} \mid \text{LOOP recovered within first 30 min}) = 0.1 \times (6.0 \times 10^{-2}) = 6.0 \times 10^{-3}$$

$$p(\text{MCC-5 failed and not recovered} \mid \text{LOOP not recovered within first 30 min}) = 0.125 \times (6.0 \times 10^{-2}) = 7.5 \times 10^{-3}\,.$$

Calculations for LOOP Conditioning Sequences 1 and 3 (IRRAS Case 2.1)

To reflect the conditions assumed in Figure C.2.1 for these sequences, the IRRAS model for Haddam Neck was evaluated with the LOOP initiator set to 1.0, both PORVs failed for feed-and-bleed only (set to true) and nonrecoverable for LOOP conditions (see General Modeling considerations for a discussion of the PORV operability), emergency power successful (basic events for both EDGs set to false), and short-term LOOP nonrecovery set to 1.0. Potential EDG failures are addressed in the conditioning event tree (Figure C.2.1). Other initiators were ignored for this calculation.

Calculations for LOOP Conditioning Sequences 2 and 4 (IRRAS Case 2.2)

For these two sequences, two calculations were performed. In the first, the IRRAS model was evaluated with the LOOP initiator set to 1.0, both PORVs failed for feed-and-bleed only (set to true) and nonrecoverable under LOOP conditions, emergency power successful (basic events for both EDGs set to false), short-term LOOP nonrecovery set to 1.0, and both HPI pumps failed (set to True) and nonrecoverable for both HPI and HPR. HPI is assumed unavailable if MCC-5 is not recovered ~0.5 h following a seal LOCA. HPI following a stuck-open SRV and feed-and-bleed are also assumed to be unavailable since MCC-5 is unavailable at 30 min. Potential EDG failures are addressed in the conditioning event tree on Figure C.2.1.

In addition to the IRRAS calculation, an event tree was developed to address the possibility of a seal LOCA (Figure C.2.2). This tree was quantified as follows.

MCC-5 Recovered Before Seal LOCA and Seal LOCA Probabilities

Operator action is required to recover either means of RCP seal cooling (seal injection and thermal barrier cooling) following a LOOP and the loss of MCC-5. Component cooling water, which provides thermal barrier cooling, is lost following the LOOP due to the loss of instrument air. The charging pumps, which provide seal injection, also trip following a LOOP due to an automatic tripping feature that had recently been installed. During the 1993 ABT failure event, because the main lube oil pumps for the charging pumps were powered from MCC-5, the charging pumps could not be restarted without first recovering MCC-5 or aligning the alternate lube oil pumps. After the 1993 event, the power supply to A charging pump lube oil pump was realigned to MCC-12. However, instrument air is powered from MCC-5, and loss of MCC-5 would cause the charging flow control valve to go wide open, depriving RCP seals of flow. Operator actions would be required to either recover MCC-5 or to throttle charging flow and restore seal injection.

The potential impact of an RCP seal LOCA following loss of MCC-5 but with emergency power available was addressed in the event tree model shown in Figure C.2.2. This model is applicable to sequences involving emergency power and auxiliary feedwater (AFW) success with the SRV closed. In this model, MCC-5 must be recovered or the charging system must be restarted and realigned to prevent an RCP seal LOCA. Given that a seal LOCA has occurred, HPI and HPR are required to prevent core damage. Recovery of HPI requires recovery of MCC-5 or the charging system.

To simplify the analysis, an RCP seal LOCA was assumed likely in nonblackout sequences if MCC-5 or the charging system are not recovered at 1 h. The probability of not recovering MCC-5/charging system at 1 h, given that they were not recovered at 0.5 h (this probability is addressed in a conditioning event tree branch), was estimated to be

$$p(\text{MCC-5 recovered at 1 h} \mid \text{MCC-5 not recovered at 0.5h}) = (5.6 \times 10^{-3}/6.0 \times 10^{-2}) = 9.3 \times 10^{-2}.$$

The probability of seal LOCA occurring at this time was assumed to be 0.7, consistent with other ASP analyses.

HPI High-Pressure Injection

Following the loss of MCC-5, the HPI system is lost (Haddam Neck IPE Table B-1, System/Function 2, Sump Recirculation). Restoration of power to MCC-5 is required to regain HPI function. The charging pumps are also unavailable following a loss of MCC-5 until they are realigned and restarted.

For a stuck-open SRV, the probability of HPI failure, given that MCC-5 was not recovered at 0.5 h, was assumed to be 1.0. For an RCP seal LOCA with emergency power initially available, the failure probability for HPI was estimated to be 0.17:

$$p(\text{MCC-5 not recovered 0.5 h after a potential seal LOCA} \mid \text{MCC-5 not recovered at 1.0 h})^*$$
$$= 9.5 \times 10^{-4}/5.6 \times 10^{-3}$$
$$= 0.17 .$$

HPR High-Pressure Recirculation

The failure probability for HPR was determined by using the system failure probability from the IRRAS model for Haddam Neck.

Calculations for LOOP Conditioning Sequence 5

The event tree model used to address potential seal LOCAs following a station blackout is shown in Figure C.2.3. This model utilizes the same assumptions regarding the onset of a seal LOCA and recovery of HPI as the nonblackout case.

AFW Auxiliary Feedwater

Normal AFW flow control is dependent on MCC-5. However, flow control is also possible using the hydraulically powered turbine steam admission valves. AFW flow is controlled using these valves during startup and shutdown, so operators are familiar with their use. Therefore, nominal AFW response was assumed following the postulated loss of MCC-5.

* Onset of seal LOCA assumed at 1 h—see MCC-5 failure and restoration.

MCC-5 Vulnerable to Failure When Power Restored

Following restoration of power, MCC-5 is vulnerable to failure if breaker 9C fails to operate. The failure probability of breaker 9C is assumed to be 0.1 (the same as the beta factor) since the breaker was exposed to the same maintenance practices that led to the failure of breaker 11C.

AC Power and MCC-5 Recovered in 1 h

For blackout sequences, both ac power and MCC-5 (or charging) must be recovered to prevent an RCP seal LOCA. The probability of not recovering both in 1 h (the time at which RCP seal LOCAs are assumed to begin) is estimated to be 0.17 based on a convolution approach.

When MCC-5 is not vulnerable to failure when power is restored, the probability of failing to recover ac power is estimated to be 0.12 based on LOOP recovery models described in ORNL/NRC/LTR-89/11.

Seal LOCA Probability

As discussed above for the event tree in Figure C.2.2, the probability of an RCP seal LOCA occurring at 1 h was assumed to be 0.7, consistent with other ASP analyses.

HPI High-Pressure Injection

Following the loss of MCC-5, HPI is lost (Haddam Neck IPE Table B-1, System/Function 2, Sump Recirculation). Restoration of power to MCC-5 is required to regain HPI function. The charging pumps are also unavailable following a loss of MCC-5 until they are realigned and restarted.

For an RCP seal LOCA following a station blackout, HPI recovery requires the recovery of both AC power and MCC-5 (or charging). The probability of failing to recover either of these, given they were not recovered at 1 h, is estimated to be 0.57. This value was approximated as:

$$p(\text{offsite power not recovered at 1.5 h} \mid \text{offsite power not recovered at 1 h}, 0.47) +$$

$$p(\text{MCC-5 not recovered at 1.5 h} \mid \text{MCC-5 not recovered at 1 h}, 0.17)\,.$$

AC Power Recovered in 6 h (Prior to Battery Depletion)

The probability of failing to recover offsite power before battery depletion at 6 h was estimated to be 0.037, based on LOOP recovery models described in ORNL/NRC/LTR-89/11. These models are based on the results of the data contained in NUREG-1032. The probabilities of ac recovery at 6 h, given it was not recovered at 1 h, were calculated as follows:

$$p(\text{offsite power recovered at 6 h} \mid \text{offsite power not recovered at 1 h and MCC-5 vulnerable to failure when power is restored})$$

$$= 0.037/0.17$$

$$= 0.22,$$

$$p(\text{offsite power recovered at 6 h} \mid \text{offsite power not recovered at 1 h and MCC-5 NOT vulnerable to failure when power is restored})$$

$$= 0.037/0.12$$

$$= 0.31.$$

C.2.4.4 Core Damage Probability Calculation

Calculations were structured to parallel the similar precursor analysis of MCC-5 potential unavailability coincident with PORV failures, which was performed in 1993 for AIT 213/93-80, LERs 213/93-006 and -007 (see NUREG/CR-4674, ORNL/NOAC-232, Vols. 19 and 20).

The impact of the failed PORVs on feed-and-bleed following postulated transients and small-break LOCAs was assessed by setting the PORVs to true (failed) in the model and calculating the associated conditional core damage probability given the initiator. This value was then multiplied by the probability that those initiators would occur during the time interval between startup in July 1993 and discovery of the PORV failure in Februar '994.

To address the loss of MCC-5 and the failed PORVs following a postulated LOOP, a conditioning event tree was used. This event tree characterizes potential plant conditions involving EDG success and failure, short-term (30 min) LOOP recovery, and short-term MCC-5 recovery. The event tree is shown in Figure C.2.3.

Table C.2.3 provides the relevant branch and conditioning sequence probabilities and identifies the calculation or IRRAS case associated with each sequence. Specific model probability modifications are indicated in the tables of selected basic events that are included with this analysis.

The conditional probabilities estimated in calculations 1A (feed-and-bleed unavailable during transients), 1B (feed-and-bleed unavailable following a small-break LOCA), 2-1 (conditioning sequences 1 and 3), 2-2 (conditioning sequences 2 and 4), Figure C.2.2 (seal LOCA for nonblackout sequences), and Figure C.2.3 (station blackout) were combined with the probabilities of such sequences occurring in the observation period to estimate the conditional probability for the combined event.

The sum of the probabilities for the sequences is 1.4×10^{-4}.

For operational events involving unavailabilities such as this event, the ASP Program estimates the core damage probability for the event by calculating the probability of core damage during the unavailability period conditioned on the failures observed during the event and subtracting a base-case probability for the same period, assuming plant equipment performs nominally. Because a conditioning event tree was used to analyze some of the sequences associated with a postulated LOOP, the computer code was not used to perform this differential calculation. Instead, the calculation program was used to calculate the probability of core damage given the conditions observed during the event and a postulated initiating event. This probability was then multiplied by the probability of the initiator during the unavailability period. The nominal core damage probability was estimated in the same way. For this analysis, the nominal core damage probability for the period analyzed was found to be small and was neglected.

Table C.2.3. Summary of conditional core damage probabilitie*s*

Sequence	p(sequence)	p(cd | sequence)	p(cd)	% Contribution
1A Transient	5.8×10^{-1}	5.2×10^{-5} (IRRAS Case 1A)	3.0×10^{-5}	21.0
1B Small-break LOCA	4.7×10^{-3}	6.6×10^{-4} (IRRAS Case 1B)	3.1×10^{-6}	2.2
2.1 LOOP*	5.5×10^{-2}	7.9×10^{-4} (IRRAS Case 2-1)	4.3×10^{-5}	30.0
2.2 LOOP*	3.3×10^{-4}	5.9×10^{-2} (IRRAS Case 2-2)	1.9×10^{-5}	13.3
		1.1×10^{-2} (seal LOCA, Fig. C.2.2.)	3.6×10^{-6}	2.5
2.3 LOOP*	1.7×10^{-2}	7.9×10^{-4} (IRRAS Case 2-1)	1.3×10^{-5}	9.1
2.4 LOOP*	1.3×10^{-4}	5.9×10^{-2} (IRRAS Case 2-2)	7.7×10^{-6}	5.4
		1.1×10^{-2} (seal LOCA, Fig. C.2.2.)	1.4×10^{-6}	1.0
2.5 LOOP*	1.7×10^{-4}	1.3×10^{-1} (blackout, Fig. C.2.3.)	2.2×10^{-5}	15.4
		Total	1.4×10^{-4}	100

*See Table C.2.2 for a description of the LOOP sequences.

C.2.5 Analysis Results

The conditional core damage probability estimated for the combined event is 1.4×10^{-4}. Postulated LOOPs (Cases 2.1 through 2.5) contribute approximately 77% of the core damage probability. The dominant sequence, shown in Figure C.2.4, which contributes about 30% of the total, involves a postulated LOOP, emergency power success, recovery of ac power and MCC-5, and failure of AFW and feed-and-bleed cooling. Selected basic event probabilities, sequence probabilities, system names, and conditional cut sets for each of the IRRAS cases are shown in Tables C.2.4 through C.2.19.

C.2.6 References

1. LER 213/94-004, Rev. 1, "Automatic 480 Volt Bus Transfer Failure Due to Circuit Breaker Malfunction," May 26, 1994.
2. LER 213/94-005, "Pressurizer PORVs Failed to Fully Stroke Open During Testing," March 18, 1994.
3. LER 213/94-007, "Potential for Radiological Release During Post-LOCA Sump Recirculation," April 5, 1994.
4. LER 213/94-013, "HPSI Pump Discharge Relief Valve Setpoint Found Low," June 3, 1994.
5. NRC Inspection Report 213/94-03, April 7, 1994.

4. LER 213/94-013, "HPSI Pump Discharge Relief Valve Setpoint Found Low," June 3, 1994.

5. NRC Inspection Report 213/94-03, April 7, 1994.

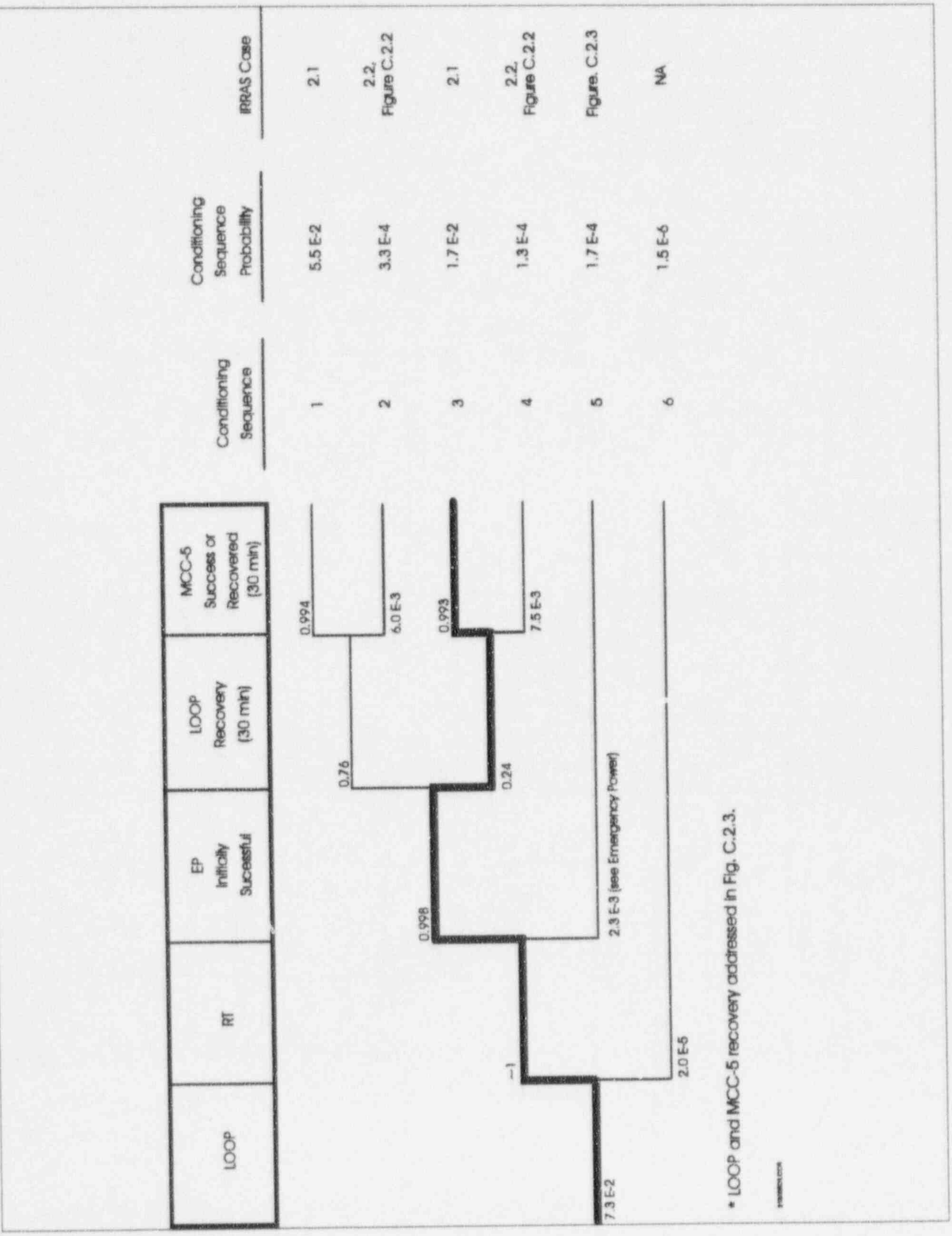


Figure C.2.1. Conditioning event tree for postulated LOOP.

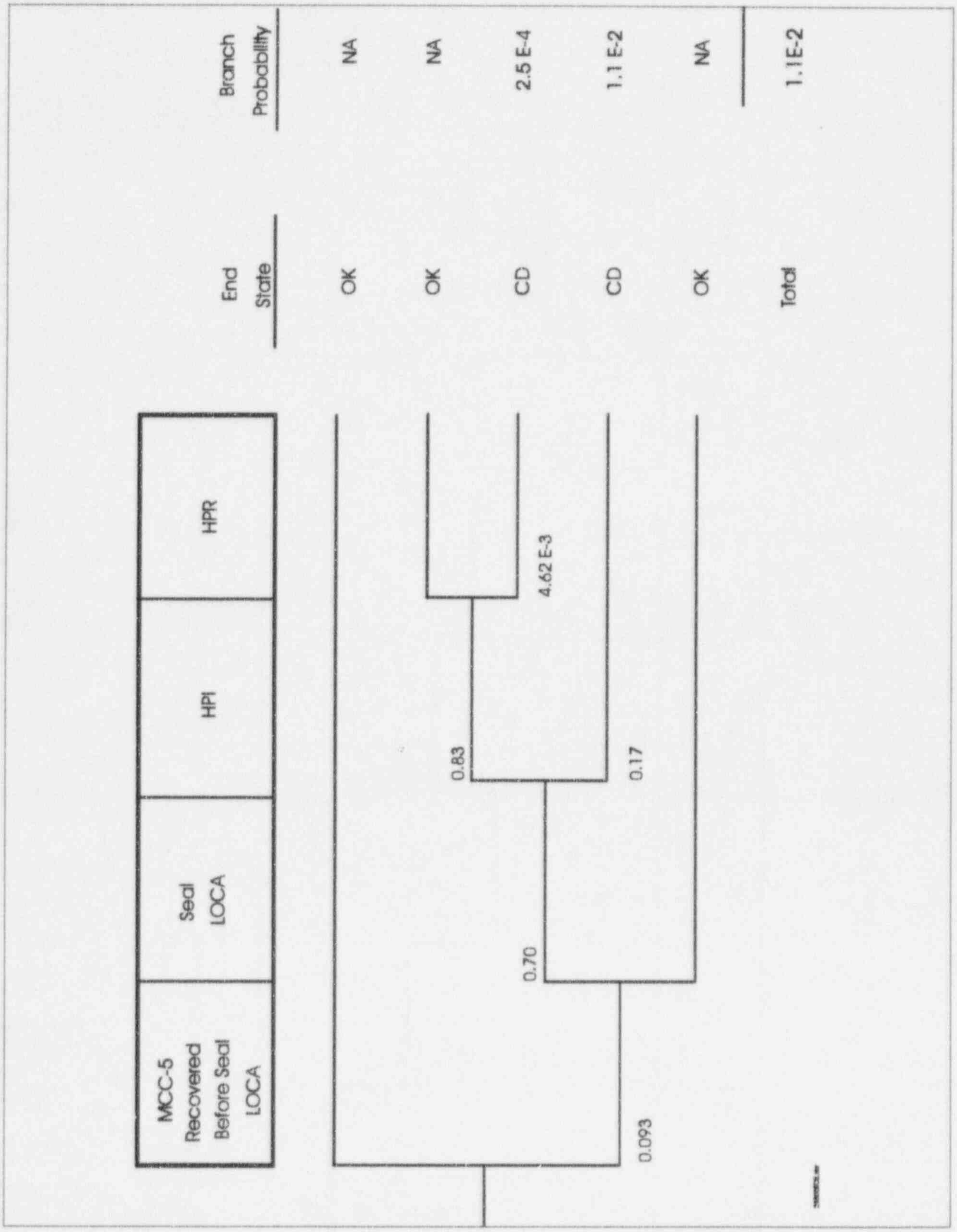


Figure C.2.2. Event tree for RCP seal LOCA (non-blackout sequences).

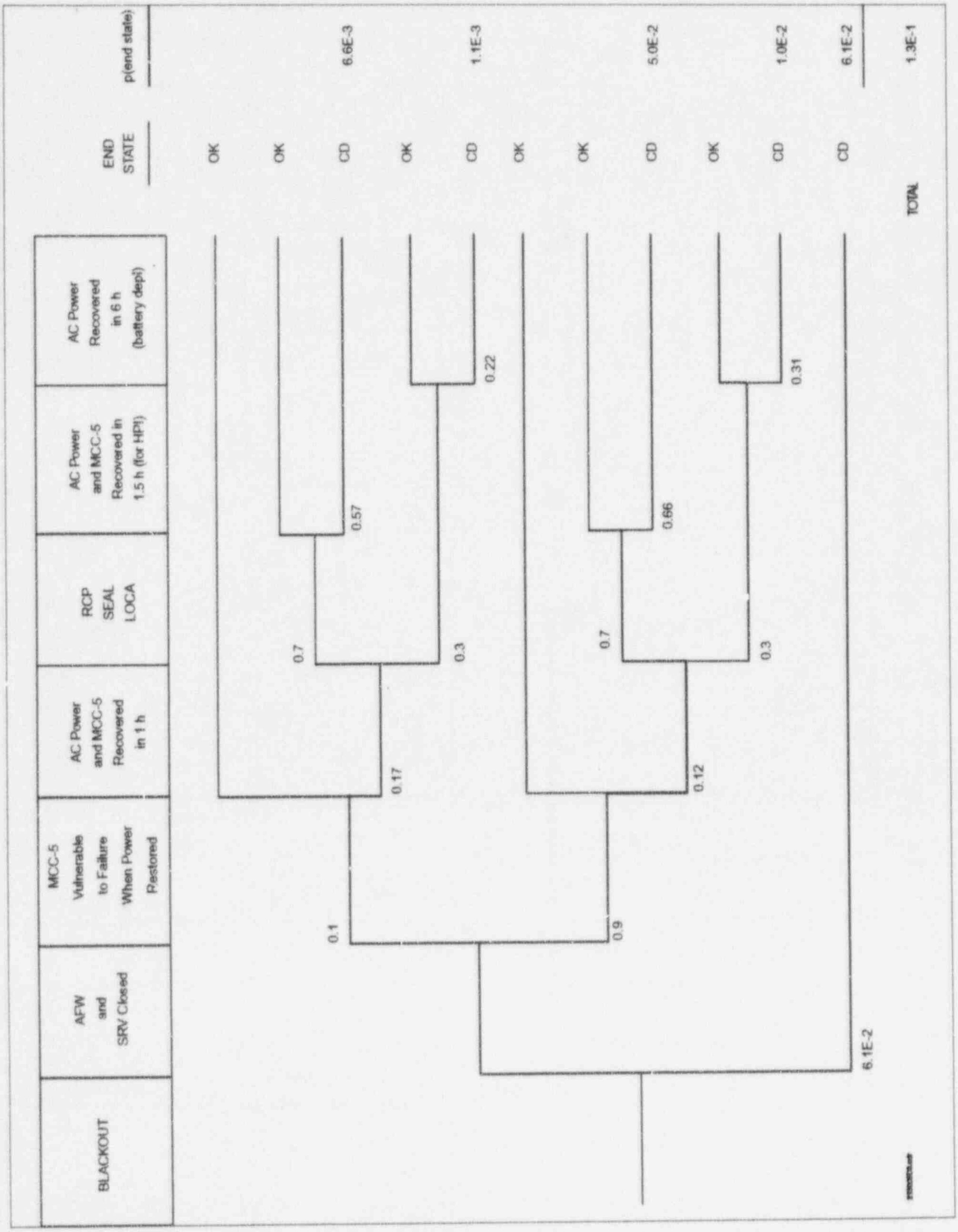


Figure C.2.3. Event tree model for blackout sequences.

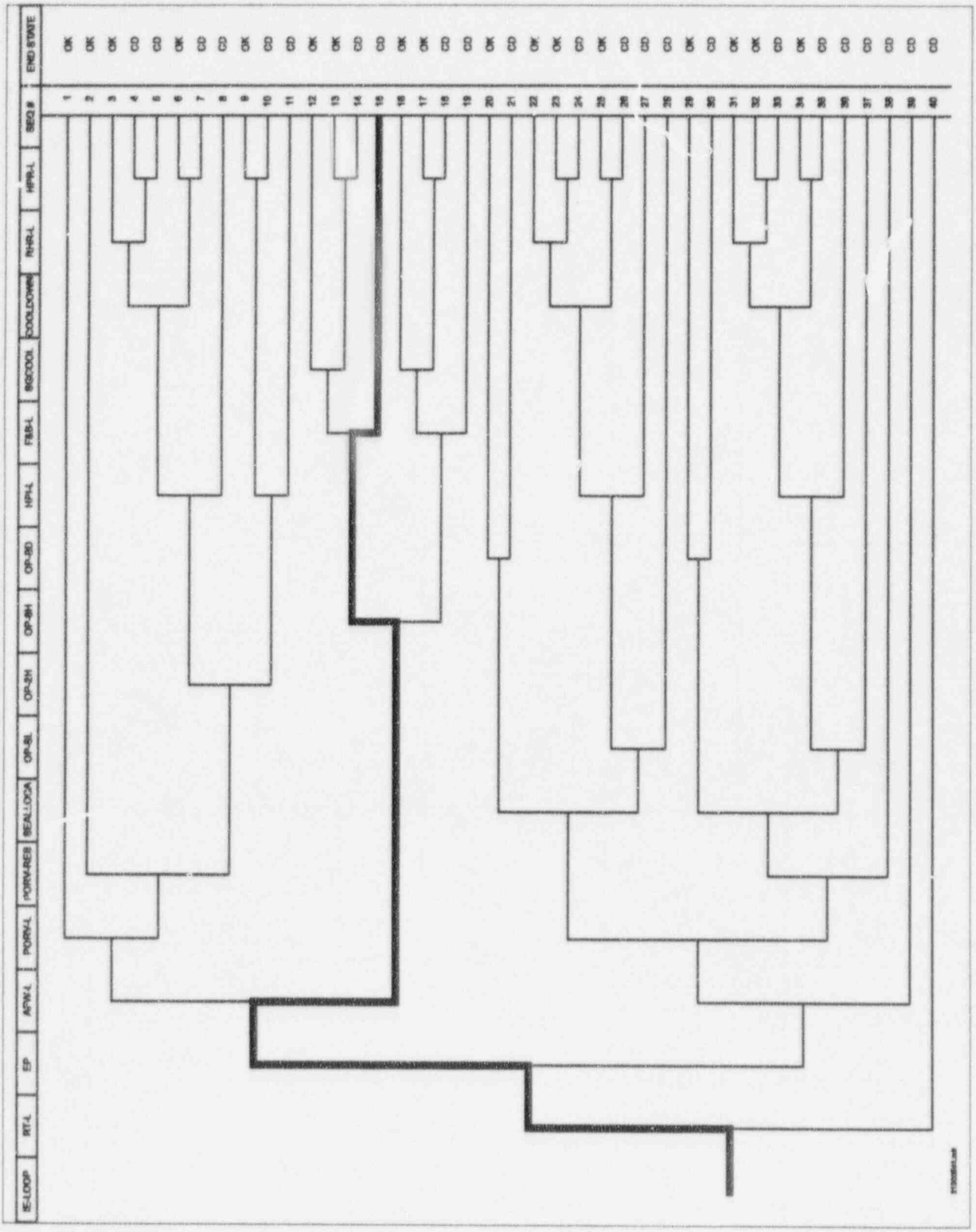


Figure C.2.4. Dominant core damage sequence for LER Nos. 213/94-004, -005, -007, -013 ; Inspection Report 213/94-03.

Table C.2.4. Selected basic events for Case 1A, PORVs unavailable during transients

Event name	Description	Base probability	Current probability	Type	Modified for this event
AFW-TDP-FC-1A	Failure of Turbine Driven Pump 1A	3.3E-002	3.3E-002		N
AFW-TDP-FC-1B	Failure of Turbine Driven Pump 1B	3.3E-002	3.3E-002		N
AFW-TDP-CF-AB	Common Cause Failures of Turbine Driven Pumps	1.4E-003	1.4E-003		N
AFW-XHE-NOREC	Operator Fails to Recover AFW System	2.6E-001	2.6E-001		N
AFW-XHE-NOREC-A	Operator Fails to Recover AFW System	2.6E-001	2.6E-001		N
AFW-XHE-RWSS-A	Operator Fails to Align Backup Water Source During ATWS	4.0E-002	4.0E-002		N
IE-LOOP	Loss-of-Offsite Power Initiating Event	8.5E-006	0.0E+000	IGNORE	Y
IE-SGTR	Steam Generator Tube Rupture Initiating Event	1.63E-006	0.0E+000	IGNORE	Y
IE-SLOCA	Small LOCA Initiating Event	1.0E-006	0.0E+000	IGNORE	Y
IE-TRANS	Transient Initiating Event	5.3E-004	1.0E+000	TRUE	Y
MFW-SYS-TRIP	Main Feedwater System Trips	2.0E-001	2.0E-001		N
MFW-XHE-NOREC	Operator Fails To Recover Main Feedwater	3.4E-001	3.4E-001		N
PPR-SRV-CC-PRV1	PORV 1 Fails To Open On Demand	6.3E-003	1.0E+000	TRUE	Y
PPR-SRV-CC-PRV2	PORV 2 Fails To Open On Demand	6.3E-003	1.0E+000	TRUE	Y
RPS-VCF-FO	Reactor Trip System Fails	6.0E-005	6.0E-005		N
RPS-XHE-XM-SCRAM	Operator Fails to Manually Trip The Reactor	3.4E-001	3.4E-001		N

Table C.2.5. Sequence probabilities for Case 1A, PORVs unavailable during transients

Event tree name	Sequence name	Frequency	% Contribution	Logic
TRANS	20	5.1E-005	98.3	/RT, AFW, MFW, F&B
TRANS	21-8	5.8E-007	1.1	RT, /RCSPRESS, AFW-ATWS
Total (all sequences)		5.2E-005	100.0	

Table C.2.6. System names for Case 1A, PORVs unavailable during transients

System name	Description
AFW	No or Insufficient AFW Flow
AFW-ATWS	No or Insufficient AFW Flow Following ATWS
F&B	Failure to Provide Feed-and-Bleed Cooling
MFW	Failure of the Main Feedwater System
RCSPRESS	Failure to Limit RCS Pressure to <3200 psi
RT	Reactor Fails to Trip During Transient

Table C.2.7. Conditional cut sets for higher probability sequences for Case 1A

Cut set No.	% Contribution	Frequency	Cut sets
TRANS Sequence: 20		5.1E-005	
1	48.0	2.4E-005	AFW-XHE-NOREC, MFW-SYS-TRIP, MFW-XHE-NOREC, AFW-TDP-CF-AB
2	37.4	1.9E-005	AFW-XHE-NOREC, AFW-TDP-FC-1B, MFW-SYS-TRIP, MFW-XHE-NOREC, AFW-TDP-FC-1A
TRANS Sequence: 21-8		5.8E-007	
1	36.0	2.1E-007	RPS-VCF-FO, RPS-XHE-XM-SCRAM, AFW-XHE-NOREC-A, AFW-XHE-RWSS-A
2	29.7	1.7E-007	RPS-VCF-FO, RPS-XHE-XM-SCRAM, AFW-XHE-NOREC-A, AFW-TDP-FC-1A
3	29.7	1.7E-007	RPS-VCF-FO, RPS-XHE-XM-SCRAM, AFW-XHE-NOREC-A, AFW-TDP-FC-1B
Total (all sequences)		5.2E-005	

Table C.2.8. Selected basic events for Case 1B
PORVs unavailable following a small-break LOCA

Event name	Description	Base probability	Current probability	Type	Modified for this event
AFW-TDP-FC-1A	Failure of Turbine Driven Pump 1A	3.3E-002	3.3E-002		N
AFW-TDP-FC-1B	Failure of Turbine Driven Pump 1B	3.3E-002	3.3E-002		N
AFW-TDP-CF-AB	Common Cause Failures of Turbine Driven Pumps	1.4E-003	1.4E-003		N
AFW-XHE-NOREC	Operator Fails to Recover AFW System	2.6E-001	2.6E-001		N
HPI-MOV-OC-SUC	Suction MOV From RWST Fails	4.0E-005	4.0E-005		N
HPI-XHE-NOREC	Operator Fails to Recover the HPI System	8.4E-001	8.4E-001		N
HPR-XHE-NOREC	Operator Fails to Recover the HPR System	1.0E-000	1.0E-000		N
IE-LOOP	Loss-of-Offsite Power Initiating Event	8.5E-006	0.0E+000	IGNORE	Y
IE-SGTR	Steam Generator Tube Rupture Initiating Event	1.63E-006	0.0E+000	IGNORE	Y
IE-SLOCA	Small LOCA Initiating Event	1.0E-006	1.0E+000	TRUE	Y
IE-TRANS	Transient Initiating Event	5.3E-004	0.0E+000	IGNORE	Y
MFW-SYS-TRIP	Main Feedwater System Trips	2.0E-001			N
MFW-XHE-NOREC	Operator Fails to Recover Main Feedwater	3.4E-001			N
PPR-SRV-CC-PRV1	PORV 1 Fails to Open on Demand	6.3E-003	1.0E+000	TRUE	Y
PPR-SRV-CC-PRV2	PORV 2 Fails to Open on Demand	6.3E-003	1.0E+000	TRUE	Y
RHR-HTX-CF-AB	Failure of Heat Exchangers Due to Common Cause	1.4E-005	1.4E-005		N
RHR-MDP-CF-ALL	RHR Motor Driven Pumps Fails Due to Common Cause	4.5E-004	4.5E-004		N
RHR-XHE-NOREC	Operator Fails to Recover the RHR System	1.0+000	1.0+000		N
RPS-VCF-FO	Reactor Trip System Fails	6.0E-005	6.0E-005		N
RPS-XHE-XM-SCRAM	Operator Fails to Manually Trip the Reactor	3.4E-001	3.4E-001		N

Table C.2.9. Sequence probabilities for Case 1B
PORVs unavailable following a small-break

Event tree name	Sequence name	Frequency	% Contribution	Logic
SLOCA	03	5.3E-004	80.4	/RT, /AFW, /HPI, /COOLDOWN, RHR, HPR
SLOCA	20	5.1E-005	7.7	/RT, AFW, MFW, F&B
SLOCA	06	3.6E-005	5.5	/RT, /AFW, HPI
SLOCA	21	2.0E-005	3.0	RT
SLOCA	05	1.8E-005	2.7	/RT, /AFW, /HPI, COOLDOWN, HPR
Total (all sequences)		7.1E-004		

Table C.2.10. System names for Case 1B
PORVs unavailable following a small-break LOCA

System name	Description
AFW	No or Insufficient AFW Flow
COOLDOWN	RCS Cooldown to RHR Pressure using TBVs, etc.
F&B	Failure to Provide Feed-and-Bleed Cooling
HPI	No or Insufficient Flow From the HPI System
HPR	No or Insufficient HPR Flow
MFW	Failure of the Main Feedwater System
RHR	No or Insufficient Flow From the RHR System
RT	Reactor Fails to Trip During Transient

Table C.2.11. Conditiona. cut sets for higher probability sequences for Case 1B

Cut set No.	% Contribution	Frequency	Cut sets
SLOCA Sequence: 3		5.3E-004	
1	83.9	4.5E-004	HPR-XHE-NOREC, RHR-MDP-CF-ALL, RHR-XHE-NOREC
SLOCA Sequence: 20		5.1E-005	
1	48.0	2.4E-005	AFW-XHE-NOREC, MFW-SYS-TRIP, MFW-XHE-NOREC, AFW-TDP-CF-AB
2	37.4	1.9E-005	AFW-XHE-NOREC, AFW-TDP-FC-1B, MFW-SYS-TRIP, MFW-XHE-NOREC, AFW-TDP-FC-1A
SLOCA Sequence: 06		3.6E-005	
1	92.1	3.3E-005	HPI-XHE-NOREC, HPI-MOV-OC-SUC
SLOCA Sequence: 21		2.0E-005	
1	100.0	2.0E-005	RPS-VCF-FO, RPS-XHE-XM-SCRAM
Total (all sequences)		7.1E-004	

Table C.2.12. Selected basic events for Case 2-1
LOOP conditioning sequences 1 and 3

Event name	Description	Base probability	Current probability	Type	Modified for this event
AFW-TDP-FC-1A	Failure of Turbine Driven Pump 1A	3.3E-002	3.3E-002		N
AFW-TDP-FC-1B	Failure of Turbine Driven Pump 1B	3.3E-002	3.3E-002		N
AFW-TDP-CF-AB	Common Cause Failures of Turbine Driven Pumps	1.4E-003	1.4E-003		N
AFW-TNK-FC-PWST	Primary Water Storage Tank Fails	4.1E-005	4.1E-005		N
AFW-XHE-NOREC-L	Operator Fails to Recover AFW System During Blackout	2.6E-001	2.6E-001		N
EPS-DGN-CF-ALL	Common Cause Failure of Diesel Generators	1.3E-003	+0.0E+000	FALSE	Y
EPS-DGN-FC-1A	Diesel Generator A Fails	4.2E-002	+0.0E+000	FALSE	Y
EPS-DGN-FC-1B	Diesel Generator B Fails	4.2E-002	+0.0E+000	FALSE	Y
IE-LOOP	Loss-of-Offsite Power Initiating Event	8.5E-006	1.0E+000	TRUE	Y
IE-SGTR	Steam Generator Tube Rupture Initiating Event	1.63E-006	0.0E+000	IGNORE	Y
IE-SLOCA	Small LOCA Initiating Event	1.0E-006	0.0E+000	IGNORE	Y
IE-TRANS	Transient Initiating Event	5.3E-004	0.0E+000	IGNORE	Y

Table C.2.12. Selected basic events for Case 2-1 LOOP conditioning sequences 1 and 3 (cont.)

Event name	Description	Base probability	Current probability	Type	Modified for this event
OEP-XHE-NOREC-2H	Operator Fails to Recover Offsite Power Within 2 hrs	2.2E-001	+0.0E+000		Y
OEP-XHE-NOREC-6H	Operator Fails to Recover Offsite Power Within 6 hrs	6.7E-002	+0.0E+000		Y
PPR-SRV-CC-PRV1	PORV 1 Fails to Open on Demand	6.3E-003	1.0E+000	TRUE	Y
PPR-SRV-CC-PRV2	PORV 2 Fails to Open on Demand	6.3E-003	1.0E+000	TRUE	Y
PPR-SRV-00-PRV1	PORV 1 Fails to Reclose After Opening	3.0E-002	3.0E-002		N
PPR-SRV-00-PRV2	PORV 2 Fails to Reclose After Opening	3.0E-002	3.0E-002		N
PPR-XHE-NOREC-L	Operator Fails to Close Block Valves During Loop	1.1E-002	1.0E+000	TRUE	Y

Table C.2.13. Sequence probabilities for Case 2-1 LOOP conditioning sequences 1 and 3

Event tree name	Sequence name	Frequency	% Contribution	Logic
LOOP	15	7.5E-004	95.5	/RT-L, /EP, AFW-L, /OP-6H, F&B-L
Total (all sequences)		7.9E-004	100.0	

Table C.2.14. System names for Case 2-1 LOOP conditioning sequences 1 and 3

System name	Description
AFW-L	No or Insufficient AFW Flow During LOOP
EP	Failure of Both Trains of Emergency Power
F&B-L	Failure of Feed-and-Bleed Cooling During LOOP
OP-6H	Operator Fails to Recover Offsite Power Within 6 hrs
RT-L	Reactor Fails to Trip During LOOP

Table C.2.15. Conditional cut sets for higher probability sequences for Case 2-1

Cut set No.	% Contribution	Frequency	Cut sets
LOOP Sequence: 15		7.5E-004	
1	48.1	3.6E-004	AFW-XHE-NOREC-L, AFW-TDP-CF-AB
2	37.4	2.8E-004	AFW-TDP-FC-1A, AFW-TDP-FC-1B, AFW-XHE-NOREC-L
Total (all sequences)		7.9E-004	

Table C.2.16. Selected basic events for Case 2-2 LOOP conditioning sequences 2 and 4

Event name	Description	Base probability	Current probability	Type	Modified for this event
AFW-TDP-FC-1A	Failure of Turbine Driven Pump 1A	3.3E-002	3.3E-002		N
AFW-TDP-FC-1B	Failure of Turbine Driven Pump 1B	3.3E-002	3.3E-002		N
AFW-TDP-CF-AB	Common Cause Failures of Turbine Driven Pumps	1.4E-003	1.4E-003		N
AFW-XHE-NOREC-L	Operator Fails to Recover AFW System During Blackout	2.6E-001	2.6E-001		N
EPS-DGN-CF-ALL	Common Cause Failure of Diesel Generators	1.3E-003	+0.0E+000	FALSE	Y
EPS-DGN-FC-1A	Diesel Generator A Fails	4.2E-002	+0.0E+000	FALSE	Y
EPS-DGN-FC-1B	Diesel Generator B Fails	4.2E-002	+0.0E+000	FALSE	Y
HPI-MDP-FC-1A	HPI Motor Driven Pump 1A Fails	3.9E-003	1.0E+000	TRUE	Y
HPI-MDP-FC-1B	HPI Motor Driven Pump 1B Fails	3.9E-003	1.0E+000	TRUE	Y
HPI-XHE-NOREC-L	Operator Fails to Recover the HPI System	8.4E-001	1.0E+000	TRUE	Y
HPR-XHE-NOREC-L	Operator Fails to Recover the HPR System	1.0E-003	1.0E+000		
IE-LOOP	Loss-of-Offsite Power Initiating Event	8.5E-006	1.0E+000	TRUE	Y
IE-SGTR	Steam Generator Tube Rupture Initiating Event	1.63E-006	0.0E+000	IGNORE	Y
IE-SLOCA	Small LOCA Initiating Event	1.0E-006	0.0E+000	IGNORE	Y

Table C.2.16. Selected basic events for Case 2-2 LOOP conditioning sequences 2 and 4 (cont.)

Event name	Description	Base probability	Current probability	Type	Modified for this event
IE-TRANS	Transient Initiating Event	5.3E-004	0.0E+000	IGNORE	Y
OEP-XHE-NOREC-2H	Operator Fails to Recover Offsite Power Within 2 hrs	2.2E-001	2.7E-001		Y
OEP-XHE-NOREC-6H	Operator Fails to Recover Offsite Power Within 6 hrs	6.7E-002	3.7E-002		Y
PPR-SRV-CC-PRV1	PORV 1 Fails to Open on Demand	6.3E-003	1.0E+000	TRUE	Y
PPR-SRV-CC-PRV2	PORV 2 Fails to Open on Demand	6.3E-003	1.0E+000	TRUE	Y
PPR-SRV-OO-PRV1	PORV 1 Fails to Reclose After Opening	3.0E-002	3.0E-002		N
PPR-SRV-OO-PRV2	PORV 2 Fails to Reclose After Opening	3.0E-002	3.0E-002		N
PPR-XHE-NOREC-L	Operator Fails to CLose Block Valves During LOOP	1.1E-002	1.0E+000	TRUE	Y

Table C.2.17. Sequence probabilities for Case 2-2 LOOP conditioning sequences 2 and 4

Event tree name	Sequence name	Frequency	% Contribution	Logic
LOOP	08	5.9E-002	98.7	/RT-L, /EP, /AFW-L, PORV-L, PRVL-RES, /OP-2H, HPI-L
LOOP	15	7.5E-004	1.2	/RT-L, /EP, AFW-L, /OP-6H, F&B-L
Total (all sequences)		5.9E-002	100.0	

Table C.2.18. System names for Case 2-2 LOOP conditioning sequences 2 and 4

System name	Description
AFW-L	No or Insufficient AFW Flow During LOOP
EP	Failure of Both Trains of Emergency Power
F&B-L	Failure of Feed-and-Bleed Cooling During LOOP
HPI-L	No or Insufficient Flow From the HPI System During LOOP
OP-2H	Operator Fails to Recover Offsite Power Within 2 hrs
OP-6H	Operator Fails to Recover Offsite Power Within 6 hrs
PORV-L	PORVs Open During LOOP
PRVL-RES	PORVs and Block Valves Fail to Reseat (EP Successful)
RT-L	Reactor Fails to Trip During LOOP

Table C.2.19. Conditional cut sets for higher probability sequences for Case 2-2

Cut set No.	% Contribution	Frequency	Cut sets
LOOP Sequence: 08		5.9E-002	
1	50.0	3.0E-002	PPR-SRV-OO-PRV1
2	50.0	3.0E-002	PPR-SRV-OO-PRV2
LOOP Sequence: 15		7.5E-004	
1	48.1	3.6E-004	AFW-XHE-NOREC-L, AFW-TDP-CF-AB
2	37.4	2.8E-004	AFW-TDP-FC-1A, AFW-TDP-FC-1B, AFW-XHE-NOREC-L
Total (all sequences)		5.9E-002	

C.3 LER No. 237/94-018

Event Description: Motor Control Center Trips Due to Improper Breaker Settings

Date of Event: June 8, 1994

Plant: Dresden 2

C.3.1 Summary

Following an unexpected trip of a motor control center (MCC) at Dresden 2 during surveillance testing, three MCCs were identified at Dresden 2 and Dresden 3 with improperly set feeder breakers. A review of MCC loading indicated that load additions since the original settings were determined had created an overload situation. For two of the MCCs, the overload condition would only have existed if an emergency diesel generator (EDG) had been running following a reactor trip with offsite power available. Load shedding following a loss-of-offsite power (LOOP) would have precluded an overload condition for this initiating event. For one of the MCCs, the overload condition would also have existed following a LOOP. The conditional core damage probability estimated for the event is 6.1×10^{-6}.

C.3.2 Event Description

On June 8, 1994, Dresden Unit 2 was operating at 99% power, and Unit 3 was in refueling. The Unit 2/3 standby gas treatment (SBGT) system was in operation, and a 24-h endurance run for EDG 3 was in progress, as was a Unit 2 high-pressure coolant injection (HPCI) surveillance.

Shortly after the Unit 2 HPCI auxiliary oil pump started, MCC 39-2 tripped. As a result of the loss of power at MCC 39-2, (1) EDG 3 tripped on high temperature following loss of power to its cooling water pump and ventilation fan, (2) the 125-V dc and 250-V dc battery systems had to be realigned to alternate chargers, (3) a half-scram for Unit 3 was generated as a result of loss of power to a reactor protection system (RPS) motor-generator, and (4) SBGT train A automatically started following loss of power to train B components.

MCC 39-2 loads were stripped, and the MCC feeder breaker was reclosed. MCC 39-2 loads were reenergized within 30 min of the breaker trip.

The trip of MCC 39-2 was caused by an incorrectly set feeder breaker. The feeder breaker for the MCC had a General Electric dashpot type EC-2A overcurrent trip device, which was original equipment. The setting for this breaker was 400 A. A review of the original loading on the MCC indicated that the 400-A setting was adequate, but load additions made to the MCC over time had increased the available running load current above the 400-A setting.

Two other breakers were subsequently identified with similar problems—MCC 28-3 and 38-3. The EC-2A trip devices for both of these MCCs had been replaced with newer General Electric solid state type RMS-9 trip devices. Both of these MCCs were also set to trip at 400 A. The licensee noted in the licensee event report (LER) that the setting for MCC 38-3 was chosen to be identical with the original breaker setting based on the assumption that MCC loading had not changed over time. However, since the loading had changed, the total connected load was greater than the protective device setting. At the time of the MCC 28-3 trip device replacement, it was recognized that the overcurrent setting was lower than the total connected load. However, it was assumed that the running load during accident conditions would be within the setting of the protective device.

Based on the loads associated with each MCC, the licensee concluded that MCCs 38-3 and 39-2 could be overloaded and trip during a safety actuation in which the associated EDG was running (e.g., for testing or following a spurious start) while offsite power was still available. For these MCCs, loads shed following a LOOP would preclude an overload condition. For MCC 28-3, however, the overload condition could exist for both LOOPs and other events in which the associated EDG was running.

C.3.3 Additional Event-Related Information

Three EDGs provide emergency power to the two Dresden units: EDG 2 provides power to Unit 2 bus 24-1, EDG 3 provides power to Unit 3 bus 34-1, and swing EDG 2/3 provides power to either Unit 2 bus 23-1 or Unit 3 bus 33-1 in the event of a LOOP on Unit 2 or Unit 3, respectively. In the event of a dual-unit LOOP with a loss-of-coolant accident (LOCA) on one unit, EDG 2/3 provides power to the unit with the LOCA. In the event of a dual-unit LOOP without a LOCA, EDG 2/3 powers the unit that suffers the LOOP first. Unit 2 bus 24-1 and Unit 3 bus 34-1 can be cross-tied by closing two normally open breakers.

Two 250-V dc and two 125-V dc batteries are shared between both units. The 250-V dc batteries primarily power large loads, such as dc-powered pumps and valves, while the 125-V dc batteries provide control power to components such as circuit breakers. Battery chargers that normally supply dc power and provide battery charging can be powered from buses associated with EDG 2 (Unit 2) or EDG 3 (Unit 3) or the swing EDG. Each battery is sized to power its respective loads for 4 h.

The isolation condenser (IC) and HPCI can provide decay heat removal in the event of a LOOP with unavailability of on-site ac power. Diesel-driven pumps provide IC secondary side makeup in this case. Since the IC does not provide RPV makeup, it cannot be used if an SRV sticks open or if a recirculation pump seal fails. The model also assumes that if ac power (the EDGs or offsite power) is not recovered prior to battery depletion core damage occurs. Following battery depletion, all instrumentation would be lost, as would control power for breaker, turbine-driven pump, and dc valve operation. Potential recovery after this time, although possible, is extremely difficult and beyond the scope of this analysis.

C.3.4 Modeling Assumptions

Four possible situations were addressed in the analysis of this complex event. All three MCCs could have tripped following an initiating event in which emergency core cooling system (ECCS) actuation was required, offsite power was available, and the EDG associated with the MCC was running (e.g., for testing or following a spurious start). Analysis Case 1a addresses the situation in which one EDG was running. Analysis Case 1b addresses the situation in which two EDGs were running. In addition, MCC 28-3 could have tripped following a LOOP. Analysis Cases 2a and 2b consider a plant-centered LOOP at Unit 2 and dual-unit LOOPs at Units 2 and 3. In all cases, the MCCs were assumed to trip if they could have tripped. This assumption may be conservative.

Case 1a. Postulated initiating event with offsite power available and one EDG running. This situation could exist if a transient or small-break LOCA occurred and one of the two EDGs associated with a unit was undergoing monthly surveillance testing. The greatest potential impact is associated with MCCs 39-2 and 38-3 at Unit 3. These MCCs, in addition to supplying power to EDG components (and turning gear components for MCC 38-3), also supply power to containment cooling service water (CCSW) cubicle fans. CCSW provides decay heat removal for the containment cooling mode of low-pressure coolant injection. The analysis assumed the two CCSW trains associated with the running EDG would be unavailable after the MCC tripped. The trip of MCC 38-3 at Unit 3 (and 28-3 at Unit 2) also impacts fire protection panel FP-3 (and FP-2). The analysis assumes these panels do not influence the use of firewater as an alternate source of low-pressure injection. The probability of a running EDG was estimated to be 1.4×10^{-3}, based on an assumed 1-h surveillance run-time for each EDG per month.

The significance for this case was estimated by setting basic events associated with the two impacted CCSW trains to true (failed) and calculating the increase in core damage probability for non-LOOP (transient and small-break LOCA) initiating events over a 1-year period using the IRRAS-based ASP model for Dresden. Long-term unavailabilities such as this event have typically been modeled in the ASP Program for a 1-year period, assuming the plant was at power 70% of the time; this is equal to 6132 h (365 d × 24 h/d × 0.7). The increase in core damage probability was multiplied by the probability that an EDG would be running to estimate the conditional probability for Case 1a. This conditional probability is less than 1.0×10^{-8}. Since this is substantially below the 1.0×10^{-6} documentation limit used in the ASP Program, the calculational results are not inciuded here.

Case 1b. Postulated initiating event with offsite power available and two EDGs running. This situatirn could exist if a transient or a small-break LOCA occurred and both EDGs associated with a unit were spuriously started. The analysis for this case is similar to Case 1a, except all trains of CCSW were assumed to be unavailable. The probability of spurious EDG start was estimated using a Sequence Coding and Search System search of Boiling Water Reactor (BWR) automatic or manual reactor trips with spurious EDG starts. Three such events were identified in 573 trips from power, resulting in an estimated probability of spurious EDG actuation of 5.2×10^{-3}. The resulting conditional core damage probability is estimated to be 4.3×10^{-8}, also well below 1.0×10^{-6}. As for Case 1a, the calculational results are not included here.

Case 2a. Postulated plant-centered LOOP at Unit 2. For a postulated plant-centered LOOP at Unit 2 only, offsite power remains available at Unit 3. Trip of MCC 28-3 will result in inoperability of swing EDG 2/3 and unavailability of power to 4-kV bus 23-1. Power can be recovered to bus 24-1 if EDG 2 fails by recovering offsite power or by closing the cross-tie from Unit 3 bus 34-1. Because of the shared dc system at Dresden, dc power will remain available for instrumentation even if Unit 2 batteries are depleted. Therefore, a sequence involving safety relief valve (SRV) reseat and isolation condenser or HPCI success following a postulated station blackout will not proceed to core damage (essentially all of sequence 44).

The probability of failing to recover power to bus 24-1 through closure of the cross-tie breakers from Unit 3 was assumed to be 0.12 [Accident Sequence Precursor (ASP) nonrecovery class R3, see Appendix A, Sect. A.1 to the 1992 Annual Report, NUREG/CR-4674, Vol. 17]. This value was chosen because recovery appeared possible in the required time from the control room, but was not considered routine (the value chosen for this failure probability for this case is considered a bounding probability and does not substantially impact the overall analysis results). This value is used in lieu of the failure probability for EDG 3 in the IRRAS-based ASP models to reflect the failure to provide power from bus 34-1. The probability of EDG common-cause failure was set to false to reflect the unavailability of EDG 2/3 and the availability of power on bus 34-1.

After elimination of sequence 44 of the LOCP tree shown in Figure C.3.1 (since it does not proceed to core damage for a single-unit plant-centered LOOP), a conditional core damage probability of 1.6×10^{-8} is estimated. As for Cases 1a and 1b, the calculational results are not included here.

Case 2b. Dual-unit LOOP at Units 2 and 3. For a postulated dual-unit LOOP (primarily grid- and weather-related LOOPs), offsite power is unavailable to both units. If the LOOP occurs at Unit 2 first, trip of MCC 28-3 will result in unavailability of swing EDG 2/3. EDG 3 will be required to power Unit 3 loads, leaving only EDG 2 to supply power to Unit 2 loads (except for battery charging, which can be provided by either EDG 2 or EDG 3).

The frequency of a dual-unit LOOP and the probability of failing to recover offsite power in the short-term and before battery depletion were estimated to be 1.7×10^{-2}/year, 0.66, and 0.21, respectively, based on models described in *Revised LOOP Recovery and PWR Seal LOCA Models*, ORNL/NRC/LTR-89/11, August 1989. These models are based on the results of data distributions contained in *Evaluation of Station Blackout at Nuclear Power Plants*, NUREG-1032. The probability of the dual-unit LOOP occurring first at Unit 2 was assumed to be 0.5. This value is based on the assumption that a dual-unit LOOP has an equal probability of occurring first at either unit. Therefore, the initiating event probability is equal to (1.7×10^{-2}/year $\times$ 0.66 $\times$ 0.5 $\times$ 1 year). The failure probability for EDG 2/3 was set to true to reflect its unavailability following a trip of MCC 28-3. The common-cause failure probability for the EDGs was revised to 4.4×10^{-3} to reflect the unavailability of EDG 2/3. Sequence 44, which involves failure of emergency power and failure to recover offsite power prior to battery depletion, dominates the analysis results. For this sequence to occur, both EDG 2 and EDG 3 must fail; otherwise power for battery charging will exist and the batteries will not deplete. The resulting conditional core damage probability is estimated to be 6.1×10^{-6}. This is the only case that significantly contributes to the conditional core damage probability for this event. The calculational results are shown in Tables C.3.1 through C.3.5.

C.3.5 Analysis Results

The conditional core damage probability estimated for this event is 6.1×10^{-6}. The dominant core damage sequence, highlighted on the event tree in Figure C.3.1, involves a postulated dual-unit LOOP (Case 2b) with subsequent failure of all three Dresden EDGs and failure to recover offsite power prior to battery depletion. In the dominant sequence, EDG 2/3 fails due to MCC 28-3 trip following its alignment to Unit 2 (the postulated dual-unit LOOP affects Unit 2 first), and EDG 2 and 3 fail for unspecified reasons (random or common-cause failures).

The calculational results for Cases 1a, 1b, and 2a were not included since they do not provide a significant contribution to the conditional core damage probability for the event. The calculational results for Case 2b are shown in Tables C.3.1 through C.3.5. Definitions and probabilities for selected basic events are shown in Table C.3.1. The conditional probabilities associated with the highest probability sequences are shown in Table C.3.2. Table C.3.3 lists the sequence logic associated with the sequences listed in Table C.3.2. Table C.3.4 describes the system names associated with the dominant sequences. Cut sets associated with each sequence are shown in Table C.3.5.

C.3.6 Reference

1. LER 237/94-018, "Potential Trip of Motor Control Centers Due to Improper Feed Breaker Settings," July 7, 1994.

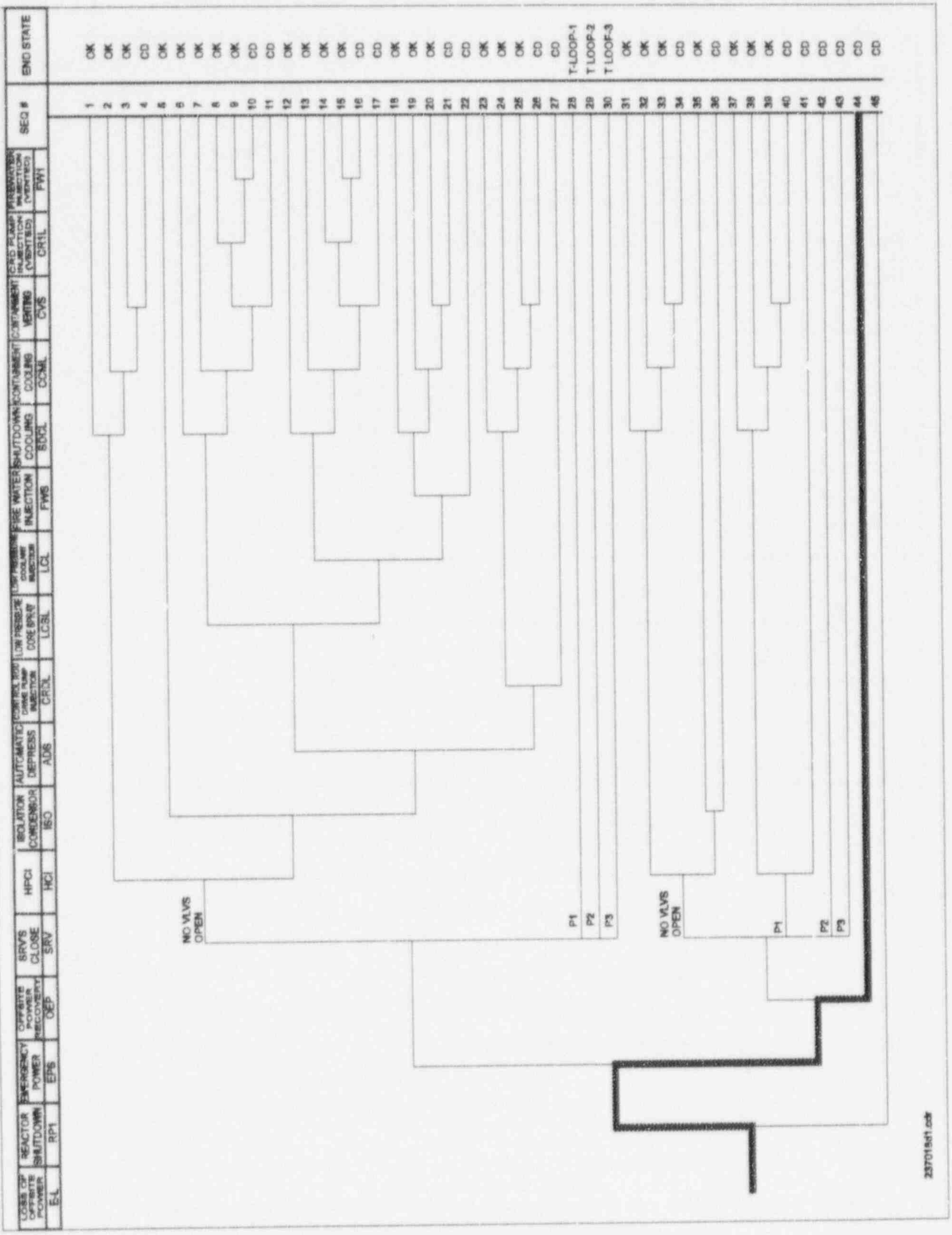


Figure C.3.1. Dominant core damage sequence for LER No. 237/94-018 (see Case 2b).

Table C.3.1. Definitions and probabilities for selected basic events for LER 237/94-018 (Case 2b)

Event name	Description	Base probability	Current probability	Type	Modified for this event
EPS-DGN-CF-DGNS	Common Cause Failure of Diesel Generators	1.2E-003	4.4E-003		Y
EPS-DGN-FC-DG2	Unit 2 Generator Fails	4.4E-002	4.4E-002		N
EPS-DGN-FC-DG3	Unit 3 Diesel Generator Failure	4.4E-002	4.4E-002		N
EPS-DGN-FC-DG23	Swing Diesel Generator Fails	4.4E-002	1.0E+000	TRUE	Y
EPS-XHE-XE-NOREC	Operator Fails to Recover Emergency Power	8.0E-001	8.0E-001		N
IE-LOOP	Loss-of-offsite Power Initiator	9.1E-007	5.6E-003		Y
IE-SLOCA	Small LOCA Initiator	1.7E-006	0.0E+000	IGNORE	Y
IE-TRAN	Transient Initiator	3.4E-004	0.0E+000	IGNORE	Y
OEP-XHE-XE-NOREC	Operator Fails to Recover Offsite Power	2.1E-001	2.1E-001		N

Table C.3.2. Sequence conditional probabilities for LER 237/94-018 (Case 2b)

Event tree name	Sequence name	Conditional core damage probability (CCDP)	Core damage probability (CDP)	Importance (CCDP-CDP)	% Contribution
LOOP	44	5.9E-006	3.5E-006	2.3E-006	96.7
Total (all sequences)		6.1E-006			

Table C.3.3. Sequence logic for dominant sequences for LER 237/94-018 (Case 2b)

Event tree name	Sequence name	Logic
LOOP	44	/RP1, EPS, OEP

Table C.3.4. System names for LER 237/94-018 (Case 2b)

System name	Description
EPS	Emergency Power System Fails
OEP	Offsite Power Recovery
RP1	Reactor Shutdown Fails

Table C.3.5. Conditional cut sets for higher probability sequences for LER 237/94-018

Cut set No.	% Contribution	Frequency	Cut sets
LOOP Sequence: 44		6.0E-006	
1	69.5	4.1E-006	EPS-DGN-CF-DGNS, EPS-XHE-XE-NOREC, OEP-XHE-XE-NOREC
2	30.6	1.8E-006	EPS-XHE-XE-NOREC, OEP-XHE-XE-NOREC, EPS-DGN-FC-DG2, EPS-DGN-FC-DG3
Total (all sequences)		6.0E-006	

C.4 LER No. 237/94-021

Event Description: Long-Term Unavailability of High Pressure Coolant Injection

Date of Event: August 4, 1994

Plant: Dresden Unit 2

C.4.1 Summary

On August 4, 1994, at 1559 hours, with the plant at 99% power, the high pressure coolant injection (HPCI) turbine tripped due to high exhaust pressure during a monthly surveillance test. The cause of the high exhaust pressure was determined to be a failed check valve (No. 2-2301-74). The failure mechanism indicated that, since the last monthly surveillance test, the HPCI turbine would have tripped shortly after starting if the HPCI system had been needed to perform its safety function. The conditional core damage probability estimated for this event is 3.1×10^{-6}.

C.4.2 Event Description

On August 4, 1994, at 1559 hours, with the plant at 99% power, the HPCI turbine failed the monthly surveillance test. Prior to the automatic trip, the turbine was run up to 2500 rpm and manually tripped per the surveillance after running for approximately 5 min. The turbine was restarted and automatically tripped after 1 min due to high exhaust pressure (100 psig). An inspection of the turbine drain system was performed, and the rupture diaphragm was replaced. On August 7, 1994, the HPCI turbine was retested. When the turbine was started, the exhaust pressure increased at a higher than normal rate, and the turbine was manually tripped at an exhaust pressure of 30 psig to avoid an automatic trip. At this point, the turbine exhaust check valves were examined. A local leak rate test of the check valve volume was performed, and leakage that exceeded the technical specification limit was found. Since the HPCI exhaust line check valves could not be repaired on line, the reactor was shut down on August 8, 1994.

The two HPCI turbine exhaust valves (2-2301-45 and 2-2301-74) were disassembled and inspected (see Figure C.4.1). The valve seats for 2-2301-45 were found to be slightly worn due to normal valve operation. This condition did not affect the operation of the HPCI system. When valve 2-2301-74 was disassembled and inspected, the valve disk was not attached to the valve guide piston. Further inspection revealed that the four tack welds, which prevent the assembly from rotating, had broken recently due to fatigue. Exhaust pressure observed on previous tests was determined to have been normal, supporting the assumption that the tack welds failed during the most recent test run. Once the tack welds were broken and the valve disc was off the closed seat, the steam flow was able to rapidly rotate the valve disc on the valve stem, causing the valve to close by elongating the stem and valve disc assembly. This, in turn, caused the exhaust pressure to increase as observed in the last two tests.

C.4.3 Additional Event-Related Information

The HPCI system is designed to pump water into the reactor vessel under loss-of-coolant accident (LOCA) conditions that do not result in rapid depressurization of the reactor pressure vessel (RPV). The HPCI system is designed to pump 5600 gpm within an RPV pressure range of about 165 to 1135 psia. The size of the system is selected to provide sufficient core cooling to prevent clad melting until the RPV pressure decreases to the point where the core spray system and/or the low-pressure coolant injection (LPCI) subsystem become effective.

For medium-break LOCAs, RPV pressure decays away too slowly for the low-pressure injection pumps to inject and prevent core damage without operator action to depressurize. Therefore, following HPCI failure, the automatic depressurization system (ADS) is required to depressurize the RPV so that core spray and/or the LPCI subsystem become effective.

C.4.4 Modeling Assumptions

The event was modeled as a long-term nonrecoverable unavailability of HPCI. Once the tack welds broke, the exhaust check valve elongated itself closed in a matter of minutes (approximately 6 min during the failed surveillance). At this point, the exhaust pressure would increase to the turbine trip set point (unless the pump was manually tripped). It was assumed that any safety demand for the HPCI turbine, subsequent to the last successful monthly surveillance, would have resulted in several minutes of high pressure injection followed by a HPCI turbine trip. Therefore, the HPCI train was modeled as failed (HCI-TDP-FC-TRAIN set to TRUE). The difficulty encountered in identifying the root cause of the pump failure indicates that the failure would not have been recovered during an actual demand. Therefore, the failure was modeled as nonrecoverable (HCI-XHE-XE-NOREC set to TRUE). The HPCI system was considered unavailable for one surveillance period (i.e., 720 h) prior to the failed surveillance. The system was also unavailable for an additional 107 h following the failed surveillance prior to the unit shutdown. As a result, a total failure period of 827 h was modeled.

The run time involved in a successful surveillance of the HPCI turbine is less than the subsequent mission time that would be required in certain accident scenarios. If the running vibration of the turbine is considered to be a significant contributor to the tack weld failure mechanism, then previous tests could be viewed as consuming the remaining run time available prior to the tack weld failure. Under this scenario, the failure period could include several previous successful surveillances. If this were the case, the 827-h unavailability period would be increased to encompass these additional surveillance periods. However, this time period is difficult to estimate with the information available. Therefore, the 827-h failure period modeled was utilized, although this may be nonconservative.

A loss of the HPCI turbine leaves the plant more susceptible to core damage from a medium-break LOCA; therefore, a medium-break LOCA event tree was added to the model that is consistent with the event tree in the Dresden individual plant examination (IPE). The existing fault trees that are used in conjunction with the other event trees for Dresden were applied to the medium-break LOCA event tree. The medium-break LOCA initiating event frequency was modified to 8×10^{-4}/year, consistent with the value used in the Dresden IPE (Table 1.5.1-1). This was converted to a per hour frequency of 1.3×10^{-7} by dividing the 8×10^{-4}/year value by 6132 h, assuming a 70% plant availability [(365 days/year) (24 h/day) (0.7 unit availability)].

Two different values were used for the operator error prevents depressurization probability under different conditions.For medium-break LOCAs and transient-induced medium-break LOCAs (sequences 39 and 38–39), a probability of 0.01 was used. For conditions where a medium-break LOCA were not present, a value of 0.001 was used. These values were derived from a review of the individual plant examinations (IPEs) for a number of BWRs.

C.4.5 Analysis Results

The conditional core damage probability estimated for this event is 3.1×10^{-6}. The dominant sequence highlighted on the event tree in Figure C.4.2 involves a postulated medium-break LOCA, failure of HPCI, and failure of ADS.

For BWRs with isolation condensers (ICs) loss of HPCI under a medium-break LOCA (or transient-induced medium-break LOCA) requires the use of the ADS system to depressurize to allow injection of low-pressure systems. Medium-break LOCAs are defined as those that do not depressurize the system fast enough to allow low-pressure systems to be effective on their own. However, core damage will be minimal if depressurization fails because the break will eventually cause sufficient depressurization to allow low-pressure systems to inject. If HPCI works for a short period of time prior to failure, this will accelerate the depressurization such that ADS may not be required. The two medium-break LOCA sequences (39 and 38–39) contribute 63% of the overall conditional core damage probability for this event.

Definitions and probabilities for basic events are shown in Table C.4.1. The conditional probabilities associated with the highest probability sequences are shown in Table C.4.2. Table C.4.3 lists the sequence logic associated with the sequences listed in Table C.4.2. Table C.4.4 describes the system names associated with the dominant sequences. Cutsets associated with each sequence are shown in Table C.4.5.

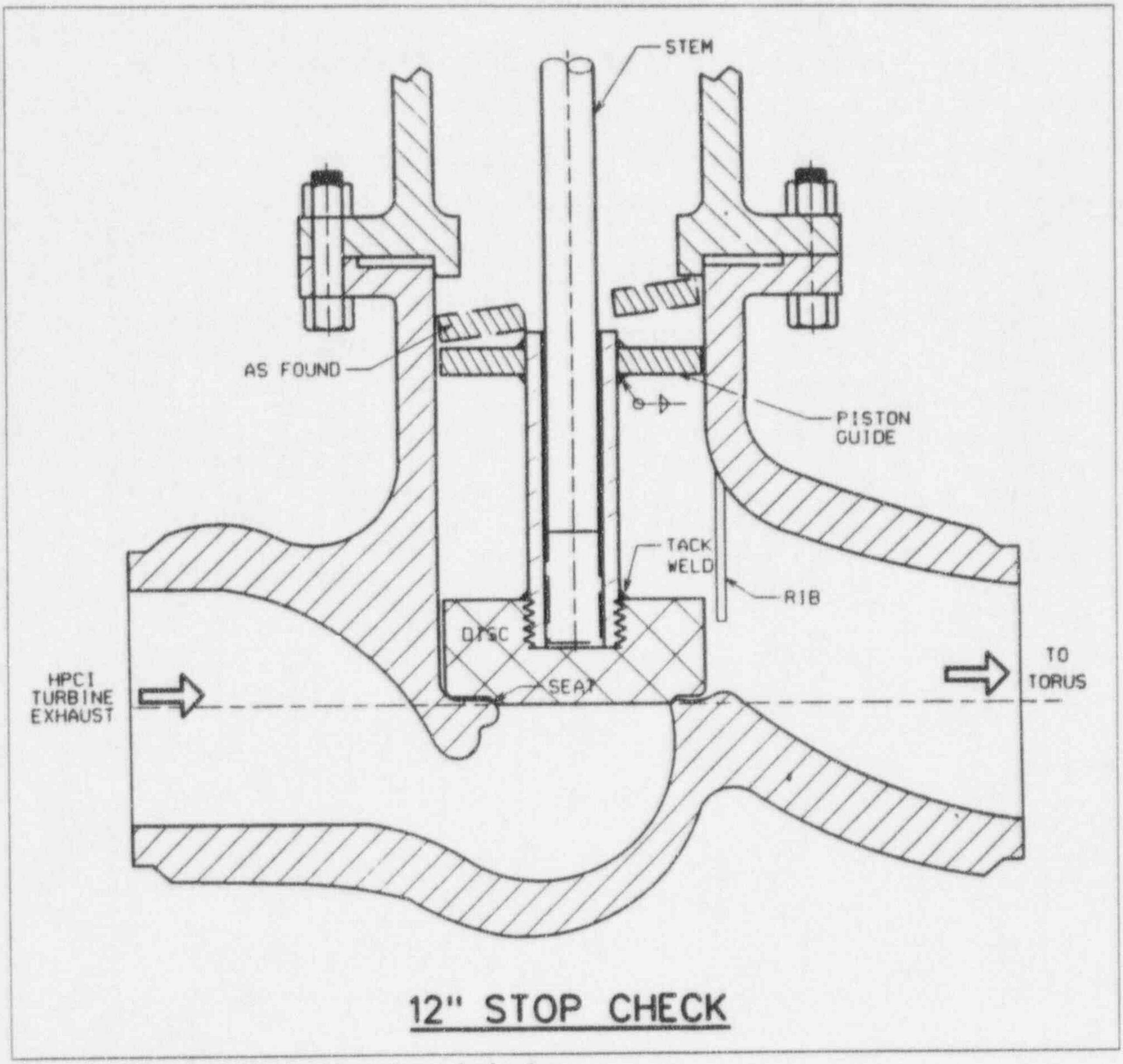


Figure C.4.1.Dresden 2 HPCI turbine exhaust check valve.

C.4.6 Reference

1. LER 237/94-021, "HPCI Turbine Tripped on High Exhaust Pressure Due to a Failed Exhaust Check Valve," September 2, 1994.

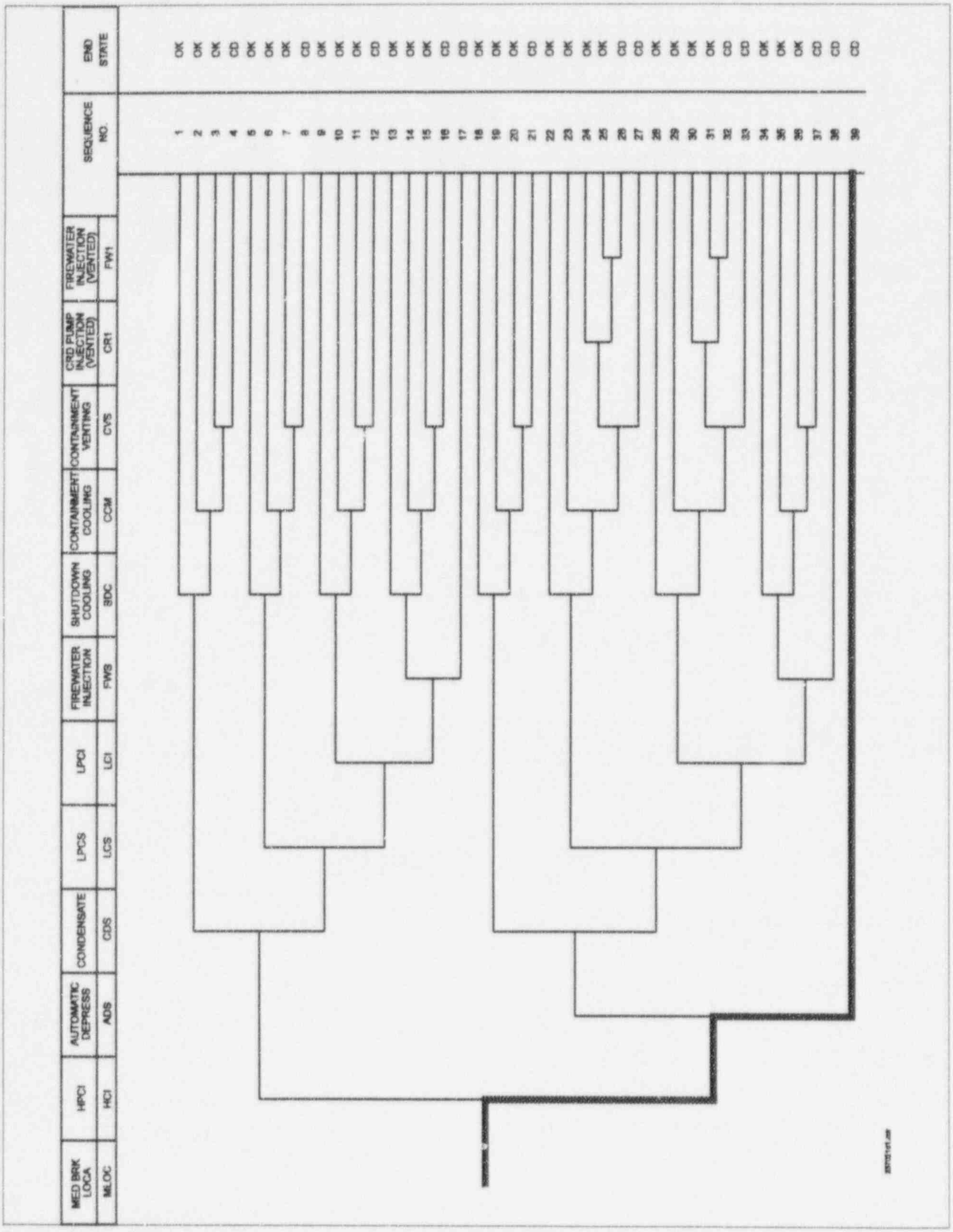


Figure C.4.2. Dominant core damage sequence for LER 237/94-021.

Table C.4.1. Definitions and probabilities for selected basic events for LER 237/94-021

Event name	Description	Base probability	Current probability	Type	Modified for this event
ADS-SRV-CC-VALVS	ADS Valves Fail to Open	3.7E-003	3.7E-003		N
ADS-XHE-XE-ERROR	Operator Error Prevents Depressurization	1.0E-002	1.0E-002*		N
ADS-XHE-XE-NOREC	Operator Fails to Recover ADS	7.1E-001	7.1E-001		N
CRD-MDP-FC-TRNA	Train A Failure	3.7E-003	3.7E-003		N
CRD-MDP-FC-TRNB	Train B Failure	3.7E-003	3.7E-003		N
CRD-XHE-XE-ERROR	Operator Fails to Align CRD	1.0E-002	1.0E-002		N
CRD-XHE-XE-NOREC	Operator Fails to Recover CRD	1.0E+000	1.0E+000		N
EPS-DGN-CF-DGNS	Common Cause Failure of Diesel Generators	1.4E-003	1.4E-003		N
EPS-DGN-FC-DG2	Unit 2 Generator Fails	7.8E-002	7.8E-002		N
EPS-DGN-FC-DG23	Swing Diesel Generator Fails	7.8E-002	7.8E-002		N
EPS-DGN-FC-DG3	Unit 3 Diesel Generator Failure	7.8E-002	7.8E-002		N
EPS-XHE-XE-NOREC	Operator Fails to Recover Emergency Power	8.0E-001	8.0E-001		N
HCI-TDP-FC-TRAIN	HPCI Train Level Failures	3.9E-002	1.0E+000	TRUE	Y
HCI-XHE-XE-NOREC	Operator Fails to Recover HPCI	7.1E-001	1.0E+000	TRUE	Y
IE-LOOP	Loss-of-Offsite Power Initiator	5.9E-006	4.9E-003		Y
IE-SLOCA	Small LOCA Initiator	1.7E-006	1.4E-003		Y
IE-TRAN	Transient Initiator	3.4E-004	2.8E-001		Y
IE-MLOCA	Medium-Break LOCA Initiator	1.3E-007	1.1E-004		Y
OEP-XHE-XE-NOREC	Operator Fails to Recover Offsite Power	6.6E-002	6.6E-002		N
PCS-SYS-VF-MISC	PCS Hardware Components Fail	1.7E-001	1.7E-001		N
PCS-XHE-XE-NOREC	Operator Fails to Recover PCS	1.0E+000	1.0E+000		N
PPR-SRV-OO-2VLVS	Two SRVs Fail to Close	1.3E-003	1.3E-003		N
PPR-SRV-OO-1VLV	One or Less SRVs Fail to Close	3.6E-002	3.6E-002		N

*0.01 used for MLOCA sequences, 0.001 used for other sequences.

Table C.4.2. Sequence conditional probabilities for LER 237/94-021

Event tree name	Sequence name	Conditional core damage probability (CCDP)	Core damage probability (CDP)	Importance (CCDP-CDP)	% Contribution
MLOCA	39	1.3E-006	1.5E-007	1.2E-006	43.0
TRAN	38-39	7.8E-007	8.9E-008	6.9E-007	25.3
LOOP	44	4.8E-007	4.8E-007	0.0E+000	15.6
LOOP	41	2.6E-007	2.9E-008	2.3E-007	8.2
Total (all sequences)		3.1E-006	8.3E-007	2.3E-006	

Table C.4.3. Sequence logic for dominant sequences for LER 237/94-021

Event tree name	Sequence name	Logic
IE-MLOCA	39	HCI, ADS
TRAN	38-39	/RPS, PCS, P2, HCI, ADS
LOOP	44	/RP1, EPS, OEP
LOOP	41	/RP1, EPS, /OEP, P1, HCI

Table C.4.4. System names for LER 237/94-021

System name	Description
ADS	Automatic Depressurization Fails
EPS	Emergency Power System Fails
HCI	HPCI Fails to Provide Sufficient Flow to Reactor Vessel
OEP	Offsite Power Recovery
P1	One or Less SRV Fail to Close
P2	Two SRVs Fail to Close
PCS	Power Conversion System
RP1	Reactor Shutdown Fails
RPS	Reactor Shutdown Fails

Table C.4.5. Conditional cut sets for higher probability sequences for LER 237/94-021

Cut set No.	% Contribution	Frequency	Cut sets
IE-MLOCA Sequence: 39		1.3E-006	
1	79.4	1.1E-006	ADS-XHE-XE-ERROR
2	20.8	2.8E-007	ADS-SRV-CC-VALVS, ADS-XHE-XE-NOREC
TRAN Sequence: 38-39		7.8E-007	
1	79.2	6.2E-007	ADS-XHE-XE-ERROR, PCS-SYS-VF-MISC, PCS-XHE-XE-NOREC, PPR-SRV-OO-2VLVS
2	20.8	1.7E-007	ADS-SRV-CC-VALVS, ADS-XHE-XE-NOREC, PCS-SYS-VF-MISC, PCS-XHE-XE-NOREC, PPR-SRV-OO-2VLVS
LOOP Sequence: 44		4.9E-007	
1	74.7	3.6E-007	EPS-DGN-CF-DGNS, EPS-XHE-XE-NOREC, OEP-XHE-XE-NOREC
2	25.3	1.2E-007	EPS-XHE-XE-NOREC, OEP-XHE-XE-NOREC, EPS-DGN-FC-DG23, EPS-DGN-FC-DG2, EPS-DGN-FC-DG3
LOOP Sequence: 41		2.7E-007	
1	74.7	2.0E-007	EPS-DGN-CF-DGNS, EPS-XHE-XE-NOREC, PPR-SRV-OO-1VLV
2	25.3	6.7E-008	EPS-XHE-XE-NOREC, PPR-SRV-OO-1VLV, EPS-DGN-FC-DG23, EPS-DGN-FC-DG2, EPS-DGN-FC-DG3
Total (all sequences)		3.1E-006	

C.5 LER No. 250/94-005

Event Description: Load Sequencers Periodically Inoperable

Date of Event: November 3, 1994

Plant: Turkey Point 3 and 4

C.5.1 Summary

During a Unit 4 Integrated Safeguards Test, the 3A sequencer failed to respond to the opposite unit's safety actuation signal. Troubleshooting resulted in the discovery of an error in the sequencer software logic that could prevent each of the four Turkey Point sequencers from responding to a safety actuation signal. As a result of the software error, each sequencer was unavailable one-fourth of the time to respond to automatic safety actuation signals from its own train and one-sixteenth of the time to respond to automatic signals from the other unit during both automatic self-testing and manual testing. Unavailability of each sequencer would prevent the automatic actuation of safety-related equipment associated with that train including the high head safety injection (HHSI) and residual heat removal (RHR) pumps.

The estimated increase in core damage probability for this event for a 1-year period is 1.8×10^{-6}, over a nominal value for the same period of 9.5×10^{-5}. This value is applicable to each unit.

C.5.2 Event Description

On November 3, 1994, Turkey Point Unit 3 was operating at 100% power, and Unit 4 was in Mode 5 during a refueling outage. During the Unit 4 Integrated Safeguards Test, the 3A sequencer failed to respond to the opposite unit's safety actuation signal. Troubleshooting resulted in the discovery of an error in the sequencer software logic that could prevent each sequencer from responding to a safety actuation signal. The error impacted the Turkey Point 3 s :quencers since November 1992 and the Turkey Point 4 sequencers since May 1993.

The Turkey Point design utilizes four sequencers, one for each train at each unit. The sequencers are programmable logic controller (PLC)-based cabinets that use a PLC for bus stripping and logic control. The sequencers are designed to respond to losses of offsite power (LOOPs), loss-of-coolant accidents (LOCAs), and combined LOOP/LOCA events. The sequencers start the diesel generators and sequentially load safety-related equipment required to respond to the initiating event. Each sequencer responds to safety actuation signals associated with its train plus signals from the opposite unit.

Each sequencer is provided with manual and automatic self-test capabilities. The automatic test mode is normally in operation. In the automatic test mode, the sequencer continually tests the input cards, output cards, and output relay coils and exercises the program logic. The automatic self-test cycles through 15 of 16 possible sequencer test steps. The test steps start roughly an hour apart and individually take about 10 s to complete. There is 1 h during which no testing takes place. The complete automatic test cycle, therefore, takes about 16 h and then begins again. The sequencer is designed to abort the manual and automatic test modes in response to a valid input. If a valid input signal is received during sequencer testing, the testing stops, the test signal clears, and the inhibit signal, if present, is supposed to clear. The valid signal is then allowed to sequentially energize the output relays for the associated safety-related equipment.

The 3A sequencer had dropped out of the automatic self-test without alarming, indicating that it had received a valid input signal. During troubleshooting, the input light emitting diode (LED) for the 4A safety actuation signal was found to be lit, indicating the signal was still present. The 3A sequencer response should have been to start the 3A HHSI pump. However, the pump failed to start because it did not receive a start signal from the sequencer.

A software design error was discovered that inhibited the 3A HHSI pump start signal even though a valid input signal was present. The design error was found to affect all sequencers during both manual and automatic testing in 5 of the 16 test steps. If a valid input signal was received 15 s or later into one of the hour-long test step periods, the test signal cleared as intended, but the inhibit signal was maintained by means of latching logic. This latching logic is established by the test signal but could be maintained by the process input signal if it arrived prior to removal of the test signal.

This software logic error was introduced during the detailed logic design phase of the software development. The error was not discovered during the validation and verification (V&V) process because the response to valid inputs was not tested during all test sequences of the testing logic. In four loading sequence tests, the error prevented the sequencer from responding to a valid safety actuation signal on the same train. In one other loading sequence test, the error prevented the sequencer from responding to a valid safety actuation signal on the opposite unit. This software error did not impact response to LOOP or a combined LOOP and LOCA; only safety actuation with offsite power available was affected. The logic error also did not affect sequencer operation with the test selector switch in the "off" position.

A detailed review of the sequencer software resulted in the discovery of one other error in the software, which was independent of the test mode. A condition was identified that would have prevented the automatic start of the containment spray pumps. The condition would occur when a hi–hi containment pressure signal is received by the sequencer during a 60-ms time window beginning 12.886 s after receipt of a LOCA signal or 28.886 s after receipt of a LOOP/LOCA signal. This error does not impact core damage sequences and was not addressed in this analysis.

C.5.3 Additional Event-Related Information

For non-LOOP events, each sequencer sends start signals to the following equipment associated with its train: one RHR pump, one HHSI pump, two intake cooling water pumps, two emergency containment cooler fans, two component cooling water pumps, and two emergency containment filter fans. Some equipment may already be in operation and would not be affected by a sequencer failure.

Turkey Point has four HHSI pumps, one per train for each unit. All four trains are normally cross-connected at the discharge of the pumps. Each HHSI pump is capable of providing 50% of the required injection; two of the four pumps are, therefore, required for high-pressure injection success following a small-break LOCA. To meet single failure criteria for a safety actuation, each sequencer signals its associated HHSI pump to start, and the opposite unit's sequencers signal their associated HHSI pumps to start. For example, a safety actuation signal on Unit 3, Train A, signals the 3A sequencer and both of the Unit 4 sequencers. With no equipment failures, all four HHSI pumps will respond to a safety actuation signal on either unit. Other equipment provided for each unit, including the two RHR pumps, is only started by its associated sequencer.

C.5.4 Modeling Assumptions

This event was modeled as an unavailability of HHSI and RHR pump automatic actuation for LOCA-related sequences during a 1-year period. Assuming the units were at power 70% of the time, an unavailability of 6132 h is estimated.

The Accident Sequence Precursor (ASP) Program typically considers the potential for core damage following three postulated offsite-power-available pressurized water reactor (PWR) initiating events: transient, small-break LOCAs, and steam generator tube rupture (SGTR). For each of these initiating events, unavailability of high-pressure injection, when required to make up inventory lost from the reactor coolant system, is assumed to result in core damage. Two additional initiating events also exist that are impacted by the unavailability of the HHSI and RHR pumps: medium- and large-break LOCAs. For both of these initiating events, unavailability of low-pressure injection is assumed to result in core damage.

The significance of an unavailability such as this event is estimated in the ASP Program in terms of the increase in core damage probability during the unavailability period. Since a nonrecoverable failure of multiple sequencers will fail high- and low-pressure injection, and, since unavailability of high- and low-pressure injection following a LOCA proceeds to core damage, the significance of this event can be estimated directly from the change in high- and low-pressure injection failure probabilities due to the sequencer software error and the probability of a small-, medium-, and large-break LOCA in the 6132-hour unavailability period.

Small-break LOCA. Small-break LOCA initiating events, SGTRs, and transient-induced LOCAs (primarily stuck-open relief valves for non-LOOP transients) were considered small-break LOCAs in this analysis. The frequencies of these three events, based on data used in the ASP models, are 1.4×10^{-8}/h (transient induced LOCA), 4.7×10^{-7}/h [small-break LOCA initiating events (spurious relief valve lifts, reactor coolant pump seal failures)], and 1.6×10^{-6}/h (SGTRs). Summing these values results in an overall small-break LOCA frequency of 2.1×10^{-6}/h. For the 6132-hour unavailability period, the probability of a small-break LOCA is 1.3×10^{-2}.

For a small-break LOCA, two of four HHSI pumps provide injection success; failure of three of the four pumps will, therefore, fail high-pressure injection. Since the software error did not affect sequencer response to LOOPs, only single-unit initiating events are of concern in the analysis (if LOOP response was affected, then potential dual-unit events such as a severe weather-related LOOP would also have to be considered). Assume the small-break LOCA occurs at Unit 3. The probability of the sequencers failing to actuate the four HHSI pumps is 0.25 for HHSI pumps 3A and 3B (the sequencers would not respond to a valid signal on the same train during 4 of the 16 loading sequence tests) and 0.0625 for HHSI pumps 4A and 4B (the sequencers would not respond to a valid signal from the opposite unit during one of the 16 loading sequence tests). The probability of three of the four pumps failing is estimated by considering the pump failure combinations that can result in injection failure:

$$p(3A) \times p(3B) \times p(4A) + p(3A) \times p(3B) \times p(4B) +$$

$$p(3A) \times p(4A) \times p(4B) + p(3B) \times p(4A) \times p(4B) = 9.8 \times 10^{-3}\ .$$

Consideration of the sequencer testing process indicates that an assumption that the sequencers fail independently is reasonable. If the testing of the two seauencers on each unit is synchronized, the increased HHSI failure probability is

$$0.25 \times 1.0 \times 0.0625 + 0.25 \times 1.0 \times 0.0625 + 0.25 \times 0.0625 \times 1.0 + 0.25 \times 0.0625 \times 1.0 = 6.3 \times 10^{-2}\ ,$$

using the same approach as in the last paragraph. If the testing of the four sequencers were somehow synchronized, the increased HHSI failure probability would be zero, since the test step that prevents response from the opposite unit is different from the steps that prevent response on the same train. The potential impact of synchronized testing of both sequencers on an individual unit was addressed as a sensitivity analysis.

For a small-break LOCA, manual initiation of safety injection (SI) within 30 min of the LOCA is assumed to result in injection success. Assuming 5 min to reach the procedure step to verify SI, 25 min would be available for operator action. The probability of failure to recover SI due to operator error was estimated by assuming that the failure probability can be represented as a time-reliability correlation (TRC) as described in *Human Reliability Analysis* (E. M. Dougherty and J. R. Fragola, John Wiley and Sons, New York, 1988). Operator response was assumed to be rule-based and without hesitancy. For the 25-min period, a failure probability of 1.8×10^{-4} is estimated.

The increase in core damage probability for small-break LOCAs resulting from the sequencer software error is, therefore,

1.3×10^{-2}(probability of a small-break LOCA in the 6132-h period) ×

9.8×10^{-3}(probability of HHSI actuation failure due to the software error) ×

1.8×10^{-4}(probability that the operators fail to manually initiate SI prior to core damage)

$= 2.2 \times 10^{-8}$.

Medium- and large-break LOCAs. The analysis of postulated medium- and large-break LOCAs follows the same approach as a small-break LOCA. The frequency of medium- and large-break LOCAs is estimated to be 1×10^{-3}/year and 2.7 × 10^{-4}/year, respectively (see *Analysis of Core Damage Frequency: Internal Events Methodology*, NUREG/CR-4550, Vol. 1, Rev. 1, Table 8.2-4 and Appendix H to this report). Mitigation of both medium- and large-break LOCAs requires low-pressure safety injection (LPSI) success. Two RHR pumps are available for injection, and one of two provides success. Since the two RHR pumps are actuated only by their same-train sequencers, an actuation failure probability of 0.25 × 0.25 = 0.0625 is estimated.

Assuming manual initiation of SI within 20 min of a medium-break LOCA provides injection success (this value is consistent with *Analysis of Core Damage Frequency: Surry, Unit 1, Internal Events*, NUREG/CR-4550, Vol. 3, Rev. 1, Part 1, Table 4.8-4), an operator failure probability of 2.2 × 10^{-3} is estimated, using the same apprcach as described for small-break LOCAs.

For a large-break LOCA an operator failure probability of 0.095 is estimated. This value was developed from simulator data provided in the licensee event report (LER) using the same TRC approach that was used to estimate operator failure probabilities for small- and medium-break LOCAs. The data provided in the LER were assumed to represent unburdened response; their standard deviation was revised to reflect burdened response as described on p. 127 of *Human Reliability Analysis*. The allowed response time was assumed to be 7.1 min, as specified in Appendix D.4 of NUREG/CR-4550, Vol. 3, Rev. 1. This is the time to core uncovery estimated using the MARCH code during source term calculations performed in 1984.

These estimates result in the following increase in core damage probability for medium- and large-break LOCAs:

1.0 × 10^{-3}(probability of a medium-break LOCA in a 1-year period (6132 at-power hours) ×

0.0625(probability of LPSI actuation failure due to the software error) ×

2.2 × 10^{-3}(probability that the operators fail to manually initiate LPSI)

= 1.4 × 10^{-7} (medium-break LOCA),

and

2.7 × 10^{-4} (probability of a large-break LOCA in a 1-year period (6132 at-power hours) ×

0.0625 (probability of LPSI actuation failure due to the software error) ×

0.095 (probability that the operators fail to manually initiate LPSI)

= 1.6 × 10^{-6} (large-break LOCA).

C.5.5 Analysis Results

Combining the probability estimates for small-, medium-, and large-break LOCAs results in an overall increase in core damage probability for the sequencer software error over a 1-year period of 1.8 × 10^{-6}, contributed almost entirely by postulated large-break LOCAs. This value is applicable to each unit. The dominant core damage sequence for the event involves a postulated large-break LOCA and failure of low-pressure injection. This sequence is highlighted in Figure C.5.1.

A greater than usual uncertainty is associated with this estimate. It is based on an estimated frequency of a large-break LOCA (no large-break or medium-break LOCAs have occurred), an estimated time to core uncovery developed in conjunction with source term calculations (there is large uncertainty in this estimated time), and assumptions regarding operator actions following a large-break LOCA.

The nominal core damage probability over a 1-year period estimated using the ASP models for Turkey Point is approximately 9.5×10^{-5}. The failed sequencers increased this probability by 2% to 9.7×10^{-5}. This value is the conditional core damage probability for the 1-year period in which the sequencers were degraded.

For most ASP analyses of conditions (equipment failures over a period of time during which postulated initiating events could have occurred), sequences and cutsets associated with the observed failures dominate the conditional core damage probability (the probability of core damage over the unavailability period, given the observed failures). The increase in core damage probability because of the failures is therefore essentially the same as the conditional core damage probability, and the conditional core damage probability can be considered a reasonable measure of the significance of the observed failures.

For this event, however, sequences unrelated to the degraded sequencers dominate the conditional core damage probability estimate. The increase in core damage probability given the degraded sequencers, 1.8×10^{-6}, is, therefore, a better measure of the significance of the sequencer problems.

If the sequencer testing was synchronized at each unit, the actuation failure probability for the HHSI pumps would increase to 6.3×10^{-2} as described in the modeling assumptions. The failure probability for low-pressure injection actuation would also increase to 0.25. These failure probabilities were used in a sensitivity analysis to estimate the potential impact if the testing were synchronized. The resulting estimated increase in core damage probability is 7.1×10^{-6}, again primarily from large-break LOCAs.

C.5.6 Reference

1. LER 250/94-005, Rev. 1, "Design Defect in Safeguards Bus Sequence Test Logic Places Both Units Outside the Design Basis," February 9, 1995.

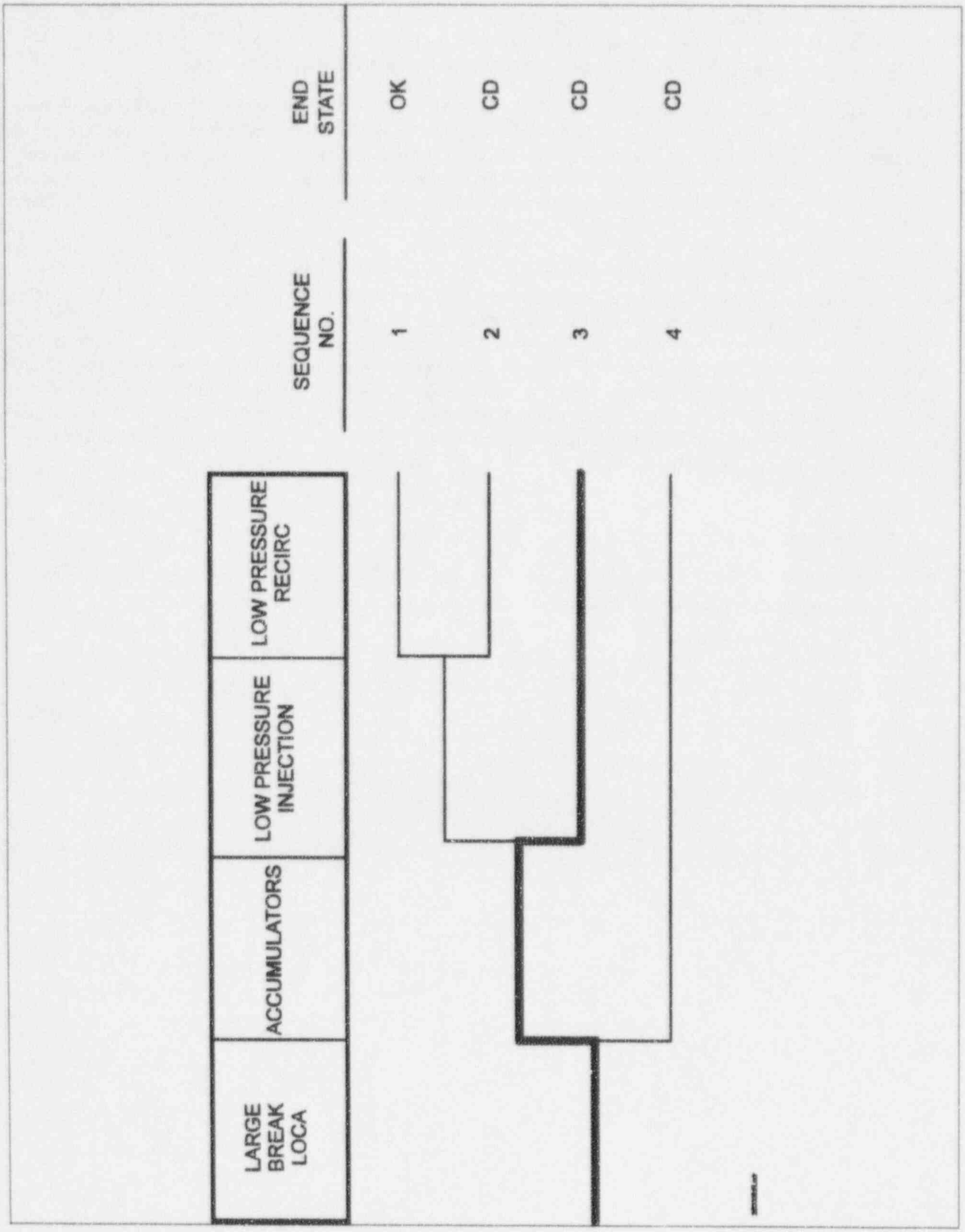


Figure C.5.1. Dominant core damage sequence for LER 250/94-005.

C.6 LER No. 266/94-002

Event Description: Both Diesel Generators Inoperable

Date of Event: February 8, 1994

Plant: Point Beach 1 and 2

C.6.1 Summary

Point Beach Units 1 and 2 were operating at 100% power when emergency diesel generator (EDG) G02 was taken out of service for maintenance. Plant technical specifications require that, if one EDG is removed from service, the other must be tested daily to verify its operability. When the EDG remaining in service was tested, electric fuel pump and exciter failures were experienced, and the EDG was declared inoperable. Both EDGs were, therefore, simultaneously unavailable. These unavailabilities would have impacted the Point Beach plant response to a loss-of-offsite power (LOOP) had it occurred during the unavailability period. The conditional core damage probability estimated for this event, 1.2×10^{-5}, is applicable to both units.

C.6.2 Event Description

EDG G02, the B train emergency power source for both units at Point Beach, was removed from service for maintenance at 0339 hours on February 7, 1994. At 0753 hours on February 8, 1994, an operability test of the A train emergency power source, EDG G01, was begun. At 0951 hours trouble annunciations were received for that EDG.

Investigation determined that the electric fuel pump for EDG G01 had failed. The EDG continued to run, however, with fuel supplied by a shaft-driven mechanical pump. The diesel was allowed to continue to run unloaded while repairs were made to the electric fuel pump. At 1940 hours repairs were complete, and the EDG was shut down.

At 2046 hours EDG G01 was started and loaded for a hard run to clean its exhaust system of deposits accumulated during the prior prolonged no-load run. At 2100 hours power swings were noted on the EDG varmeter. These swings increased in intensity, and at 2204 hours EDG G01 was declared inoperable.

A stationary brush jumper cable in the EDG's exciter was found to be contacting a rotating bus bar, shorting out the dc excitation voltage. This condition was repaired, and the EDG was declared operable at 0244 hours on February 9, 1994.

C.6.3 Additional Event-Related Information

The Licensee Event Report (LER) for this event indicates that the brush jumper cable was installed incorrectly during an annual maintenance outage on February 3, 1994. The report further indicates that EDG G01 was run for 3 h on February 4, 1.9 h on February 7, and 10.3 h on February 8 (while the electric fuel pump was repaired). The LER also indicates that a gas turbine generator was available as a backup source of emergency ac power.

C.6.4 Modeling Assumptions

This event was modeled as a 47-h simultaneous unavailability of both EDGs. As it was out of service for maintenance, EDG G02 was assumed to be unavailable after 0339 hours on February 7, 1994. EDG G01 experienced fuel pump and exciter failures that resulted in its being declared inoperable on February 8, 1994. After investigation, the exciter failure was attributed to maintenance errors that occurred on February 3, 1994. EDG G01 was operated on occasion between February 3 and February 8; however, the EDG ran unloaded for most of this time. After it was restarted to run under load on February 8, the EDG only operated for about 15 min before erratic exciter performance was observed. While it is possible that the EDG could have successfully run for an extended time in a loaded condition, this analysis assumes EDG G01 was unavailable to perform its safety function of supplying long-term emergency power until the exciter repair was completed on February 9, 1994. Due to the nature of the EDG unavailabilities, no EDG recovery was assumed to be possible. Because of the unavailability of both EDGs, the core damage sequences of primary concern in this analysis are those associated with a postulated LOOP and subsequent station blackout.

The probability of a LOOP in the 47-h period, the probability of its short-term and long-term recovery, and the probability of a reactor coolant pump (RCP) seal loss-of-coolant accident (LOCA) following a postulated station blackout were developed based on data contained in NUREG-1032, *Evaluation of Station Blackout Accidents at Nuclear Power Plants*, and RCP seal loss-of-coolant (LOCA) models developed as part of the NUREG-1150 probabilistic risk assessment (PRA) efforts, as described in *Revised LOOP Recovery and PWR Seal LOCA Models*, ORNL/NRC/LTR-89/11, August 1989.

The Final Safety Analysis Report (FSAR) indicates that a gas turbine generator is available at the Point Beach site that can be started and loaded within 10 min. This gas turbine generator is credited as a source of emergency ac power in the Point Beach Individual Plant Examination (IPE), and failure to recover ac power using the gas turbine is assigned a probability of 0.13 in the IPE. That value is employed in this analysis for the probability of failure to recover emergency ac power.

The IRRAS-based ASP model for Point Beach was modified to reflect the conditions observed during the event by setting the independent failure basic events associated with each EDG (EPS-DGN-FC-1A, B) to true, the EDG common-cause failure basic event (EPS-DGN-CF-ALL) to false, and the emergency power nonrecovery probability (EPS-XHE-NOREC) to 0.13. Basic events and their probabilities are shown in Table C.6.1. The incremental core damage probability over 47 h was then calculated by re-solving the accident sequence model.

The current ASP LOOP model for Point Beach assumes that the PORVs will be challenged, and that they will fail to reclose with a probability of 3×10^{-3} (IRRAS model default value) each. This assumption may be conservative, but it did not affect the dominant sequence for the event.

Calculations were performed for Point Beach Unit 1, the unit reported in the LER. Since EDG G01 and G02 also provide emergency power for Unit 2, the calculations are equally applicable to that unit.

The FSAR for Point Beach also indicates that the station batteries are designed to carry shutdown loads following a plant trip and loss of all ac power for a period of 1 h. Information provided by Point Beach indicates that the expected battery lifetime is 2 h. This analysis was performed based on the expected 2 h battery lifetime.

C.6.5 Analysis Results

The estimated conditional core damage probability associated with this event at each unit is 1.2×10^{-5}. The dominant core-damage sequence, highlighted on the event tree in Figure C.6.1, involves a postulated loss-of-offsite power, unavailability of emergency power because of the unavailability of both EDGs, failure to recover emergency power through use of the gas turbine generator, RCP seal LOCA, and failure to recover ac power prior to core uncovery.

Definitions and probabilities for selected basic events are shown in Table C.6.1. The conditional probabilities associated with the highest probability sequences are shown in Table C.6.2. Table C.6.3 lists the sequence logic associated with the sequences listed in Table C.6.2. Table C.6.4 describes the system names associated with the dominant sequences. Cutsets associated with each sequence are shown in Table C.6.5.

C.6.6 Reference

1. LER 266/94-002, "Inoperability of Both Emergency Diesel Generators," March 9, 1994.

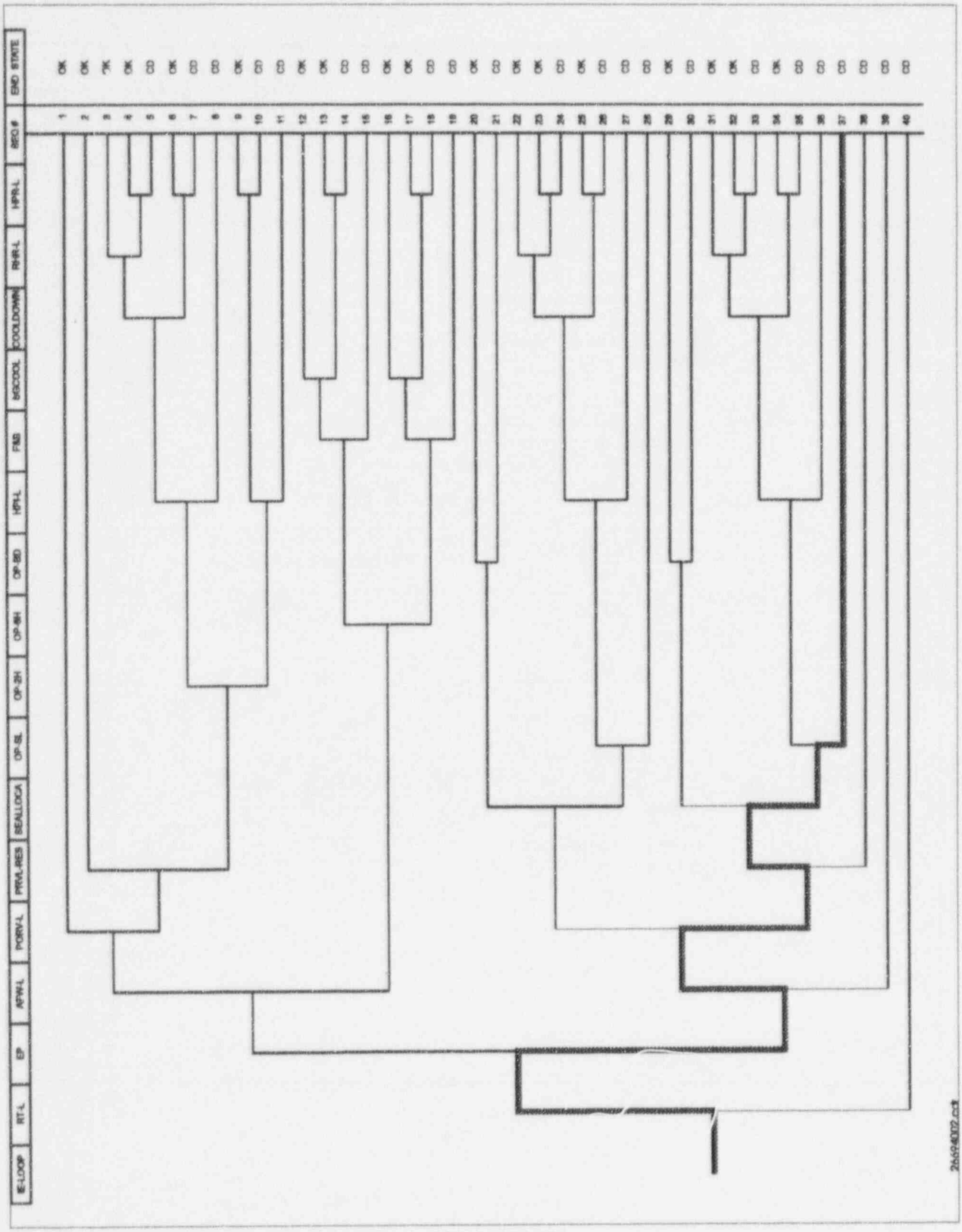


Figure C.6.1. Dominant core damage sequence for LER 266/94-002.

Table C.6.1. Definitions and probabilities for selected basic events for LER 266/94-002

Event name	Description	Base probability	Current probability	Type	Modified for this event
AFW-TDP-FC-1A	AFW Turbine Driven Pump Fails	3.3E-002	3.3E-002		N
AFW-XHE-NOREC-EP	Operator Fails to Recover AFW During Station Blackout	3.4E-001	3.4E-001		N
AFW-XHE-XA-PSWEP	Operator Fails to Align Backup Water Source During SBO	4.0E-002	4.0E-002		N
EPS-DGN-CF-ALL	Common Cause Failure of two diesel generators	1.1E-003	0.0E+000	FALSE	Y
EPS-DGN-FC-1A	Diesel Generator A Fails	4.2E-002	1.0E+000	TRUE	Y
EPS-DGN-FC-1B	Diesel Generator B Fails	4.2E-002	1.0E+000	TRUE	Y
EPS-XHE-NOREC	Operator Fails to Recover Emergency Power	8.0E-001	1.3E-001		Y
IE-LOOP	Loss-of-Offsite Power Initiating Event	5.8E-006	2.7E-004		Y
IE-SGTR	Steam Generator Tube Rupture Initiating Event	0.0E+000	0.0E+000		Y
IE-SLOCA	Small LOCA Initiating Event	0.0E+000	0.0E+000		Y
IE-TRANS	Transient Initiating Event	0.0E+000	0.0E+000		Y
OEP-XHE-NOREC-BD	Operator Fails to Recover Offsite Power Before Battery Depletion	8.3E-002	8.3E-002		N
OEP-XHE-NOREC-SL	Operator Fails to Recover Offsite Power (Seal LOCA)	6.5E-001	6.5E-001		N
PPR-SRV-OO-PRV1	PORV 1 Fails to Reclose After Opening	3.0E-002	3.0E-002		N
PPR-SRV-OO-PRV2	PORV 2 Fails to Reclose After Opening	3.0E-002	3.0E-002		N
RCS-MDP-LK-SEALS	RCP Seals Fail Without Cooling and Injection	2.6E-001	2.6E-001		N

Table C.6.2. Sequence conditional probabilities for LER 266/94-002

Event tree name	Sequence name	Conditional core damage probability (CCDP)	Core damage probability (CDP)	Importance (CCDP-CDP)	%Contribution
LOOP	37	5.9E-006	3.9E-007	5.5E-006	49.4
LOOP	30	2.9E-006	1.6E-008	2.9E-006	25.8
LOOP	38	2.1E-006	5.5E-008	2.0E-006	18.2
LOOP	39	8.7E-007	5.9E-008	8.1E-007	7.2
Total (all sequences)		1.2E-005			

Table C.6.3. Sequence logic for LER 266/94-002

Event tree name	Sequence name	Logic
LOOP	37	/RT-L, EP, /AFW-L-EP, PORV-L, /PORV-EP, SEALLOCA, OP-SL
LOOP	30	/RT-L, EP, /AFW-L-EP, PORV-L, /PORV-EP, /SEALLOCA, OP-BD
LOOP	38	/RT-L, EP, /AFW-L-EP, PORV-L, PORV-EP
LOOP	39	/RT-L, EP, AFW-L-EP

Table C.6.4. System names for LER 266/94-002

System name	Description
AFW-L-EP	No or Insufficient AFW Flow During Station Blackout
EP	Failure of Both Trains of Emergency Power
OP-BD	Operator Fails to Recover Offsite Power Before Battery Depletion
OP-SL	Operator Fails to Recover Offsite Power (Seal LOCA)
PORV-EP	PORVs Fail to Reclose (No Electric Power)
PORV-L	PORVs Open During LOOP
RT-L	Reactor Fails To Trip During LOOP
SEALLOCA	RCP Seals Fail During LOOP

Table C.6.5. Conditional cut sets for higher probability sequences for LER 266/94-002

Cut set No.	% Contribution	Conditional core damage probability (CCDP)	Cut sets
LOOP Seq: 37		5.9E-006	
1	100.0	5.9E-006	EPS-XHE-NOREC, OEP-XHE-NOREC-SL, RCS-MDP-LK-SEALS
LOOP Seq: 30		2.9E-006	
1	100.0	2.9E-006	EPS-XHE-NOREC, OEP-XHE-NOREC-BD
LOOP Seq: 38		2.1E-006	
1	50.1	1.0E-006	EPS-XHE-NOREC, PPR-SRV-OO-PRV1
2	50.1	1.0E-006	EPS-XHE-NOREC, PPR-SRV-OO-PRV2
LOOP Seq: 39		8.7E-007	
1	54.8	4.8E-007	AFW-XHE-NOREC-EP, EPS-XHE-NOREC, AFW-XHE-XA-PSWEP
2	45.2	3.9E-007	AFW-TDP-FC-1A, AFW-XHE-NOREC-EP, EPS-XHE-NOREC
Total (all sequences)		1.2E-005	

C.7 LER No. 304/94-002

Event Description: Unavailability of Turbine-Driven Auxiliary Feedwater Pump and Emergency Diesel Generator

Date of Event: March 7, 1994

Plant: Zion Unit 2

C.7.1 Summary

During a refueling outage, with Unit 2 in hot shutdown, operators were performing a surveillance test on the turbine-driven auxiliary feedwater (TDAFW) pump and an endurance test on the 2B emergency diesel generator (EDG). During the tests, the TDAFW pump tripped on "overspeed," and the EDG experienced frequency swings and was manually tripped. An operator also observed an increase in lube oil and jacket water cooler temperatures for the EDG before it was manually tripped. The cause of the TDAFW pump trip could not be determined. The EDG frequency swings were caused by a blown fuse, and the elevated lube oil and jacket water cooler temperatures were caused by zebra mussel shells in the lube oil and jacket water coolers for EDG 2B. The conditional core damage probability estimated for this event is 2.3×10^{-5}.

C.7.2 Event Description

Zion Unit 2 was performing several tests required to conclude a refueling outage. During a surveillance test on the TDAFW pump, the pump tripped at 0533 hours on March 7, 1994. The cause of the TDAFW pump trip could not be determined. An endurance test of the 2B EDG was also being performed. During the endurance test, the EDG experienced frequency swings, and lube oil and jacket water cooler temperatures increased. The EDG was manually tripped at 0618 hours on March 7, 1994. It was later determined that the frequency swings were caused by a blown fuse, and the increased coolant temperatures were caused by zebra-mussel shells in the lube oil and jacket water coolers. The zebra mussels were from the fire protection header that was used to supply EDG cooling during a dual-unit service water outage.

The zebra-mussel shells were cleaned from EDG 2B, and the blown fuse was replaced. The coolers for the 0 EDG and the 2A EDG were inspected and few or no shells were found. The 1A and 1B EDGs were not inspected, but testing was performed to verify that the EDGs were operable.

C.7.3 Additional Event-Related Information

The auxiliary feedwater (AFW) system consists of two 200% capacity subsystems. One subsystem utilizes two 100% capacity motor-driven pumps that are powered from separate engineered safety features (ESF) buses. Each motor-driven pump supplies a header, which in turn supplies all four of the steam generators (SGs). The TDAFW pump supplies all four of the SGs. Steam to drive the TDAFW pump is supplied from either SG 2A or SG 2D.

There are three safety-related buses for each unit. There are three sources of power for each bus—a normal feed from the respective unit's transformers, a cross-tie to the opposite unit, and an emergency diesel generator. There are five diesel generators—two for Unit 1, two for Unit 2, and one common diesel that can serve one bus on both units. If a safety injection signal is present, the common diesel generator will align to the unit with the safety injection signal. If a safety injection signal is absent, the common diesel generator is capable of supplying power to the associated electrical bus of each unit simultaneously.

C.7.4 Modeling Assumptions

Although this event occurred during a refueling outage, it was modeled assuming it could have occurred with the plant at power. The fuse failure that rendered the EDG inoperable could have occurred at any time. The failure mechanism for the TDAFW pump could not be determined, but is was assumed that the failure could also have occurred at any time. The zebra mussel shells could have been introduced during a short outage, and the plant could have been returned to a power condition prior to performing an endurance run of the EDG. Therefore, this event was modeled as *if* it occurred during power operation.

It was assumed that the EDG 2B was inoperable for one-half of its 30-day surveillance period. It was assumed that the EDG surveillance tests performed every 30 days would have run the EDG long enough to detect the degraded cooling condition. It was also assumed that the TDAFW pump would have tripped on "overspeed" during this period. The equipment powered by the 2B EDG would be unavailable during a LOOP event prior to restoration of offsite power.

This event was modeled as an unavailability of the 2B EDG and the TDAFW pump for a period of 15 days (360 h). The TDAFW pump failure to start and run probability (AFW-TDP-FC-1C) was set to 1.0 (TRUE) to reflect its condition, and the operator nonrecovery probability was set to 0.04 because recovery was considered to be proceduralized and could have been performed from the control room. Note, this value is the default value and is nearly identical to the probability used for the failure of auxiliary feedwater. The 2B EDG failure probability (EPS-DGN-FC-1B) was set to 1.0 (TRUE). The emergency power system was treated as a three-train system because of the common diesel. Common-cause failure probabilities are estimated using the MGL model. In this model, the nominal common-cause basic event for a three-train system is $Q \times \beta \times \gamma$. If one train suffers a random failure and the other trains are exposed to this failure mechanism, then the common-cause basic event becomes $\beta \times \gamma$. Therefore, the common-cause failure probability becomes 2.7×10^{-2} (0.1×0.27). The initiating event frequency for all initiators was calculated for a 360-h period.

C.7.5 Analysis Results

The conditional core damage probability estimated for this event is 2.3×10^{-5}. The dominant sequence highlighted on the event tree in Figure C.7.1 involves a postulated LOOP, a successful reactor trip, failure of emergency power, a PORV lift and successful reseat, recovery of AFW, and failure to recover offsite power prior to core uncovery following a reactor coolant pump seal LOCA. If the zebra mussels were judged not to be a common cause failure, then the CCDP would be 7×10^{-6}.

Definitions and probabilities for selected basic events are shown in Table C.7.1. The conditional probabilities associated with the highest probability sequences are shown in Table C.7.2. Table C.7.3 lists the sequence logic associated with the sequences listed in Table C.7.2. Table C.7.4 describes the system names associated with the dominant sequences. Cutsets associated with each sequence are shown in Table C.7.5.

C.7.6 Reference

1. LER 304/94-002, Revision 1, "Exceeded Limiting Condition for Operation 3.7.2 Action e for Placing Unit in Mode 4 with a Turbine-Driven and Motor-Driven AFW Pump Inoperable," July 25, 1994.

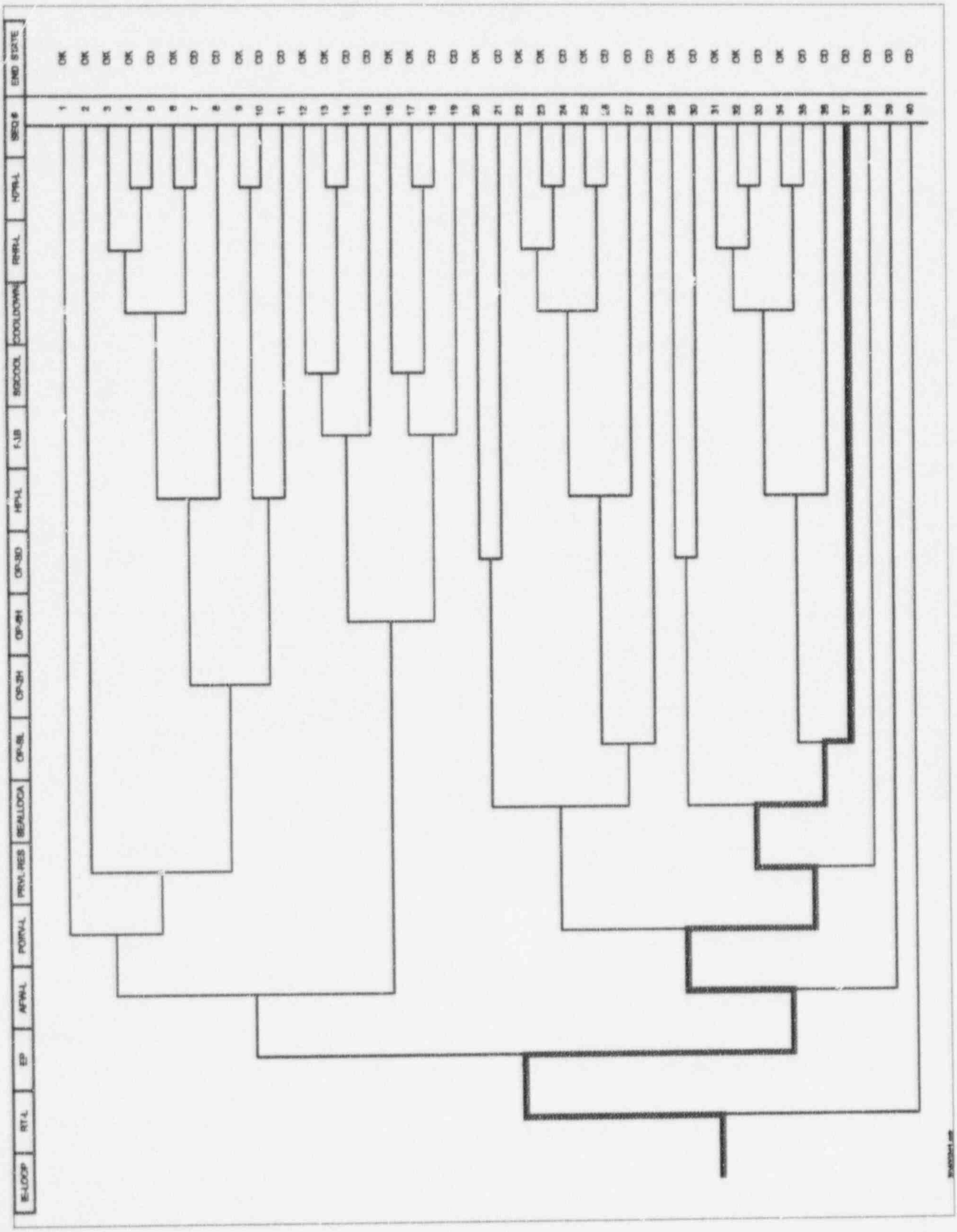


Figure C.7.1. Dominant core damage sequence for LER 304/94-002.

Table C.7.1. Definitions and probabilities for selected basic events for LER 304/94-002

Event name	Description	Base probability	Current probability	Type	Modified for this event
AFW-TDP-FC-1C	AFW Turbine Driven Pump Fails	3.9E-002	1.0E+000	TRUE	Y
AFW-XHE-NOREC-EP	Operator Fails to Recover AFW During Station Blackout	3.4E-001	4.0E-002		Y
AFW-XHE-NOREC-L	Operator Fails to Recover AFW System During LOOP	2.6E-001	4.0E-002		Y
EPS-DGN-CF-ALL	Common Cause Failure of Diesel Generators	1.0E-003	3.7E-003		Y
EPS-DGN-FC-10	Diesel Generator 0 Fails	3.7E-002	3.7E-002		N
EPS-DGN-FC-1A	Diesel Generator 1A Fails	3.7E-002	3.7E-002		N
EPS-DGN-FC-1B	Diesel Generator 1B Fails	3.8E-002	1.0E+000	TRUE	Y
EPS-XHE-NOREC	Operator Fails to Recover Emergency Power	8.0E-001	8.0E-001		N
HPI-MOV-OO-RWST	HPI RWST Isolation MOV Fails	3.0E-003	3.0E-003		N
HPR-MOV-CC-RHRB	RHR Train B Discharge MOV Fails	3.0E-003	3.0E-003		N
HPR-MOV-CC-SMPB	Failure of Sump MOV SI-8811B	3.0E-003	3.0E-003		N
HPR-XHE-NOREC-L	Operator Fails to Recover HPR System During LOOP	1.0E+000	1.0E+000		N
IE-LOOP	Loss-of-Offsite Power Initiating Event	8.6E-006	3.1E-003		Y
IE-SGTR	Steam Generator Tube Rupture Initiating Event	1.6E-006	5.9E-004		Y
IE-SLOCA	Small Loss of Coolant Accident Initiating Event	1.0E-006	3.6E-004		Y
IE-TRANS	Transient Initiating Event	5.3E-004	1.7E-001		Y
OEP-XHE-NOREC-BD	Operator Fails to recover offsite power before battery depletion	3.1E-002	3.1E-002		N
OEP-XHE-NOREC-SL	Operator Fails to Recover Offsite Power (Seal LOCA)	5.7E-001	5.7E-001		N
PPR-SRV-OO-1	PORV 1 Fails to Reclose After Opening	3.0E-002	3.0E-002		N
PPR-SRV-OO-2	PORV 2 Fails to Reclose After Opening	3.0E-002	3.0E-002		N
RCS-MDP-LK-SEALS	RCP Seals Fail Without Cooling and Injection	2.7E-001	2.7E-001		N
RHR-MDP-FC-1B	RHR Train B Fails	4.0E-003	4.0E-003		N
RHR-MOV-CF-RWST	Common Cause Failure of RHR/RWST MOVs	2.6E-004	2.6E-004		N

Table C.7.1. Definitions and probabilities for selected basic events for LER 304/94-002 (cont.)

Event name	Description	Base probability	Current probability	Type	Modified for this event
RHR-MOV-OO-RWSTA	RHR/RWST Isolation MOV 8812A Fails to Close	3.0E-003	3.0E-003		N
RHR-MOV-OO-RWSTB	RHR/RWST Isolation MOV 8812B Fails to Close	3.0E-003	3.0E-003		N
RHR-XHE-NOREC	Operator Fails to Recover the RHR System	1.0E+000	1.0E+000		N
RHR-XHE-NOREC-L	Operator Fails to Recover the RHR System During LOOP	1.0E+000	1.0E+000		N

Table C.7.2. Sequence conditional probabilities for LER 304/94-002

Event tree name	Sequence name	Conditional core damage probability (CCDP)	Core damage probability (CDP)	Importance (CCDP-CDP)	% Contribution
LOOP	37	1.0E-005	1.2E-006	9.6E-006	46.2
LOOP	38	4.2E-006	1.7E-007	4.0E-006	18.0
LOOP	39	2.8E-006	1.8E-007	2.6E-006	12.0
LOOP	30	2.1E-006	5.1E-008	2.1E-006	9.3
LOOP	05	1.7E-006	1.7E-007	1.5E-006	7.4
Total (all sequences)		2.3E-005	2.4E-006	2.1E-005	

Table C.7.3. Sequence logic for LER 304/94-002

Event tree name	Sequence name	Logic
LOOP	37	/RT-L, EP, /AFW-L-EP, PORV-L, /PORV-EP, SEALLOCA, OP-SL
LOOP	38	/RT-L, EP, /AFW-L-EP, PORV-L, PORV-EP
LOOP	39	/RT-L, EP, AFW-L-EP
LOOP	30	/RT-L, EP, /AFW-L-EP, PORV-L, /PORV-EP, /SEALLOCA, OP-BD
LOOP	05	/RT-L, /EP, /AFW-L, PORV-L, PRVL-RES, /OP-2H, /HPI-L, /COOLDOWN, RHR-L, HPR-L

Table C.7.4. System names for LER 304/94-002

System name	Description
AFW-L	No or Insufficient AFW Flow During LOOP
AFW-L-EP	No or Insufficient AFW Flow During Station Blackout
COOLDOWN	RCS CoolDown to RHR Pressure Using TBVs, etc.
EP	Failure of Both Trains of Emergency Power
HPI-L	No or Insufficient Flow From HPI System During LOOP
HPR-L	No or Insufficient HPR Flow During LOOP
OP-2H	Operator Fails to Recover Offsite Power Within 2 hrs
OP-BD	Operator Fails to Recover Offsite Power Before Battery Depletion
OP-SL	Operator Fails to Recover Offsite Power (Seal LOCA)
PORV-EP	PORVs Fail to Reclose (No Electric Power)
PORV-L	PORVs Open During LOOP
PRVL-RES	PORVs and Block Valves Fail to Reclose (EP Succeeds)
RHR-L	No or Insufficient Flow From RHR System During LOOP
RT-L	Reactor Fails to Trip During LOOP
SEALLOCA	RCP Seals Fail During LOOP

Table C.7.5. Conditional cut sets for higher probability sequences for LER 304/94-002

Cut set No.	% Contribution	Frequency	Cut sets
LOOP Seq: 37		1.1E-005	
1	94.9	1.0E-005	EPS-DGN-CF-ALL, EPS-XHE-NOREC,,OEP-XHE-NOREC-SL, RCS-MDP-LK-SEALS
2	5.0	5.4E-007	EPS-DGN-FC-1A, EPS-XHE-NOREC, OEP-XHE-NOREC-SL, RCS-MDP-LK-SEALS, EPS-DGN-FC-10
LOOP Seq: 38		4.2E-006	
1	47.4	2.0E-006	EPS-DGN-CF-ALL, EPS-XHE-NOREC, PPR-SRV-OO-2
2	47.4	2.0E-006	EPS-DGN-CF-ALL, EPS-XHE-NOREC, PPR-SRV-OO-1
LOOP Seq: 39		2.8E-006	
1	94.9	2.7E-006	AFW-XHE-NOREC-EP, EPS-DGN-CF-ALL, EPS-XHE-NOREC
2	5.0	1.4E-007	AFW-XHE-NOREC-EP, EPS-DGN-FC-1A, EPS-XHE-NOREC, EPS-DGN-FC-10
LOOP Seq: 30		2.2E-006	
1	94.9	2.1E-006	EPS-DGN-CF-ALL, EPS-XHE-NOREC, OEP-XHE-NOREC-BD
2	5.0	1.1E-007	EPS-DGN-FC-1A, EPS-XHE-NOREC, OEP-XHE-NOREC-BD, EPS-DGN-FC-10

Table C.7.5. Conditional cut sets for higher probability sequences for LER 304/94-002 (cont.)

Cut set No.	% Contribution	Frequency	Cut sets
LOOP Seq: 05		1.8E-006	
1	20.5	3.6E-007	/EPS-DGN-FC-1A, HPR-XHE-NOREC-L, PPR-SRV-OO-2, RHR-MDP-FC-1B, RHR-XHE-NOREC-L
2	15.3	2.7E-007	/EPS-DGN-FC-1A, HPR-XHE-NOREC-L, PPR-SRV-OO-2, RHR-XHE-NOREC-L, HPR-MOV-CC-RHRB
3	15.3	2.7E-007	/EPS-DGN-FC-1A, HPR-XHE-NOREC-L, PPR-SRV-OO-2, RHR-XHE-NOREC-L, RHR-MOV-OO-RWSTA
4	15.3	2.7E-007	/EPS-DGN-FC-1A, HPR-XHE-NOREC-L, PPR-SRV-OO-2, RHR-XHE-NOREC-L, HPI-MOV-OO-RWST
5	15.3	2.7E-007	/EPS-DGN-FC-1A, HPR-XHE-NOREC-L, PPR-SRV-OO-2, RHR-XHE-NOREC-L, HPR-MOV-CC-SMPB
Total (all sequences)		2.3E-005	

C.8 LER No. 318/94-001

Event Description: Trip, Loss of 13.8-kV Bus, and Short-Term Saltwater Cooling System Unavailable

Date of Event: January 12, 1994

Plant: Calvert Cliffs 2

C.8.1 Summary

Calvert Cliffs Units 1 and 2 were both operating at 100% power with emergency diesel generator (EDG) 11 and saltwater (SW) loop 11 for Unit 1 removed from service for scheduled maintenance. A modification to install three 13.8-kV voltage regulators on each unit was also in progress. The new voltage regulator protective trip circuits to the 13.8-kV supply feeder breakers, which had been connected earlier in the modification sequence, were believed by the plant staff tc be functionally isolated from existing plant equipment.

Howeve, the protective trip circuits were not completely isolated, and a ground on Unit 2 dc bus 21 resulted in the spurious tripping of three 13.8-kV breakers for Unit 2 over a 27-min period. Unit 2 tripped and power was lost to 4-kV safeguards bus 14. Flow was consequently lost to the remaining Unit 1 SW loop, but this was recovered by the manual closure of an alternate feeder breaker that reenergized bus 14. The conditional core damage probability estimated for this event is 1.3×10^{-5}.

C.8.2 Event Description

Calvert Cliffs Units 1 and 2 were operating at 100% power on January 12, 1994. At 0405 hours, EDG 11 and SW loop 11 for Unit 1 were removed from service for scheduled maintenance.

Also at this time, a modification was in progress to install six 13.8-kV voltage regulators, three for each unit, between the unit service transformers (USTs) and their 13.8-kV supply feeder breakers (a simplified drawing of the electrical distribution system as it impacted this event is included as Figure C.8.1). On the morning of January 12, 1994, all six voltage regulators were mounted in place, but the 13.8-kV cables were not connected to existing plant equipment. Their annunciation circuits were tagged out with the fuses removed.

The voltage regulator protective trip circuits to the 13.8-kV supply feeder breakers had been connected earlier in the modification sequence. These protective circuits are designed to open the associated feeder breaker and deenergize the regulator and UST in the event of a sudden pressure increase from a fault inside a winding compartment. Utility staff believed these protective trip circuits were functionally isolated from existing plant equipment.

At 0552 hours, a sudden pressure trip relay actuated in voltage regulator 2H2103, tripping open the 13.8-kV feeder breaker (breaker 252-2103, see Figure C.8.1) to UST U-4000-22. The feeder breakers for buses 22, 23, and 24 also tripped open on undervoltage, and Unit 2 tripped. Auxiliary feedwater (AFW) flow was initiated, and EDG 21 started and loaded as designed. The 13.8-kV electrical components were inspected. There was no local indication of any breaker protective devices tripped, but the UST U-4000-22 feeder breaker's lockout device was tripped.

At 0617 hours (+25 min), the 13.8-kV feeder breaker (252-2102) to UST U-4000-21 tripped open, with a subsequent undervoltage trip of the Unit 1 4-kV bus 14 feeder breaker (152-1414). Flow was lost in Unit 1 No. 12 SW loop when the No. 12 SW pump stopped due to the loss of power to bus 14. Since the No. 11 SW loop had previously been removed from service for maintenance, SW cooling was unavailable to Unit 1. Swing EDG 12 started upon loss of power to bus 14. Unit 1 control room operators closed alternate feeder breaker 152-1401, which reenergized bus 14. No. 12 SW pump was restarted, and SW flow was restored in the No. 12 SW loop approximately 2 min after flow was lost.

At 0619 hours (+27 min), the 13.8-kV feeder breaker (252-2101) to UST U-4000-23 tripped open, resulting in a loss of power to Unit 2 buses 25 and 26. By 0628 hours (+36 min) the operators concluded that the spurious 13.8-kV breaker trips were isolated to 13.8-kV bus 21, and they deenergized the bus by opening feeder breaker 252-2104.

Approximately 2 min later, plant electricians determined that a ground existed on Unit 2 125-V dc bus 21. Subsequent troubleshooting isolated the dc ground to voltage regulator 2H2102 (the regulator for UST U-4000-21, which supplies power to 4-kV bus 14). The sudden pressure trip circuits for the breakers associated with the Unit 2 13.8-kV voltage regulators were disconnected. The three Unit 2 voltage regulator transfer switch assemblies were then tagged and locked in the bypass mode.

At 1535 hours, 9.75 h after Unit 2 tripped, 13.8-kV bus 21 was reenergized. At 1550 hours, the other Unit 2 4-kV buses were restored to a normal lineup. Unit 1 buses were restored to a normal electrical lineup, with the voltage regulators isolated and the trip circuits removed, at about 1845 hours.

The actuation of the sudden pressure trip circuits for the 13.8-kV voltage regulators was caused by intermittent grounds on their associated 125-V dc bus. Electrical bench testing after the event confirmed that the circuit would actuate in the presence of a dc ground in the condition the circuit was in at the time of the event. An actuation would not occur if the circuit was in its final (completely installed) designed configuration. The utility believed the ground was due to loose leads from a terminal block in the 2H2102 bypass transfer switch cabinet coming in contact with the inner cabinet door.

C.8.3 Additional Event-Related Information

UST power is provided from two 13.8-kV buses, bus 11 for Unit 1 and bus 21 for Unit 2 (a simplified drawing of the electrical distribution system is included as Figure C.8.1.). Each bus powers equipment associated with its own unit with the exception of one safety-related 4-kV bus, which is powered from the other unit. Unit 2 4-kV bus 21 is powered from Unit 1 13.8-kV bus 11, and Unit 1 4-kV bus 14 is powered from Unit 2 13.8-kV bus 21.

Three EDGs provide power to four safety-related buses. EDGs 11 and 21 can provide power to one bus in either unit. EDG 12 can provide power to any one of the safety-related buses.

The SW cooling system for each Calvert Cliffs unit is a three-pump, two-train system. The SW system provides cooling for the service water heat exchangers, the component cooling water (CCW) heat exchangers, and the emergency core cooling system coolers. SW pumps 11 and 12 supply SW headers 11 and 12, respectively. SW pump 13 can supply either header 11 or 12 and is normally aligned to header 12 and powered by bus 11.

The CCW heat exchangers provide cooling for the low-pressure safety injection (LPSI) and high-pressure safety injection (HPSI) pumps, the shutdown cooling heat exchangers, the reactor coolant pump (RCP) seal and lube oil coolers, and control element drive mechanism (CEDM) coolers. The service water heat exchangers provide cooling for the EDGs, the feed pump turbine and condensate pump lube oil coolers, and the instrument and plant air compressors.

Bus 14 supplies power to LPSI pump 12, HPSI pumps 12 and 13, containment spray pump 12, service water pumps 12 and 13, and SW pumps 12 and 13.

The AFW pumps at Calvert Cliffs are self-cooled and are not affected by the loss of the SW cooling system. The HPSI pumps require CCW for both the injection and recirculation phases following a loss-of-coolant accident (LOCA) or if required for feed and bleed.

Unlike many other RCP seals that utilize both seal injection and thermal barrier cooling, the RCP seals at Calvert Cliffs use only thermal barrier cooling. Unavailability of CCW for an extended period of time, resulting from the loss of SW cooling, may result in seal failure and a small-break LOCA.

C.8.4 Modeling Assumptions

The analysis considered three situations relevant to the event: (1) the trip and loss of power to the 13.8-kV buses at Unit 2, (2) the potential for an extended loss of SW cooling at Unit 1, and (3) the potential for a trip-induced loss-of-offsite power (LOOP) in conjunction with the loss of SW cooling and potential trip of Unit 1 following the Unit 2 trip.

Case 1: Trip and loss of power to 13.8-kV buses at Unit 2

The loss of power to the Unit 2 USTs resulted in an effective plant-centered LOOP to Unit 2 with the exception of 4-kV bus 21, which remained powered from Unit 1. The IRRAS-based ASP model for Calvert Cliffs was revised as follows to reflect the conditions observed during the event.

Because EDG 11 was out of service for maintenance and Unit 2 4-kV bus 21 remained powered from Unit 1, the LOOP-related fault trees were modified by deleting basic events associated with a loss of power to bus 21 and including both EDG 12 and EDG 21 as power sources for 4-kV bus 24. Failure of ac power to bus 24 components was modeled as (1) the common-cause failure of EDGs 12 and 21, (2) the independent failure of both EDGs, or (3) the failure of EDG 21 and alternate feeder breaker 152-1401 (if this breaker failed to close, EDG 12 would be needed to provide power to bus 14 in order to recover SW cooling to Unit 1):

EPS-DGN-CF-ALL + (EPS-DGN-FC-B × (EPS-DGN-FC-SWG + EPS-152-1401)).

Since one of the safety-related buses remained powered from Unit 1, a Unit 2 station blackout was assumed to be impossible. Failure of emergency power was made false by setting the emergency power nonrecovery basic event (EPS-XHE-NOREC) to false. This effectively eliminated station blackout sequences from consideration in the analysis of this case. Due to the length of time required to identify the cause of the breaker trips, the probability of failing to recover offsite power to Unit 2 4-kV buses 22-26 before 6 h (the longest recovery time considered in the ASP models) was assumed to be 1.0, and OEP-XHE-NOREC-2H, -6H were set to TRUE to reflect this. Similarly, short-term LOOP nonrecovery (in IE-LOOP) was revised to 1.0. The other LOOP recovery values (OPE-XHE-NOREC-BD and OPE-XHE-NOREC-SL) and the RCP seal LOCA due to failure of cooling (RCP-MDP-LK-SEALS) have no effect on the results since failure of emergency power is precluded in this case.

The common-cause failure probability for the EDGs (EPS-DGN-CF-ALL) was also revised from 1.1×10^{-3} to 4.2×10^{-3} to reflect the unavailability of EDG 11.

The basic event changes for this case are shown in Table C.8.1. The core damage probability associated with this case was calculated by solving the accident sequence model for the LOOP sequences using the modified fault trees and this change set.

Case 2: Potential loss of SW cooling at Unit 1

Since SW cooling loop 11 was out of service for scheduled maintenance, the loss of power to 4-kV bus 14 resulted in a total loss of SW cooling at Unit 1. If SW cooling 14 had not been quickly recovered, heat removal via the CCW and SW systems would have been lost. The resulting loss of cooling to the feed pump lube oil coolers, instrument air compressors, RCP lube oil coolers, and CEDMs was assumed to result in an automatic or manual scram and a loss of feedwater (LOFW).

The AFW pumps at Calvert Cliffs are self-cooled and were considered available without the SW cooling system. Because the high-pressure safety injection (HPSI) pumps require CCW for both the injection and recirculation phases following a LOCA or if required for feed and bleed, high-pressure injection (HPI) would have been unavailable until the SW cooling system was recovered. This analysis assumes the operators stop operating components prior to their being damaged by the loss of cooling.

The core damage model used to analyze this case considered the potential failure of the operators to recover SW cooling (a) prior to a reactor trip and LOFW resulting from the unavailability of cooling to the feedwater pump and RCP lube oil coolers, instrument air compressors, and CEDMs; and (b) prior to the need for HPI to mitigate a LOCA resulting from a potential stuck-open primary relief valve or RCP seal failure or for feed and bleed.

A conditioning event tree was used to characterize the plant status associated with success or failure in recovering SW cooling through restoration of power to 4-kV bus 14. This event tree is shown in Figure C.8.2. Six sequences involving failure to recover SW cooling prior to reactor trip are listed, along with the associated plant status, the conditioning sequence probability, the conditional core damage probability given the conditioning sequence, and the overall core damage probability for the sequence. The probabilities are for Unit 1 alone; the combined impact of the event at both units is developed later in this analysis. The following assumptions were made when developing this event tree.

Successful recovery of SW cooling within 10 min was assumed to prevent a reactor trip (although a plant shutdown may still be required). Failure to recover SW cooling at 40 min (one-half hour after the assumed trip) was assumed to render HPI inoperable if it were required to mitigate a stuck-open primary relief valve or if it were required for feed and bleed. The RCP seals were also assumed to be vulnerable to failure if SW cooling was not recovered within 40 min. Failure to recover SW cooling within 30 min of an RCP seal failure was also assumed to render HPI unavailable.

The event tree includes the following branches related to the recovery of 4-kV bus 14 and SW cooling:

Loss of SW cooling. The initiating event is a loss of SW cooling caused by the loss of power on 4-kV bus 14.

SW cooling not recovered (component failures). This branch represents nonrecoverable component failures that prevent recovery of SW cooling at Unit 1. SW cooling can be recovered by recovering power to bus 14. Bus 14 was assumed to be recoverable either through the use of alternate feeder breaker 152-1401 (this breaker was used during the event) or through the use of EDG 12. SW cooling can also be recovered by manually starting SW pump 13 and providing flow to SW header 12. Failure to recover SW cooling is assumed to result in core damage if an RCP seal LOCA occurs, since neither SW loop is available for heat removal. The probability for this branch can be approximated by

$$[p(\text{EPS-DGN-FC-SWG}) + p(\text{EPS-DGN-CF-ALL})] \times p(\text{EPS-152-1401}) \times p(\text{SW pump 13 fails to start and run})$$

$$[4.2 \times 10^{-2} + 1.1 \times 10^{-3}] \times 3.0 \times 10^{-3} \times 3.7 \times 10^{-3} = 4.8 \times 10^{-7}.$$

However, the cutsets must be preserved to ensure EDG 12 is not credited with powering loads on Unit 1 and Unit 2 at the same time.

SW cooling recovered prior to trip. The control room operators recover SW cooling within approximately 10 min. A reactor trip and LOFW resulting from loss of cooling to the feedwater pumps, RCPs, CEDMs, and instrument air compressors are prevented. The probability of failing to recover SW cooling due to operator error was estimated by assuming the failure probability can be represented as a time-reliability correlation (TRC) as described in *Human Reliability Analysis*, E. M. Dougherty and J. R. Fragola, John Wiley and Sons, New York, 1988. Because of the sequential nature of the failures and the lack of understanding of their cause, the "response (rule-based) with hesitancy" TRC, as described in Chap. 11, was utilized in the analysis. The probability distribution for this TRC is lognormal, with a median response time of 2 min and an error factor of 6.4. The probability of crew failure at 10 min, estimated using this TRC, is 0.073.

SW cooling recovered at 40 min. SW cooling is recovered within 40 min of its initial loss. HPI is available to mitigate a stuck-open relief valve and for feed and bleed cooling. Using the approach described above, the conditional probability of failing to recover SW cooling at 40 min, given it was not recovered at 10 min, is estimated to be 0.047. Recovery of SW cooling within 40 min is assumed to result in a LOFW with unavailability of the one train of the emergency core cooling system (ECCS) cooled by the SW loop out of service for maintenance.

RCP seal failure. Unavailability of RCP seal cooling may result in an RCP seal failure and a small-break LOCA. In this analysis, the probability of an RCP seal LOCA was assumed to be zero up to 60 min after the reactor trip (70 min after the loss of SW cooling). Beginning at 60 min after the trip, the probability of an RCP seal LOCA was assumed to increase linearly to 0.083 at 1.5 h after the trip, after which no additional seal failures were assumed to occur (see Appendix H for additional information concerning this seal failure model). This type of seal failure model is similar to that used in the ASP Program for modeling station blackout sequences (see ORNL/NRC/LTR-89/11, *Revised LOOP Recovery and PWR Seal LOCA Models*, August 1989).

For example, the probability of sequence 5, which involves an RCP seal failure and the failure to recover SW cooling following the seal failure is calculated as follows:

$$\text{p(seq 5)} = \text{p(opr fails to recover SW cooling at 40 min)} \times \int f_{SL}(t) \times p_{SW}(t + 0.5)dt\,,$$

where $f_{SL}(t)$ is the probability density function for an RCP seal LOCA and p_{SW} $(t + 0.5)$ is the probability of not recovering SW at t + 0.5 h. Since f_{SL} (t) is assumed to be nonzero only between 1.0 and 1.5 h following the trip, and $p_{SW} = \Phi\{[\ln(t + 0.5) - \ln(\text{median})]/\sigma\}$, the probability of the sequence is

$$0.073 \times 0.047 \times \int_{70}^{100} \frac{0.083}{30} \times \Phi\left[\frac{\ln(t + 30) - \ln(2)}{\ln(6.4)/1.645}\right] dt = 0.0033.$$

SW cooling recovered following a seal LOCA. Failure to recover SW cooling within one-half hour of an RCP seal LOCA is assumed to result in core damage, since HPI is unavailable for RCS makeup. Recovery of SW cooling within the half-hour is assumed to result in a LOCA with one train of ECCS unavailable.

Using a convolution approach similar to that in ORNL/NRC/LTR-89/11 allows estimation of the probabilities of conditioning event tree sequences involving potential RCP seal failures and SW cooling recovery.

Probabilities estimated for the combined events involving RCP seal failure and SW cooling following a seal LOCA are as follows:

p(RCP seal failure occurs and SW cooling recovered) = 0.0061;

p(RCP seal failure occurs and SW cooling not recovered) = 0.0033;

p(RCP seal failure does not occur) = 0.99.

The basic event changes associated with the plant status for each conditioning sequence included in Figure C.8.2 are shown in Tables C.8.2 through C.8.4. The core damage probability given each conditioning sequence was calculated by solving the accident sequence model for the relevant sequences using the appropriate change set. These conditional probabilities are included in Figure C.8.2, along with overall sequence probabilities.

Case 3: Potential trip-induced LOOP at Unit 1 following the Unit 2 trip

If SW cooling had not been quickly recovered at Unit 1 and the unit had tripped, then the potential would have existed for a LOOP to Unit 1 caused by the sudden separation of both Calvert Cliffs units from the grid. If this were to occur, EDG 12 would have been required to supply emergency power to Unit 1. Both units would have been required to respond to LOOPs with only one EDG per unit.

The probability of a trip-induced LOOP is 1.0×10^{-3} (*Reactor Safety Study*, WASH-1400, NUREG-75/014, p. I-90). Combining this value with the probability of trip given the loss of SW cooling, 0.1 from Case 2, results in a probability of LOOP given the loss of power to the Unit 2 13.8-kV buses of 1.0×10^{-4}. The postulated LOOP would be grid-related for Unit 1 and for Unit 2 (since bus 21 is recovered once offsite power is recovered to Unit 1). The basic event changes for this case are shown in Tables C.8.5 and C.8.6. In addition to the basic event changes, the electric power fault tree was revised to reflect the one EDG per unit that would be available. Combining the sequence conditional probabilities for LOOP calculated using the basic event changes with the probability of LOOP results in the LOOP sequence probabilities for this case.

The probability of long-term offsite power recovery was developed based on data contained in NUREG-1032, *Evaluation of Station Blackout Accidents at Nuclear Power Plants.*

C.8.5 Analysis Results

The conditional probability estimated for this event is 1.3 × 10^{-5}. The conditional probabilities for Cases 1, 2, and 3 are 1.3 × 10^{-6}, 1.1 × 10^{-5}, and 5.1 × 10^{-8}, respectively. Case 2 contributes 85% of the total conditional probability. The dominant sequence highlighted on the event tree in Figure C.8.2 is from Case 2 and involves a postulated loss of SW cooling on Unit 1, failure to recover SW cooling, and a subsequent RCP seal LOCA.

The results of this analysis are strongly dependent on assumptions concerning the probability of not recovering SW cooling and the probability of a subsequent RCP seal LOCA. Because of the uncertainties inherent in both probability estimates, the overall conditional probability estimate is also subject to considerable uncertainty. As an example of this impact, an assumption that the seal failure probability is a factor of ten lower than that used in the analysis results in a conditional probability estimate of 2.9 × 10^{-6}, a factor of 4.5 lower.

The conditional probabilities associated with the highest probability sequences are shown in Table C.8.7. Table C.8.8 describes the system names associated with the dominant sequences.

C.8.6 Reference

1. LER 318/94-001, Rev. 1, "Reactor Trip Due to Opening of 13.8 Kilovolt Feeder Breaker," March 16, 1994.

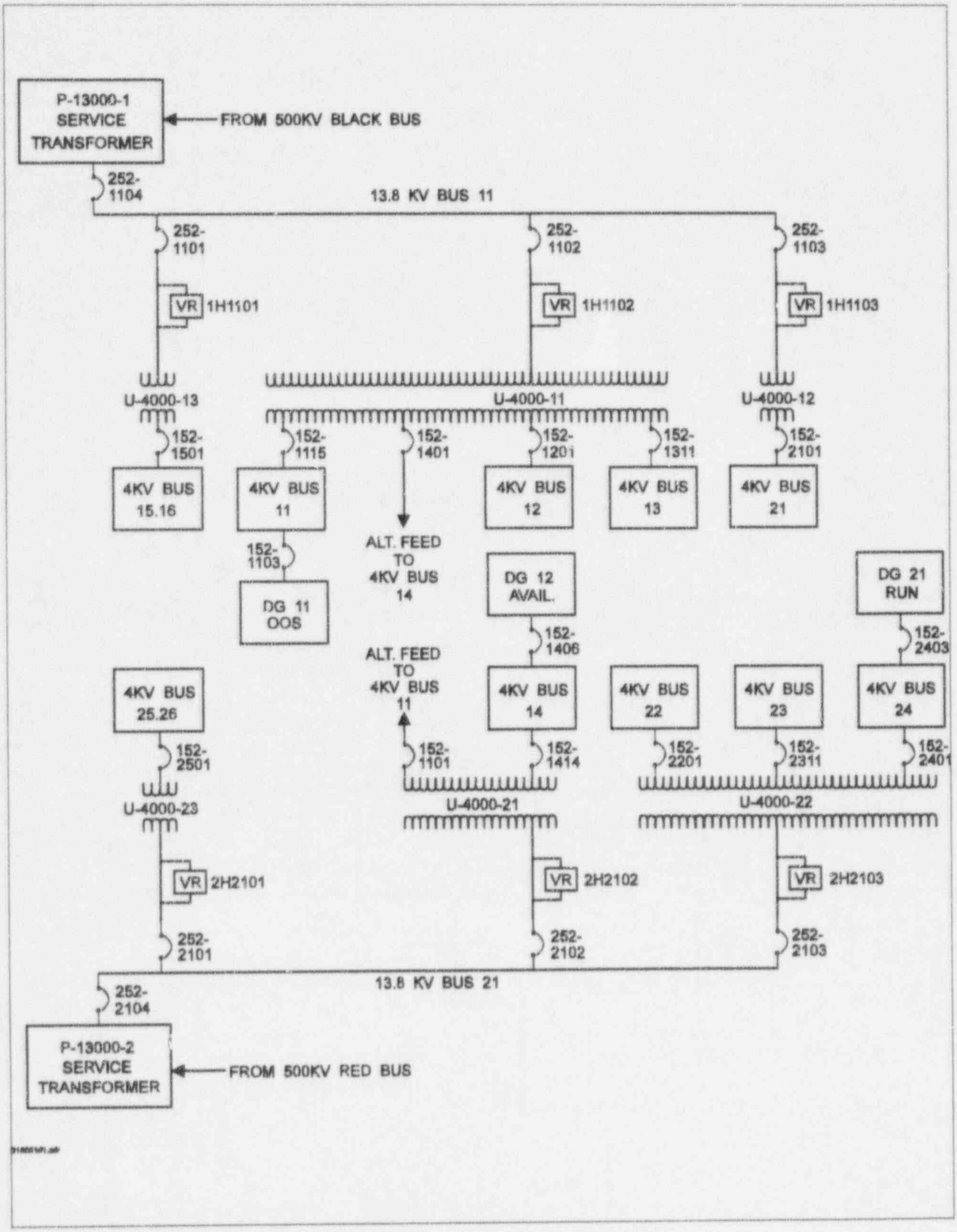
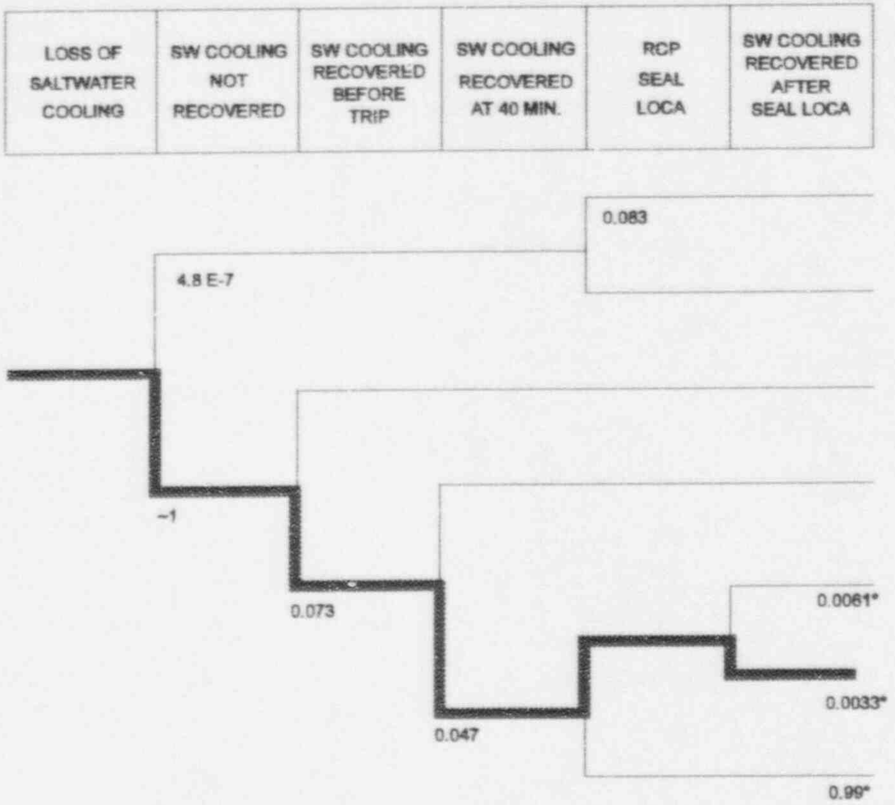


Figure C.8.1. Simplified drawing of Calvert Cliffs electrical distribution system.


LOSS OF SALTWATER COOLING
SW COOLING NOT RECOVERED
SW COOLING RECOVERED BEFORE TRIP
SW COOLING RECOVERED AT 40 MIN.
RCP SEAL LOCA
SW COOLING RECOVERED AFTER SEAL LOCA
0.083
4.8 E-7
~1
0.073
0.047
0.0061*
0.0033*
0.99*

SEQUENCE	CONDITIONING SEQUENCE PROBABILITY	RESULTING STATUS AND CONDITIONAL PROBABILITY	SEQUENCE CONDITIONAL PROBABILITY
1	4.0E-8	NOTE 1 1.0	4.0E-8
2	4.4E-7	NOTE 2 9.4E-5	<1.0E-8
No Trip			
3	7.0E-2	NOTE 3 3.5E-7	2.5E-8
4	2.1E-5	NOTE 4 2.1E-3	4.4E-8
5	1.1E-5	NOTE 1 1.0	1.1E-5
6	3.4E-3	NOTE 2 9.4E-5	3.2E-7
			1.1E-5

NOTE 1: This sequence results in an RCP seal LOCA with unavailable ECCS [p(cd|sequence) = 1.0].

NOTE 2: This sequence results in a LOFW with Bus 14 and ECCS unavailable to mitigate a stuck-open relief valve or for feed and bleed [p(cd|sequence) = 9.4E-5].

NOTE 3: This sequence results in a LOFW with one ECCS train unavailable to mitigate a stuck-open relief valve or for feed and bleed [p(cd|sequence) = 3.5E-7].

NOTE 4: This sequence results in an RCP seal LOCA with one train of ECCS unavailable [p(cd|sequence) = 2.1E-3].

* These values include the RCP seal LOCA probability

31800102.CRD

Figure C.8.2. Dominant core damage sequence for LER 318/94-001.

Table C.8.1. Basic event changes for Case 1

Event name	Description	Base probability	Current probability	Type
EPS-DGN-CF-ALL	Common Cause Failure of Diesel Generators	1.1E-003	4.2E-003	
EPS-DGN-FC-A	Diesel Generator A Failures	4.2E-002	1.0E+000	TRUE
EPS-XHE-NOREC	Operator Fails to Recover Emergency Power	8.0E-001	0.0E+000	FALSE
IE-LOOP	Initiating Event – Loss of Offsite Power	8.6E-006	1.0E+000	
IE-SGTR	Initiating Event – Steam Generator Tube Rupture	1.6E-006	0.0E+000	
IE-SLOCA	Initiating Event – Small Break LOCA	1.0E-006	0.0E+000	
IE-TRANS	Initiating Event – Transient	4.0E-004	0.0E+000	
OEP-XHE-NOREC-2H	Operator Fails to Recover Offsite power Within 2 hrs	2.2E-001	1.0E+000	TRUE
OEP-XHE-NOREC-6H	Operator Fails to Recover Offsite Power Within 6 hrs	6.7E-002	1.0E+000	TRUE
OEP-XHE-NOREC-BD	Operator Fails to Recover Offsite Power Before Battery Depletion	1.4E-002	2.2E-005	
OEP-XHE-NOREC-SL	Operator Fails to Recover Offsite Power (Seal LOCA)	5.5E-001	4.8E-001	
RCS-MDP-LK-SEALS	RCP Seals Fail Without Cooling and Injection	1.4E-001	2.8E-002	

Table C.8.2. Basic event changes associated with Case 2
Note 2 of Figure C.8.2

Event name	Description	Base probability	Current probability	Type
CSR-HTX-CF-ALL	Common Cause Failure of Shutdown Heat Exchangers	1.4E-005	1.0E+000	TRUE
CSR-MDP-CF-AB	Common Cause Failure of CSR MDPs	4.1E-004	1.0E+000	TRUE
HPI-MDP-CF-ALL	Common Cause Failure of HPI MDPs	1.0E-004	1.0E+000	TRUE
IE-LOOP	Initiating Event – Loss of Offsite Power	8.6E-006	0.0E+000	
IE-SGTR	Initiating Event – Steam Generator Tube Rupture	1.6E-006	0.0E+000	
IE-SLOCA	Initiating Event – Small Break LOCA	1.0E-006	0.0E+000	
IE-TRANS	Initiating Event – Transient	4.0E-004	1.0E+000	
LPI-MDP-CF-AB	Common Cause Failure of LPI Trains	5.6E-004	1.0E+000	TRUE
MFW-SYS-TRIP	Main Feedwater System Trips	2.0E-001	1.0E+000	TRUE
MFW-XHE-NOREC	Operator Fails to Recover Main Feedwater	3.4E-001	1.0E+000	TRUE
PCS-VCF-HW	TBVs/COND/CIRC Failures	3.0E-003	1.0E+000	TRUE
PPR-MOV-OO-BLK2	PORV 2 Block Valve Fails to Close	3.0E-003	1.0E+000	TRUE

Table C.8.3. Basic event changes associated with Case 2 Note 3 of Figure C.8.2

Event name	Description	Base probability	Current probability	Type
CSR-HTX-CF-ALL	Common Cause Failure of Shutdown Heat Exchangers	1.4E-005	0.0E+000	FALSE
CSR-HTX-FC-1A	Shutdown Heat Exchanger A Fails	1.4E-004	1.0E+000	TRUE
CSR-MDP-CF-AB	Common Cause Failure of CSR MDPs	4.1E-004	0.0E+000	FALSE
CSR-MDP-FC-1A	CSR MDP Train 1A Failures	3.9E-003	1.0E+000	TRUE
HPI-MDP-CF-ALL	Common Cause Failure of HPI MDPs	1.0E-004	3.7E-004	
HPI-MDP-FC-1A	HPI MDP Train 1A Failures	3.9E-003	1.0E+000	TRUE
IE-LOOP	Initiating Event – Loss of Offsite Power	8.6E-006	0.0E+000	
IE-SGTR	Initiating Event – Steam Generator Tube Rupture	1.6E-006	0.0E+000	
IE-SLOCA	Initiating Event – Small Break LOCA	1.0E-006	0.0E+000	
IE-TRANS	Initiating Event – Transient	4.0E-004	1.0E+000	
LPI-MDP-CF-AB	Common Cause Failure of LPI Trains	5.6E-004	0.0E+000	FALSE
LPI-MDP-FC-1A	LPI Train A Fails	3.9E-003	1.0E+000	TRUE
MFW-SYS-TRIP	Main Feedwater System Trips	2.0E-001	1.0E+000	TRUE
MFW-XHE-NOREC	Operator Fails to Recover Main Feedwater	3.4E-001	1.0E+000	TRUE
PCS-VCF-HW	TBVs/COND/CIRC Failures	3.0E-003	1.0E+000	TRUE

Table C.8.4. Basic event changes associated with Case 2 Note 4 of Figure C.8.2

Event name	Description	Base probability	Current probability	Type
CSR-HTX-CF-ALL	Common Cause Failure of Shutdown Heat Exchangers	1.4E-005	0.0E+000	FALSE
CSR-HTX-FC-1A	Shutdown Heat Exchanger A Fails	1.4E-004	1.0E+000	TRUE
CSR-MDP-CF-AB	Common Cause Failure of CSR MDPs	4.1E-004	0.0E+000	FALSE
CSR-MDP-FC-1A	CSR MDP Train 1A Failures	3.9E-003	1.0E+000	TRUE
HPI-MDP-CF-ALL	Common Cause Failure of HPI MDPs	1.0E-004	3.7E-004	
HPI-MDP-FC-1A	HPI MDP Train 1A Failures	3.9E-003	1.0E+000	TRUE
IE-LOOP	Initiating Event – Loss of Offsite Power	8.6E-006	0.0E+000	
IE-SGTR	Initiating Event – Steam Generator Tube Rupture	1.6E-006	0.0E+000	
IE-SLOCA	Initiating Event – Small Break LOCA	1.0E-006	1.0E+000	
IE-TRANS	Initiating Event – Transient	4.0E-004	0.0E+000	
LPI-MDP-CF-AB	Common Cause Failure of LPI Trains	5.6E-004	0.0E+000	FALSE
LPI-MDP-FC-1A	LPI Train A Fails	3.9E-003	1.0E+000	TRUE
MFW-SYS-TRIP	Main Feedwater System Trips	2.0E-001	1.0E+000	TRUE
MFW-XHE-NOREC	Operator Fails to Recover Main Feedwater	3.4E-001	1.0E+000	TRUE
PCS-VCF-HW	TBVs/COND/CIRC Failures	3.0E-003	1.0E+000	TRUE

Table C.8.5. Basic event changes for Case 3
Unit 1 analysis

Event name	Description	Base probability	Current probability	Type
CSR-HTX-CF-ALL	Common Cause Failure of Shutdown Heat Exchangers	1.4E-005	0.0E+000	FALSE
CSR-HTX-FC-1A	Shutdown Heat Exchanger A Fails	1.4E-004	1.0E+000	TRUE
CSR-MDP-CF-AB	Common Cause Failure of CSR MDPs	4.1E-004	0.0E+000	FALSE
CSR-MDP-FC-1A	CSR MDP Train 1A Failures	3.9E-003	1.0E+000	TRUE
EPS-DGN-CF-ALL	Common Cause Failure of Diesel Generators	1.1E-003	0.0E+000	FALSE
EPS-DGN-FC-A	Diesel Generator A Failures	4.2E-002	1.0E+000	TRUE
EPS-DGN-FC-B	Diesel Generator B Failures	4.2E-002	1.0E+000	TRUE
HPI-MDP-CF-ALL	Common Cause Failure of HPI MDPs	1.0E-004	3.7E-004	
HPI-MDP-FC-1A	HPI MDP Train 1A Failures	3.9E-003	1.0E+000	TRUE
IE-LOOP	Initiating Event – Loss of Offsite Power	8.6E-006	4.8E-001	
IE-SGTR	Initiating Event – Steam Generator Tube Rupture	1.6E-006	0.0E+000	
IE-SLOCA	Initiating Event – Small Break LOCA	1.0E-006	0.0E+000	
IE-TRANS	Initiating Event – Transient	4.0E-004	0.0E+000	
LPI-MDP-CF-AB	Common Cause Failure of LPI Trains	5.6E-004	0.0E+000	FALSE
LPI-MDP-FC-1A	LPI Train A Fails	3.9E-003	1.0E+000	TRUE
OEP-XHE-NOREC-2H	Operator Fails to Recover Offsite Power Within 2 hrs	2.2E-001	1.1E-001	
OEP-XHE-NOREC-6H	Operator Fails to Recover Offsite Power Within 6 hrs	6.7E-002	3.6E-004	
OEP-XHE-NOREC-BD	Operator Fails to Recover Offsite Power Before Battery Depletion	1.4E-002	5.4E-006	
OEP-XHE-NOREC-SL	Operator Fails to Recover Offsite Power (Seal LOCA)	5.5E-001	4.4E-001	
RCS-MDP-LK-SEALS	RCP Seals Fail Without Cooling and Injection	1.4E-001	2.5E-002	

Table C.8.6. **Basic event changes for Case 3**
Unit 2 analysis

Event name	Description	Base probability	Current probability	Type
EPS-DGN-CF-ALL	Common Cause Failure of Diesel Generators	1.1E-003	0.0E+000	FALSE
EPS-DGN-FC-A	Diesel Generator A Failures	4.2E-002	1.0E+000	TRUE
EPS-DGN-FC-SWG	Swing Diesel Generator Failures	4.2E-002	1.0E+000	TRUE
IE-LOOP	Initiating Event – Loss of Offsite Power	8.6E-006	4.8E-001	
IE-SGTR	Initiating Event – Steam Generator Tube Rupture	1.6E-006	0.0E+000	
IE-SLOCA	Initiating Event – Small Break LOCA	1.0E-006	0.0E+000	
IE-TRANS	Initiating Event – Transient	4.0E-004	0.0E+000	
OEP-XHE-NOREC-2H	Operator Fails to Recover Offsite Power Within 2 hrs	2.2E-001	1.1E-001	
OEP-XHE-NOREC-6H	Operator Fails to Recover Offsite Power Within 6 hrs	6.7E-002	3.6E-004	
OEP-XHE-NOREC-BD	Operator Fails to Recover Offsite Power Before Battery Depletion	1.4E-002	5.4E-006	
OEP-XHE-NOREC-SL	Operator Fails to Recover Offsite Power (Seal LOCA)	5.5E-001	4.4E-001	
RCS-MDP-LK-SEALS	RCP Seals Fail Without Cooling and Injection	1.4E-001	2.5E-002	

Table C.8.7. **Sequence conditional probabilities for LER 318/94-001**

Event tree name*	Sequence name	Probability	% Contribution	Logic
SWCOOL (Case 2)	5	5.2E-005	96.3	/SWNR, SWTP, SW40, RCPLOCA, SWLOCA
LOOP (Case 1)	21	1.2E-006	1.8	/RT-L, /EP, AFW-L, OP-6H, F&B-L
Total (all sequences)		5.4E-005		

* All Case 3 sequences have probabilities of 10^{-6}

Table C.8.8. System names for LER 318/94-001

System name	Description
AFW-L	Auxiliary feedwater system fails (LOOP)
EP	Emergency power system fails
F&B-L	Feed and bleed fails (LOOP)
OP-6H	Failure to recover offsite power at 6 h (EP success)
RCPLOCA	RCP seal LOCA
RT-L	Reactor trip fails (LOOP)
SWLOCA	Bus 14 not recovered following RCP seal LOCA
SWNR	Bus 14 not recovered (component faults)
SWTP	Bus 14 not recovered before trip
SW40	Bus 14 not recovered at 40 min

C.9 LER No. 458/94-023

Event Description:	Scram, Main Turbine-Generator Fails to Trip, Reactor Core Isolation Cooling and Control Rod Drive Systems Unavailable
Date of Event:	September 8, 1994
Plant:	River Bend

C.9.1 Summary

With the plant at 97% power, spurious high-level scram signals from two newly replaced reactor level transmitters resulted in a reactor trip. Due to the nature of the trip signal, the main turbine and generator did not automatically trip and were manually tripped by plant operators. The manual generator trip resulted in a slow transfer of plant preferred power supplies to components in the condensate, feedwater, reactor protection system (RPS), circulating water, service water, and instrument air systems. A voltage transient at the time of the power supply transfer caused a control power fuse in the control rod drive (CRD) system to open, causing the loss of power to most control room indicators for the system and the CRD flow control valves to fail shut. Operators attempted to align the reactor core isolation cooling system (RCIC) to provide cooling water makeup to the reactor, but it tripped on overspeed and could not be restarted. The high pressure core spray (HPCS) system was then used to provide reactor makeup water. The conditional core damage probability estimated for this event is 1.8×10^{-5}.

C.9.2 Event Description

River Bend Station was operating at 97% power when two of four reactor water level channels simultaneously initiated spurious high-level scram signals, causing a reactor trip. Subsequent investigation determined that the two newly replaced channels of level instrumentation were insufficiently damped and were overly sensitive to random noise. Since only two of the channels sensed a high level, the logic for the turbine/generator and feedwater system trips was not satisfied.

Within 2 min of the reactor trip, the main generator megawatt output declined to zero and the generator began motoring. The reverse power relay protection for the generator failed to cause a trip due to a high power factor. Approximately 7 min after the reactor trip, the operators noticed that the main turbine had not tripped. Following a discussion, the turbine was manually tripped. The operators expected the main generator output breakers to open automatically at this point. When they did not, the operators manually tripped the breakers.

When the main generator output breakers were manually opened, the plant responded differently from the way the operators were trained to expect. The delayed power transfer resulted in the unexpected loss of the nonsafety-related electrical loads. This required the operators to manually restore power to these affected loads.

The power transfer delay caused the loss of all main feedwater pumps, all condensate pumps, both trains of the RPS, the A and C main circulating water pumps, one of two running normal service water pumps, both recirculation pumps, the turbine building ventilation system, one instrument air compressor, and miscellaneous nonessential control room indications. In addition, the main steam isolation valves (MSIVs) and other containment isolation valves closed, and the standby service water system automatically started.

The transfer delay did not affect the safety-related electrical busses (because they are normally powered from a different power source). Since no safety-related loads were lost, the emergency diesel generators did not get a start signal. The loss of the balance of plant (BOP) loads caused loss of the normal heat sink for reactor decay heat removal.

At the same time, a fuse in the CRD system blew. As a result, almost all the control room CRD indications were lost, and the CRD flow control valves failed shut. It took approximately 2-1/2 h for the operators to identify that the CRD parameters were not reading correctly. The only available indication of the CRD system operability was pump current.

Operators attempted to align RCIC to provide reactor vessel makeup, but it tripped on overspeed and could not be restarted. The HPCS pump was started to provide vessel injection. The operators also manually opened the safety relief valves (SRVs) intermittently to reduce reactor pressure by relieving steam to the suppression pool. The HPCS system isolated four times during the event due to swells from the lifting of the SRVs.

While taking the actions described above, the operators were also taking actions to return power to the RPS busses and to restore the feedwater system, condensate system, and turbine building ventilation. The condensate and feedwater systems required venting before they could be restarted.

About 1 h into the event (at 2127 hours), the residual heat removal system (RHR) was placed in the suppression pool cooling mode. At 2140 hours, the HPCS system suction switched to the suppression pool because of high suppression pool level.

At approximately 2209 hours, the shift superintendent declared an Unusual Event because (1) there was only one source of high-pressure makeup water to the reactor, (2) the event had the potential of degrading, and (3) additional personnel were required to assist in returning the BOP systems to service.

To help control the reactor pressure and water level, valves in the main steam drain system were opened to provide equalization of pressures around the MSIVs and to assist with pressure control by dumping steam to the condenser.

At approximately 2220 hours, operators had restored the condensate system, and at approximately 2321 hours the feedwater system was restored to service. The MSIVs were then opened, and the operators verified that reactor water level and pressure were being properly controlled. At 0017 hours on September 9, the HPCS pump was secured. At 0030 hours the Unusual Event was exited, and the plant was cooled down to the cold shutdown condition.

Additional information regarding this event can be found in NRC Augmented Inspection Team (AIT) Report 50-458/94-20, October 19, 1994 (Ref. 2).

C.9.3 Additional Event-Related Information

The event was initiated by a sensed high reactor water level. The reactor trip was set for +51 in. (level 8). The turbine/generator and feedwater pump trips would also occur at this level. There are four sensors (channels) in the RPS that detect a level 8 condition. The channels, identified as A, B, C, and D, are arranged in one-out-of-two-taken-twice logic for a reactor trip. The high-level condition must be detected by channels A or C and B or D. During this event, only channels C and D sensed high level. Channels A, B, and C are arranged in a two-out-of-three logic for feedwater system and turbine/generator trip signals. Since channels A and B did not sense a high level, the feedwater system and the turbine/generator did not automatically trip.

Post-event investigation revealed that the sensors for channels C and D were a different model than that used in channels A and B. The sensors for channels C and D were installed during the recent refueling outage. They were found to be overly sensitive to transient level signals.

The main generator did not automatically trip on reverse power due to the high-power factor that was experienced during the event. There are two reverse power relays. One is set at approximately 3 MW (at a 0 power factor angle) and is only enabled if the turbine stop valves are closed, as is the case following a turbine trip. The second relay is also set at approximately 3 MW (also at a 0 power factor angle) but does not require a turbine trip permissive. Post-event investigation found that these relays were sensitive to large power factor angles such as the power factor angle (approximately 85°) that existed when the main generator was motoring.

Post-event investigation revealed that the normally open RCIC governor valve was stuck in the open direction. As a result, when steam was admitted to the turbine, its speed incr?ased until the overspeed trip setpoint was reached. Upon disassembly, the governor valve stem was found to have excessive corrosion in the gland area. This corrosion caused the valve stem to stick and resist the hydraulic pressure that otherwise would have repositioned the valve.

C.9.4 Modeling Assumptions

This event was modeled as a transient with the power conversion system (PCS), condensate, feedwater, RCIC, and CRD systems unavailable.

The PCS was modeled as failed and not recoverable. During the actual event, it took approximately 2-1/2 h to equalize pressure across the MSIVs and restore the PCS. Therefore, the system failure probability (PCS-SYS-VF-MISC) and the nonrecovery value (PCS-XHE-XE-NOREC) were set to 1.0 (true).

The condensate and feedwater systems were modeled as failed and not recoverable. During the actual event, it took approximately 2 h to restore the condensate system and approximately 3 h to restore the feedwater system. A step in the feedwater system (FWS) abnormal procedure required the venting of the system under these circumstances regardless of whether system indications indicated the need for system venting. The emergency procedure for the FWS does not require the system to be vented. However, it is unclear when the emergency procedure would be used as opposed to the abnormal procedure used during this event. It is also unclear whether the system actually needed to be vented to ensure its operability under the conditions observed during this event. A high priority was placed on the restoration of the FWS, as its unavailability was, in part, the basis for declaring a Notification of Unusual Event. Given the other equipment that needed to be manually recovered during the event, it does not appear as if the FWS could have been recovered any faster. Therefore, although the pumps and valves were operable, the extended time period required to vent the system makes it unavailable as a source of high-pressure makeup. Therefore, the system failure probabilities (CDS-SYS-VF-COND and MFW-SYS-VF-FEEDW) and the nonrecovery values (CDS-XHE-XE-NOREC and MFW-XHE-XE-NOREC) were set to 1.0 (true).

Since there were no failures in the FW or condensate systems, the systems would be recoverable in the long term. The current ASP models do not account for recovery at this point in the sequences. However, since the dominant sequence (sequence 31) involves early injection system failures, incorporation of long-term feedwater recovery into the model would have little affect on the conditional core damage probability for this event.

The RCIC system was modeled as unavailable and nonrecoverable. Following the event, investigation revealed that the turbine governor would not function due to excessive corrosion. Therefore, the system failure probability (RCI-TDP-FC-TRAIN) and the nonrecovery value (RCI-XHE-XE-NOREC) were set to 1.0 (true).

The CRD system was modeled as failed and not recoverable. The lack of control room indication and the failed closed flow control valves were not identified for approximately 2-1/2 h into the event. Once the incorrect readings were noted, it took an additional 55 min to restore the system to operability. The operators were concerned with high-pressure injection systems as noted by the basis for the declaration of the notification of unusual event. It would seem unlikely that the CRD system could have been restored faster based on the number of tasks that needed to be accomplished (systems that needed to be restored) and the need for additional manpower. Therefore, modeling the system as inoperable and unrecoverable in the time period required to maintain core cooling is appropriate. The pump train failure probabilities (CRD-MDP-FC-TRNA and CRD-MDP-FC-TRNB) and the nonrecovery value (CRD-XHE-XE-NOREC) were set to 1.0 (true). It was assumed that the system could be recovered in time to operate following the successful operation of low-pressure core spray or low-pressure coolant injection, failure of RHR, and successful containment venting. Therefore, the operator nonrecovery value under these conditions (CR1-XHE-XE-NOREC) was not modified.

The HPCS isolation valve closed four times during the event due to a high vessel level (level 8 signal). The additional cycling of the isolation valve was not explicitly modeled.

Standby Service Water Pump 2A discharge valve 1-SWP*MOV40A did not fully open when the pump started and control room position indication for the valve was lost. Post-event investigation indicated that the valve opened approximately 20%. The valve was subsequently opened manually by an operator. The valve failed to fully open due to a short in one of the control cables. Although this valve did not fully open automatically, the valve was modeled with a nominal failure rate. Given that the other SSW pumps and valves operated, flow through the system was sufficient to provide the design cooling loads.

Other support systems, such as instrument air, were also impacted by the slow power transfer that occurred during this event. However, it was assumed that these systems were restored quickly following the recovery of offsite power to the nonemergency buses. It was assumed that the loss of these systems had minimal impact on the oepration of safety-related systems. As a result, the modeling was not modified as a result of these support system failures.

C.9.5 Analysis Results

The conditional core damage probability estimated for this event is 1.8×10^{-5}. The dominant sequence highlighted on the event tree in Figure C.9.1 involves a trip, failure of the PCS, operation of the SRVs with no more than one valve failing to close, failure of high-pressure makeup systems (MFW, HPCS, and RCIC), failure of the ADS system, and failure of the CRD system.

A sensitivity calculation was performed to determine the impact of assuming the condensate and main feedwater systems were unrecoverable. If the nominal nonrecovery values are used, the conditional core damage probability for the event decreases by a factor of 2.2 to 8.0×10^{-6}.

Definitions and probabilities for basic events are shown in Table C.9.1. The conditional probabilities associated with the highest probability sequences are shown in Table C.9.2. Table C.9.3 describes the system names associated with the dominant sequences. Cutsets associated with each sequence are shown in Table C.9.4.

C.9.6 References

1. LER 458/94-023, Rev. 1, "Reactor Scram Due to Spurious Signals from Undamped Rosemount Model 1153 Transmitters," December 12, 1994.
2. NRC Augmented Inspection Team Report No. 50-458/94-20, October 19, 1994.

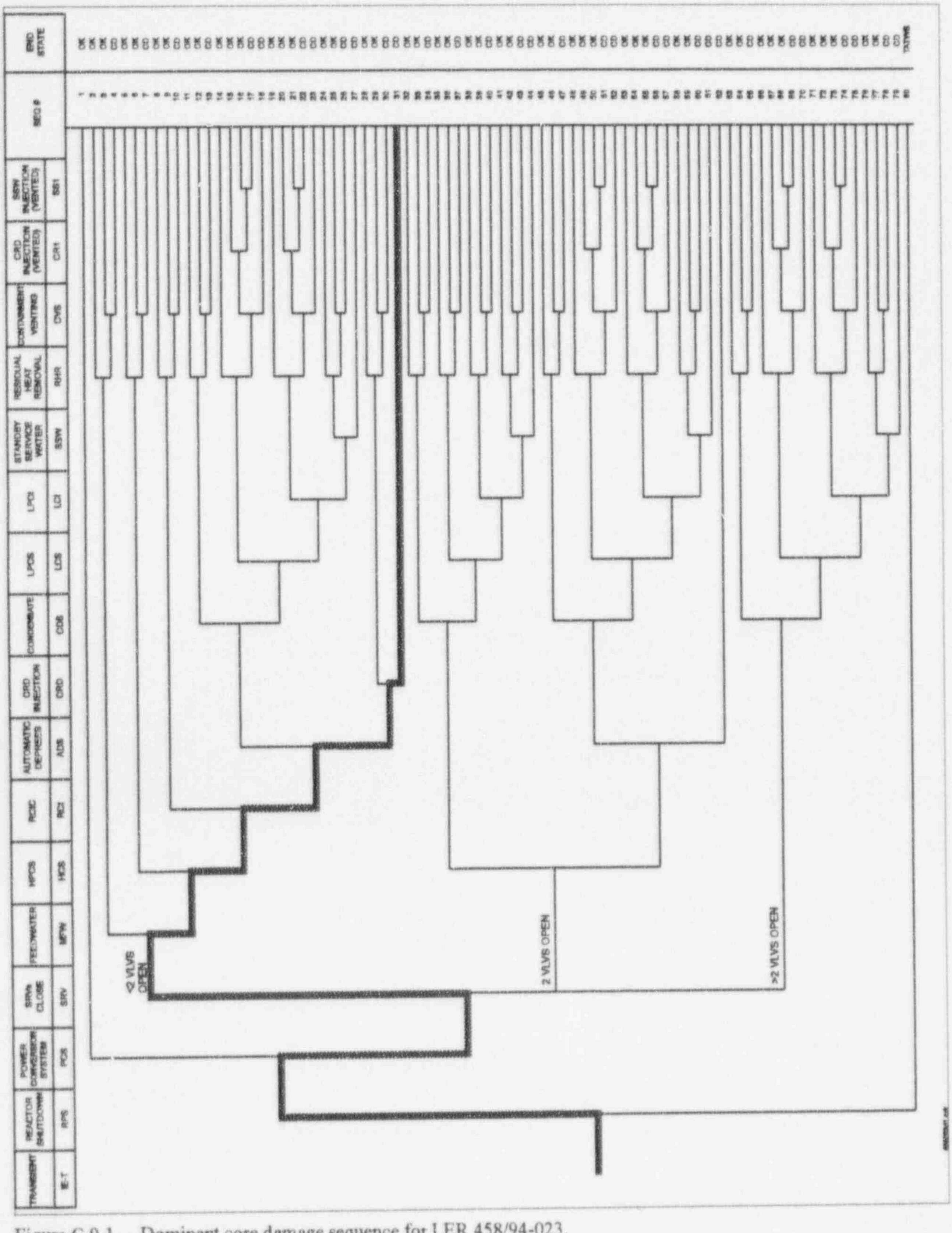


Figure C.9.1. Dominant core damage sequence for LER 458/94-023.

Table C.9.1. Definitions and probabilities for selected basic events for LER 458/94-023

Event name	Description	Base probability	Current probability	Type	Modified for this event
ADS-SRV-CC-VALVS	ADS Valves Fail to Open	3.7E-003	3.7E-003		N
ADS-XHE-XE-ERROR	Operator Error Prevents Depressurization	1.0E-003	1.0E-003		N
ADS-XHE-XE-NOREC	Operator Fails to Recover ADS	7.1E-001	7.1E-001		N
CDS-SYS-VF-COND	Condensate Hardware Components Fail	3.4E-001	1.0E+000	TRUE	Y
CDS-XHE-XE-NOREC	Operator Fails to Recover Condensate	1.0E+000	1.0E+000	TRUE	Y
CRD-MDP-FC-TRNA	Train A Failures	7.2E-004	1.0E+000	TRUE	Y
CRD-MDP-FC-TRNB	Train B Failures	7.2E-003	1.0E+000	TRUE	Y
CRD-XHE-XE-NOREC	Operator Fails to Recover CRD	1.0E+000	1.0E+000	TRUE	Y
CR1-XHE-XE-NOREC	Operator Fails to Recover CRD (After Venting)	1.0E+000	1.0E+000		N
HCS-MDP-FC-TRAIN	HPCS Train Level Failures	6.6E-003	6.6E-003		N
HCS-XHE-XE-NOREC	Operator Fails to Recover HPCS	7.0E-001	7.0E-001		N
IE-LOOP	Loss-of-Offsite Power Initiator	1.7E-005	0.0E+000	IGNORE	Y
IE-SLOCA	Small LOCA Initiator	4.8E-007	0.0E+000	IGNORE	Y
IE-TRAN	Transient Initiator	1.1E-003	1.0E+000		Y
MFW-SYS-VF-FEEDW	MFW Hardware Components Fail	4.6E-001	1.0E+000	TRUE	Y
MFW-XHE-XE-NOREC	Operators Fail to Recover Feedwater	3.4E-001	1.0E+000	TRUE	Y
PCS-SYS-VF-MISC	PCS Hardware Components Fail	1.7E-001	1.0E+000	TRUE	Y
PCS-XHE-XE-NOREC	Operator Fails to Recover PCS	1.0E+000	1.0E+000	TRUE	Y
RCI-TDP-FC-TRAIN	RCIC Train Component Failures	4.0E-002	1.0E+000	TRUE	Y
RCI-XHE-XE-NOREC	Operator Fails to Recover RCIC	7.0E-001	1.0E+000	TRUE	Y
SRV	One or Less SRV Fail to Close	2.2E-003	2.2E-003		N

Table C.9.2. Sequence conditional probabilities for LER 458/94-023

Event tree name	Sequence name	Conditional core damage probability (CCDP)	% Contribution	Logic
TRANS	31	1.6E-005	89.8	/RPS, PCS, /SRV, MFW, HCS, RCI, ADS, CRD
TRANS	07	1.5E-006	8.1	/RPS, PCS, /SRV, MFW, /HCS, RHR, CVS
Total (all sequences)		1.8E-005		

Table C.9.3. System names for LER 458/94-023

System name	Description
ADS	Automatic Depressurization Fails
CRD	Insufficient CRD Flow to RCS
CVS	Containment (Suppression Pool) Venting
HCS	HPCS Fails to Provide Sufficient Flow to Reactor Vessel
MFW	Failure of Main Feedwater System
PCS	Power Conversion System
RCI	RCIC Fails to Provide Sufficient Flow to RCS
RHR	Residual Heat Removal Fails
RPS	Reactor Shutdown Fails
SRV	One or Less SRV Fail to Close

Table C.9.4. Conditional cut sets for higher probability sequences for LER 458/94-023

Cut set No.	% Contribution	Frequency	Cut sets*
TRANS Seq: 31		1.600E-005	
1	72.3	1.200E-005	ADS-SRV-CC-VALVS, ADS-XHE-XE-NOREC, HCS-XHE-XE-NOREC, HCS-MDP-FC-TRAIN, /SRV
2	27.5	4.600E-006	ADS-SRV-XE-ERROR, HCS-XHE-XE-NOREC, HCS-MDP-FC-TRAIN, /SRV
TRANS Seq: 07		1.5E-006	
1	65.5	9.9E-007	CVS-XHE-XE-VENT, RHR-MDP-CF-MDPS, /SRV, CSS-XHE-XE-NOREC, SDC-XHE-XE-NOREC, SPC-XHE-XE-NOREC
2	9.4	1.4E-007	CVS-XHE-XE-VENT, RHR-MDP-FC-TRNB, RHR-MDP-FC-TRNA, /SRV, CSS-XHE-XE-NOREC, SDC-XHE-XE-NOREC
Total (all sequences)		1.800E-005	

Appendix D:

Shutdown Precursors

D.1 Shutdown Precursors

D.1.1 Accident Sequence Precursor Program Event Analyses for Shutdown Events for 1994

This appendix documents 1994 operational events selected as accident sequence precursors that are analyzed with the plant in a shutdown condition.

Licensee Event Reports (LERs) and other event documentation describing operational events at commercial nuclear power plants were reviewed for potential precursors if

1. the LER was identified as requiring review based on a computerized search of the Sequence Coding and Search System data base maintained at Oak Ridge National Laboratory or
2. the LER or other event documentation was identified as requiring review by the NRC Office for Analysis and Evaluation of Operational Data.

Details of the precursor review, analysis, and documentation process are provided in Chapter 2 and Appendix A of this report.

D.1.2 Shutdown Precursors Identified

One shutdown precursor was identified among the 1994 events reviewed at the Nuclear Operations Analysis Center. Events were identified as shutdown precursors if they met the following precursor selection criteria:

1. the event involved a core damage initiator such as a loss of shutdown cooling, loss of reactor vessel inventory, loss of offsite power, or a loss-of-coolant accident, and
2. the initiator could only have occurred with the plant in a shutdown condition, and
3. the conditional core damage probability estimated for the event was at least 10^{-6}.

The shutdown precursors identified are listed in Table D.1.

Table D.1 List of shutdown precursors

Event No.	Plant	Event description	Page
IR 482/94-18	Wolf Creek	Reactor Coolant System Blows Down to Refueling Water Storage Tank During Hot Shutdown	D.2-1

D.1.3 Event Documentation

Analysis documentation and precursor calculation information for each shutdown precursor are attached. The precursors are in docket/LER number order.

The analysis of each shutdown precursor includes a description of the operational event, event-related plant design information, the assumptions and approach used to model the event, conditional core damage calculation information, analysis results, and references.

D.2 LER No. Inspection Report 482/94-18

Event Description: Reactor Coolant System Blows Down to Refueling Water Storage Tank During Hot Shutdown

Date of Event: September 17, 1994

Plant: Wolf Creek

D.2.1 Summary

On September 17, 1994, about 28 h after shutting down to begin a refueling outage, an inappropriate alignment of the residual heat removal (RHR) system allowed the rapid transfer of about 9,200 gal of water from the reactor coolant system (RCS) to the refueling water storage tank (RWST). Operators corrected the misalignment within about 66 s. Subsequent analyses have shown that, had the operators not acted within about 3 min, the RCS could have been voided down to the loop piping elevation, potentially rendering all emergency core cooling systems (ECCSs) inoperable. With the RCS vented to the environment through the RWST, core uncovery could have occurred in as little as 30 min. The conditional core damage probability estimated for this event is 3.0×10^{-3}.

D.2.2 Event Description

At 0400 hours on September 17, 1994, Wolf Creek was in Mode 4 preparing to begin a refueling outage with an RCS pressure of 340 psig and temperature of 300°F. Two reactor coolant pumps (RCPs) were in service, the steam generators (SGs) were filled, and the condenser and condensate systems were secured. The safety injection (SI) pumps and one of two centrifugal charging pumps were out of service with breakers open to prevent low-temperature overpressurization. RHR train A was in service to provide shutdown cooling.

Activities in progress included monitoring RCS cooldown and depressurization, performing a 24-h emergency diesel generator test run, and responding to alarms caused by minor component cooling water (CCW) system problems. Maintenance work was being performed on RHR valve 8716A, the A RHR to SI system hot leg recirculation isolation valve, and efforts were in progress to ready RHR train B for use.

RHR train B was being lined up for recirculation back to the RWST in order to raise boron concentration before placing the train in service. This required the opening of valve 8717, a manual valve in the 8-in. common line from the RHR pump discharge headers to the RWST ECCS pump suction header. A nuclear station operator (NSO) was dispatched to locally open valve 8717.

The reactor operator was controlling the chemical and volume control system (CVCS) in preparation for taking the RCS solid. This effort was complicated by failure of the volume control tank's nitrogen cover gas pressure regulator. The balance of plant (BOP) operator was lining up the B RHR train for service and adjusting the CCW system to deal with incoming alarms. The operators then received a call from a plant electrician requesting that valve 8716A be stroked (closed and reopened) in support of a test procedure. Meanwhile, the NSO had arrived at valve 8717 and prepared to open it.

Approximately 3 ft from the NSO, the electrician was working on valve 8716A, but neither he nor the NSO recognized the significance of opening valves 8717 and 8716A simultaneously. When opened together, valves 8716A and 8717 provide a direct pathway from the RHR pump discharge to the RWST ECCS suction header. When the control room operator closed valve 8716A from the control room, the operator stationed at valve 8717 apparently had only begun opening it. As water flowed from the RCS to the RWST, pressurizer level dropped about 2%, but this was not noted until the event was reviewed later. After valve 8716A closed, the control room operator waited about 30 s and then reopened it.

Valve 8717 was fully open by this time, and reactor coolant inventory began rapidly flowing to the RWST. The operator stationed at 8717 observed loud flow and water hammer noises, called the control room to report them, and was instructed to close the valve. This instruction was apparently based on good operating practice to reclose a valve when unexpected flow and noise results from opening it, rather than from an understanding of the circumstances of the event. At the same time, control room personnel received a high RWST level alarm, the pressurizer level high annunciator cleared, and the pressurizer level instrumentation "pegged low."

Operators responded by tripping the RCPs, increasing charging flow, and manually isolating letdown. A relief supervising operator who was present at the time identified the flow path through valves 8716A and 8717 to the RWST. Operators closed valve 8716A, isolating the blowdown about 66 s into the event.

During the time that the blowdown was in progress, about 9,200 gal flowed from the RCS to the RWST causing the RWST to overflow. Approximately 650 gal overflowed from the RWST to the waste holdup tank.

The RHR and charging systems remained in service, and RCS level was gradually restored.

Additional information related to this event is contained in LER 482/94-013, "Personnel Error Resulted in an Unanticipated Loss of Reactor Coolant Level."

D.2.3 Additional Event-Related Information

Subsequent analysis determined that, had the blowdown not been quickly isolated, the primary system could have drained down to the RCS loop elevation in as little as 3 min. The RWST ECCS suction header could have been filled with steam shortly thereafter. It was further determined that an operating RHR pump could have been damaged by as little as 0.5 min of operation after the primary system drained down to the RCS loop elevation. Unisolated, the blowdown could have led to core uncovery in as little as 30 min, based on a Westinghouse analysis of the event.

The Westinghouse analysis, performed after the event, suggests that once the RWST ECCS suction header voided, operation of the multistage SI pumps would have resulted in their failure. Isolation of the blowdown path would have allowed water to flow back from the RWST into the suction header; however, there is no assurance that the ECCS pumps could fulfill their functions while drawing water from the RWST following such an event.

The Westinghouse analysis also indicates that if the suction header voided, recovery would be problematic even if the RHR pumps were shut off in time. In less than the time required to fill, vent, and restart an RHR pump, reactor pressure could exceed the RHR reactor high-pressure shutoff point.

Also noteworthy in this event is the fact that the containment was bypassed. Had the blowdown not been isolated, core damage could have occurred in as little as 30 min. A direct pathway would have existed via the RHR return line to the RWST and to the environment via the RWST vent. Off-site doses could be expected to exceed technical specification limits under such conditions.

D.2.4 Modeling Assumptions

Evaluation of this event is strongly influenced by assumptions regarding human reliability, the time and degree of effort required to recover ECCSs, and the viability of the "reflux" cooling method, wherein steam from a boiling core may be condensed in the SG tubes with the condensate draining back to the reactor. Substantial uncertainty is associated with each of these assumptions.

Approximately 3 min was available for the operators to diagnose and isolate the blowdown before all RHR and ECCS pumps were rendered inoperable. Even though procedures did not address the response to this condition, the operators' understanding of the existing system alignment allowed them to rapidly diagnose and correct the problem. During the event, the blowdown was isolated after a period of 66 s.

To estimate the likelihood that operators would fail to isolate the blowdown prior to uncovering the RCS loops, the time reliability correlation (TRC) models from *Human Reliability Analysis* (Dougherty and Fragola, Wiley, 1988) were employed. Operator response within the first 3 min was assumed to be rule-based and without hesitancy. This is considered appropriate based on the indications available to the operators at the time. Assuming the median response time to be the response time observed in this event (~60 s), and using Table 10-8 of Dougherty and Fragola, a crew error probability of 0.06 is estimated.

Had operators failed to isolate the blowdown path within 3 min, a direct vent path would have been established from the RCS through the RWST. Analyses were performed showing that core damage could have occurred as little as 27 min later.

After the RCS loops voided at 3 min, the ECCS common suction header would have begun to void. Additional consequences of a failure to terminate the event prior to this point would require more difficult operator actions. These actions were considered recovery (general diagnosis that must be used in the absence of rules) with hesitancy (due to conflict, burden, and uncertainty) within the context of the TRC model. Based on Table 10-11 in Dougherty and Fragola, a crew failure probability of 0.05 is estimated for the 27-min time period.

If the blowdown had been isolated after the loops voided (after 3 min, but before 30 min), substantial time and effort would have been required to refill and vent the RWST ECCS suction header and the ECCS pump suctions that are aligned to it. An analysis performed by Westinghouse indicates that significant voids entrained in the suction supply (5 to 20%) would guarantee a loss of ECCS prime [Reference 3], and other analyses have shown that operation in that condition for more than a minute or two would cause pump failure.

Without extensive venting and priming, the high-pressure pumps would be expected to fail after loop voiding. A report concerning the event indicated that there was no assurance that the ECCS pumps would fulfill their function while drawing water from the RWST following the event [Reference 4]. Further, questions have been raised regarding the structural integrity of the RWST, if it were subjected to the water hammer effects from a blowdown. The high-pressure ECCS pumps were, therefore, assumed in this analysis to be unavailable once the RWST ECCS suction header voided.

A conservative analysis (without consideration of SG secondary-side inventory that existed during the event) showed that, without some form of decay heat removal, pressure in the RCS could exceed the RHR shutoff head within as little as 15 min. This is less than the time that would likely be required to restore the RHR system to service. Because the power-operated relief valves were found to be inoperable subsequent to this event, it was assumed that depressurization of the RCS would have been difficult to achieve. The RHR pumps were, therefore, assumed to be inoperable once the RWST ECCS suction header voided. The only remaining decay heat removal path would be reflux cooling via the SGs. The SGs were available during the event, and reflux cooling was considered a viable core cooling method. In the short term, the water inventory in the SG would provide decay heat removal. Eventually, SG makeup and the opening of atmospheric vent valves would be required for continued heat removal via this method. Reflux cooling was assumed to require two SGs and one source of feedwater for success (consistent with SBO requirements). Assuming both motor-driven auxiliary feedwater pumps and all four SGs and their atmospheric dump valves are available, a failure probability of $\sim 7.0 \times 10^{-4}$ is estimated for reflux cooling based on component failure probabilities used in the IRRAS-based ASP models for Wolf Creek. It should be noted that this estimate addresses equipment availability only and not the uncertainty in the viability of the reflux cooling method. Since consideration of such uncertainty is beyond the scope of this analysis, the potential impact of reflux cooling being unavailable or ineffective was addressed in a sensitivity analysis.

The analysis of this event follows the simple event tree in Figure D.2.1. The tree includes the following branches:

BLOWDN. Blowdown. Blowdown of RCS inventory via valves 8717 and 8716A.

ISOS-S. Isolation in the short term (3 min). Isolation of the blowdown within 3 min is assumed to prevent voiding of the RCS. After the RCS loops voided at 3 min, RCS pressure would have rapidly dropped, and the ECCS common suction header would have begun to void. It was assumed that once the RWST ECCS suction header voided, the high-pressure ECCS pumps would be unavailable.

ISOS-L. Isolation in the long term (within the next 27 min). Had operators failed to isolate the blowdown path within 3 min, a direct vent path would have been established from the RCS through the RWST. Analyses were performed showing that core damage could have occurred as little as 27 min later.

REFLUX. Successful use of SG reflux cooling. If the blowdown is successfully isolated 3 to 30 min after the initiating event, SG reflux cooling must be successful to prevent core damage. ECCS is assumed to be unavailable due to voiding in the suction header.

D.2.5 Analysis Results

The probability of core damage for this event is the probability of sequence 3 (failure to isolate the RCS blowdown before voiding the RCS loops, successful isolation before core uncovery, and failure of reflux cooling) plus the probability of sequence 4 (failure to isolate the RCS blowdown before voiding the RCS loops and failure to isolate the blowdown before core uncovery):

$$0.06 \times (1-0.05) \times 7.0 \times 10^{-4} + 0.06 \times 0.05 = 3.0 \times 10^{-3} .$$

If reflux cooling is assumed to be viable, a core damage probability of 0.003 is estimated. This estimate is probably conservative because it assumes that all ECCS pumps are unavailable once significant voiding occurs in the ECCS common suction header. Assumptions concerning the viability of reflux cooling play an important role in the core damage probability estimated for this event. For example, it may be of interest to consider what reflux cooling failure probability would lead to a doubling of the estimated core damage probability. An assumed failure probability of ~0.05 for reflux cooling raises the estimated core damage probability by a factor of 2, to 6.0×10^{-3}.

D.2.6 References

1. LER 482/94-013, "Personnel Error Resulted in an Unanticipated Loss of Reactor Coolant Level," January 4, 1995.

2. NRC Inspection Report 482/94-18, "Drain-down event of September 17, 1994," December 9, 1994.

3. Wolf Creek RCS Draindown Event Analysis, NTD-NSRLA-95-083, Westinghouse Electric Co., February 1995.

4. Reactor Coolant System Blowdown at Wolf Creek on September 17, 1994, AEOD/S95-01, J. Kauffman and S. Israel, USNRC, March 1995.

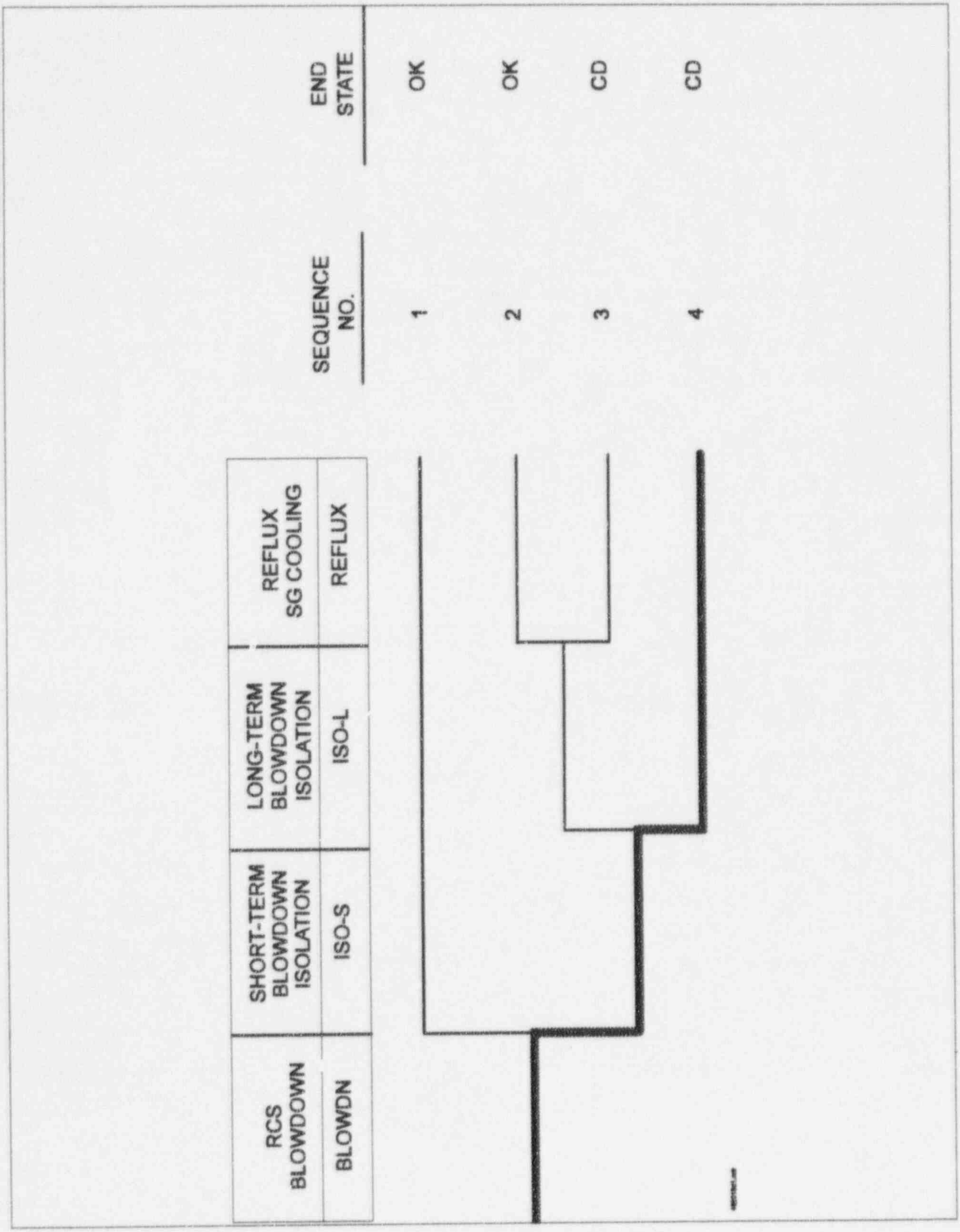


Figure D.2.1. Dominant core damage sequence for Inspection Report 482/94-18.

Appendix E:

Potentially Significant Events Considered Impractical to Analyze

E.1 Potentially Significant Events Considered Impractical to Analyze

Twelve events have been identified as potentially significant but impractical to analyze. It is believed that such events are capable of impacting core damage sequences. However, the events usually involve component degradations in which the extent of the degradation could not be determined or the impact of the degradation on plant response could not be ascertained.

The events identified for 1994 are shown in Table E.1. A summary, event description, and any additional event-related information are provided for these events.

Table E.1. Events identified as potentially significant but impractical to analyze

Event No.	Description	Plant name	Page
213/94-012	Potential Loss of Service Water Due to Potential Flooding	Haddam Neck	E.2-1
219/94-010	Emergency Service Water Declared Inoperable Due to Biological Fouling	Oyster Creek	E.3-1
237/94-004	HPCI Steamline Drain Potentially Inoperable	Dresden 2 & 3	E.4-1
237/94-006	Shutdown Cooling Pump Motor Replacement Inadequate	Dresden 2	E.5-1
249/94-S01, 254/94-S01	Cracks in Reactor Core Shroud	Dresden 3, Quad Cities 1	E.6-1
255/94-008	1E and Non-1E Circuits Not Properly Separated	Palisades	E.7-1
255/94-014	Potential Containment Sump Blockage from Signs, Labels, and Tape	Palisades	E.8-1
271/94-002	Alternate Cooling Tower System Inoperable During Warm Weather	Vermont Yankee	E.9-1
293/94-004	Reactor Core Isolation Cooling Found Inoperable During Surveillance	Pilgrim	E.10-1
295/94-011	Violation of 10CFR50, Appendix R Analysis Separation Criteria	Zion 1	E.11-1
382/94-004	Both Component Cooling Water Heat Exchangers Potentially Degraded	Waterford 3	E.12-1
454/94-003	Auxiliary Feedwater Isolation Valves Potentially Exposed to Harsh Environment	Byron 1	E.13-1

E.2 LER No. 213/94-012

Event Description: Potential Loss of Service Water Due to Potential Flooding

Date of Event: April 28, 1994

Plant: Haddam Neck

E.2.1 Summary

A previously unidentified external flooding scenario was discovered that had the potential to incapacitate the service water (SW) system during a river flood scenario less than that assumed in the design analysis.

E.2.2 Event Description

The Updated Final Safety Analysis Report (UFSAR) discusses the potential for flooding at Haddam Neck. The UFSAR states the probable maximum flood (PMF) occurs at an elevation of 39.5 ft mean sea level (MSL) and discusses the flood protection features at the site. The plant is protected from external floods up to an elevation of 30 ft MSL (plant grade level is about 21 ft MSL). Floods above 30 ft MSL are considered of very low probability, and no permanent features are provided; procedures and temporary equipment are to be used in case such floods occur.

A Service Water Operational Performance Inspection (SWOPI) was conducted to verify the ability of the SW system to meet its design basis. A flood slightly in excess of grade elevation was postulated as part of the SWOPI. This assumed flood would enter the intake structure and flood the lower level by means of a stairwell. Although the SW pumps would be protected by temporary fiberglass cans placed around the pump motors upon warning of an impending site flood, the flooding of the lower level of the intake structure would make the SW pump discharge strainers inaccessible for cleaning by normal means. River debris could then clog the discharge strainers to the point that the SW pumps would be incapable of delivering sufficient flow to maintain vital functions, such as emergency diesel generator cooling and residual heat removal.

Since the plant's emergency operating procedures require a plant shutdown prior to flooding at the plant site, the SW flow required would be greatly reduced compared to that for normal operation. The estimated total SW flow required would be ~2000 gpm compared to a single pump runout flow of about 7000 gpm. Therefore, the limited cooling requirements under this scenario would be satisfied for some period after flooding had rendered the strainers inaccessible by normal methods. Other actions would also be available to plant staff if this scenario occurred.

E.2.3 Basis for Selection as An Impractical to Analyze Event

The uncertainties with respect to the probability of the postulated flooding, the timing and magnitude of the SW flow loss, and the potential mitigating actions make this event impractical to analyze.

E.3 LER No. 219/94-010

Event Description: Emergency Service Water Declared Inoperable Due to Biological Fouling

Date of Event: July 5, 1994

Plant: Oyster Creek

E.3.1 Summary

On July 5, 1994, both containment spray (CS) and emergency service water (ESW) systems were declared inoperable due to high differential pressure on the tube side of the heat exchangers. The high differential pressure was due to biological fouling, specifically, blue mussel shells.

E.3.2 Event Description

During performance of the normal monthly system operability test for CS and ESW system 2, indications of heat exchanger tube side plugging were noticed on the control room instrumentation. The flow rate of the ESW pumps was indicating 2400 gpm versus the expected value of 3500 gpm. CS and ESW system 1 were tested, and similar results were obtained. The local heat exchanger tube side differential pressure indicators exceeded the operability limit of 40 psid for both heat exchangers. Both systems were declared inoperable.

The cause of the degraded performance was found to be plugging caused by blue mussel shells on the first pass tube sheet (the heat exchangers are a four-pass design). Almost all the mussels were found dead with very little tissue left in the shells. The source of the mussel shells was believed to be the ESW piping. The shells were released when the intake water exceeded the life supporting temperature of about 80°F, which can occur each summer. Plugging of the tube side of ESW heat exchangers has occurred during previous summers, but never to the extent observed during this event. This may have been due to the loss of the chlorination system, which is intended to operate when the ESW system is idle, but had been secured prior to this event.

Investigation revealed that the actual ESW flow rate was 3200 gpm, while the design basis flow rate is 3000 gpm. The flow rate error was due to plugging of the flow instrument sensing lines. One of the heat exchangers exceeded its structural limit of 70 psid. Inspection of the heat exchanger baffle plates indicated they were in a normal condition.

One of the additional corrective actions was to install piping inspection ports to assist in early detection of future biological growth inside the piping.

E.3.3 Basis for Selection as An Impractical to Analyze Event

Since the condition was discovered prior to complete dislodging of all the dead mussels in ESW piping, the final differential pressure that would have occurred is not known. In addition, the heat exchangers were degraded, but the flow rate was above the design basis flow rate. The effects of the degraded flow rates observed are difficult to determine. Therefore, this event is impractical to analyze.

E.4 LER No. 237/94-004

Event Description: HPCI Steamline Drain Potentially Inoperable

Date of Event: January 24, 1994

Plant: Dresden 2 & 3

E.4.1 Summary

On January 15, 1994, the Unit 3 high pressure coolant injection (HPCI) steamline drain isolation valve was replaced. During the replacement, it was determined that the existing valve had been installed backwards. On January 17, 1994, the Unit 2 valve was examined and also found to be installed backwards. The incorrect orientation could have prevented the valves from functioning as designed.

E.4.2 Event Description

During maintenance, the Unit 3 HPCI steamline drain isolation valve was disassembled and found to be installed backwards. Due to this discovery, the Unit 2 valve was also checked and also found to be installed backwards. The valves had been installed in the incorrect orientation since the plant's original construction and had been undetected during subsequent maintenance activities.

These valves are designed to open with system pressure assisting, i.e., flow under the plug. With the valves installed backwards, the flow is over the plug, and system pressure inhibits valve opening. The Unit 2 valve had a stronger spring installed on May 5, 1993. An engineering evaluation by the licensee showed that the valve would have functioned correctly after that date, even though it was installed backwards.

The HPCI steam line isolation valve is normally closed. The valve is maintained closed with air pressure and fails open due to its spring force. Upon HPCI initiation, the valve is signaled to open. If the drain valve fails to open during a HPCI initiation moisture could not drain from the HPCI steam line and would eventually back up through the drain line and the steam trap. If the HPCI turbine subsequently tripped and then was restarted, the accumulated moisture could be introduced into the HPCI turbine steam chest. In addition, if sufficient water were to collect upstream of the HPCI Turbine Steam Inlet valve, restarting the HPCI turbine could cause a slug of water to enter the turbine. The moisture in both cases potentially would damage the turbine blading, but not the turbine casing, which is designed to withstand such a condition.

Since damage could only occur after the HPCI turbine has initiated and the amount of water potentially entering the turbine is unknown, the safety significance was considered minimal. The likely principal effect would be to shorten the life of the turbine blades, but not the operability of the system. Historically, the drain valves had been the source of recurring problems, which were probably due to the incorrect installation.

E.4.3 Basis for Selection as An Impractical to Analyze Event

Although the valves were installed incorrectly, the HPCI turbine operated during previous demands of the pump. In addition, the amount of water collected was not known, and the possible HPCI turbine damage could not be quantified. Therefore, this event is impractical to analyze.

E.5 LER No. 237/94-006

Event Description: Shutdown Cooling Pump Motor Replacement Inadequate

Date of Event: February 5, 1994

Plant: Dresden 2

E.5.1 Summary

The protective relay setpoints for the shutdown cooling pump (SDC) motors were inadequate. The pump motors had been replaced without reviewing the setpoints.

E.5.2 Event Description

While installing new SDC pump motors on Dresden 3, it was recognized that the similar replacement on Dresden Unit 2 had not received an evaluation of the effect of new motors on the protective relay (breaker) settings. The Unit 2 SDC pump motors were then declared administratively inoperable.

An engineering analysis was performed to determine the correct relay setpoints and the effect on the engineered safeguard systems (ESS) buses of the old and new setpoints with the new pump motors. This analysis found that the existing settings were too low for the new pump motors. As such, the motor could have spuriously tripped its feeder breaker due to a high current signal. The feeder ESS buses would not be in jeopardy of becoming unavailable due to a fault at or on any of the SDC pump motors.

The SDC system at Dresden is not considered safety related, although it is included as one means of decay heat removal in accident sequence models. Since the protective relay settings were found to be conservative, i.e., too low, no threat to the ESS buses supplying the SDC pump motors existed due to this event.

E.5.3 Basis for Selection as An Impractical to Analyze Event

This event involves the potential loss of all or part of shutdown cooling due to false, spurious tripping of the SDC pump motor caused by relay settings. Since the probability for the tripping of one or more SDC pump motors could not be determined within the resources available to the ASP Program, this event is impractical to analyze.

E.6 LER No. 249/94-S01, 254/94-S01

Event Description: Cracks in Reactor Core Shroud

Date of Event: N/A

Plant: Dresden 3 & Quad Cities 1

E.6.1 Summary

During refueling outages, cracking in the reactor core shroud was discovered at both units.

E.6.2 Event Description

In April 1994, while both of these units were performing scheduled refueling outages, 360° circumferential cracking in the heat-affected zone (HAZ) of the "H5" weld was identified during visual inspections. Subsequent ultrasonic testing determined that the maximum crack depth for Dresden 3 was 0.84 in. (2.13 cm). The H5 weld is a horizontal weld that joins the core plate support ring to the core shroud. Crack indications had been previously reported at core shroud welds in domestic and overseas BWRs at the beltline region and higher in the shroud. Further information is available in NRC Information Notices IN 93-79, IN 94-42, and IN 94-42, Supplement 1.

The core shroud is a 2-in.-thick steel cylinder that surrounds the reactor core inside the reactor vessel. It provides the attachment point for the jet pumps and directs the water flow through the reactor core. It could be possible, during a seismic event, for the crack to completely extend through and around the core shroud.

E.6.3 Basis for Selection as An Impractical to Analyze Event

Because the probability of such catastrophic cracking occurring during a seismic event has not been quantified, this event is impractical to analyze.

E.7 LER No. 255/94-008

Event Description: 1E and Non-1E Circuits Not Properly Separated

Date of Event: March 29, 1994

Plant: Palisades

E.7.1 Summary

During the spring of 1994 while in cold shutdown, 12 instances were identified where Class 1E and non-Class 1E equipment was not isolated or separated as required.

E.7.2 Event Description

Non-Class 1E equipment is required to be isolated from Class 1E circuits so that a fault in a non-Class 1E circuit will not affect a Class 1E circuit. During inspections at the Palisades plant, the following circuits/systems were found to have cables violating these isolation requirements:

- low-temperature overpressure protection,
- inverter power cables,
- subcooled margin monitors,
- reactor protection system (power supplies),
- auxiliary feedwater system,
- condensate storage tank level,
- RPS temperature protection and thermal margin monitor,
- inverter output,

core exit thermocouples, and

- main steam isolation valves.

All but one of the discrepancies were corrected prior to starting up from the maintenance outage. The cause of the event was the inadequate or incomplete review of the system's design, which allowed the circuits to be modified or left in place without adequate isolation or separation. Contributing to the problem was the lack of composite schematic diagrams for use by engineering personnel. These problems have existed since the mid-1980s.

E.7.3 Basis for Selection as An Impractical to Analyze Event

Although a relatively large number of circuits/systems were deficient, no actual failures were observed. The probability of a fault occurring in a single non-Class 1E circuit and then affecting the nearby Class 1E circuit is unknown. This makes analyzing the event impractical.

E.8 LER No. 255/94-014

Event Description: Potential Containment Sump Blockage from Signs, Labels, and Tape

Date of Event: May 30, 1994

Plant: Palisades

E.8.1 Summary

With the plant in cold shutdown for a maintenance outage, signs, adhesive labels, and tape with the potential to block the containment sump were identified.

E.8.2 Event Description

Double-sided tape has been used to attach signs to walls, installed equipment, and piping. Self-adhesive labels and duct tape were also used within containment. In a worse-case scenario, if these items came loose, they could obstruct the containment sump screens and cause an unacceptable flow blockage for containment sump recirculation.

Following recognition of this condition, an extensive clean-up and relabeling effort was performed. All nonessential self-adhesive labels were removed from equipment including Dymo-tape labels, self-adhesive labels, duct tape, and other adhesive tapes used as markers on equipment. It was estimated that about 100 ft^2 of labeling material was removed. It was estimated that less than 10 ft^2 of labeling material remained in unaccessible areas.

An engineering analysis established that plastic signs and labels greater than 5.1-ft radial distance from the containment sump downcomer would not be drawn into the containment sump. Similarly, duct tape greater than 10.1-ft radial distance from the downcomer would also not be drawn into the sump. These areas were completely cleared of potential debris. With the limited labeling left in the containment, the analysis showed that there was no potential for affecting the operability of the containment sump.

Other corrective actions included revising the containment cleanliness checklist and the plant consumables control program. A comprehensive sign, tag, and labeling standard was also planned.

E.8.3 Basis for Selection as An Impractical to Analyze Event

Because the probability for actually degrading the containment sump cannot be quantified within the resources available to the ASP Program, this event is impractical to analyze.

E.9 LER No. 271/94-002

Event Description: Alternate Cooling Tower System Inoperable During Warm Weather

Date of Event: February 9, 1994

Plant: Vermont Yankee

E.9.1 Summary

The alternate cooling system (ACS) was found to be incapable of performing its design function under hot weather conditions.

E.9.2 Event Description

The ACS at Vermont Yankee is designed for removal of shutdown heat loads in the event all four service water (SW) pumps are unavailable due to (1) a loss of the Vernon Dam, (2) a postulated probable maximum flood (PMF), and (3) a major fire in the intake structure. There is no safety design basis for the ACS in the Final Safety Analysis Report (FSAR), and the system is not designed for redundancy, accident mitigation function, or single failure resistance.

During a self assessment of the SW and ACS, a deficiency was identified. The water supply for the ACS is a deep basin located under one of the two circulating water cooling towers. The FSAR stated that the ACS was designed to supply 85°F cooling water to the three residual heat removal service water pumps. During periods of warm weather operation, the initial temperature in the deep basin can exceed the 85°F assumed initial temperature limit of the ACS.

Analysis found that sufficient cooling would exist with a minimum flow of 8000 gpm, but this would exceed the normal heat exchanger flow limits in the operating procedures. Further analysis was performed, and the operating procedure for the ACS was revised. The revised procedure will accommodate a maximum initial deep basin temperature of 105°F (peak circulating return temperature recorded is 102°F) and the increased flows necessary. No plant equipment changes were necessary.

E.9.3 Basis for Selection as An Impractical to Analyze Event

The ACS is a nonsafety-related system designed to provide backup in case of the complete loss of the SW pumps. The probabilities of system failures from this cause are unknown. As a result, this event is impractical to analyze.

E.10 LER No. 293/94-004

Event Description: Reactor Core Isolation Cooling Found Inoperable During Surveillance

Date of Event: August 3, 1994

Plant: Pilgrim

E.10.1 Summary

On August 5, 1994, the reactor core isolation cooling (RCIC) turbine speed began to oscillate during postmaintenance testing due to problems with the turbine's lube oil system.

E.10.2 Event Description

On August 3, 1994, the RCIC system isolated on a high steam flow signal during performance of a system quarterly surveillance test. This isolation was due to binding of the governor valve. Following repair of the valve by properly aligning the fulcrum dowel pins, the system was operated on August 5, 1994. After the turbine had operated for about 15 min, the turbine speed began to oscillate, and the turbine was manually tripped. Concurrently, oil began to spray from the governor end bearing cover, the oil level on the coupling end bearing housing dropped below the sight glass level, and oil was seen on the turbine skid.

Following troubleshooting and discussions with the pump vendor, the cause of the oil level changes was determined to be air entrained in the system's lubricating oil. The air formed a bubble in the drain line from the governor end bearing, which prevented the oil from properly draining and caused the governor end bearing oil level to increase. The decreased oil level in the coupling end bearing was due to that bearing becoming the major source of oil to the sump because the other source, the governor end bearing, was not properly draining.

A number of corrective actions were taken in an attempt to prevent the entrainment of the air. These included sealing the oil pump suction tubing joints, verification of proper initial oil level, replacement of the lube oil (new oil had been used), replacement of the oil pump and oil pump regulator (relief) valve, and installation of vent line on both bearing oil drain lines. After each change, RCIC was operated, and in each case, the air entrainment occurred after 15–20 min of operation. Although a temporary vent line installation did provide conditions for a successful test run, the permanent vent installation resulted in minimal improvement.

Observations during troubleshooting and testing revealed that the oil aeration problem was minimized at turbine speeds less than rated. Since the lube oil pump is driven by the turbine shaft through worm gears, reduced lube oil pressure was a possible remedy. Based on this and with the concurrence of the turbine manufacturer, the oil relief/pressure control valve setpoint was adjusted from 12–15 to 8–10 psig. The reduced lube oil pressure proved to be successful at solving the problem.

This condition appears to be inherent to the system design. It had gone undetected since initial plant startup (more than 20 years) due to two facts: (1) prior operation, either for testing or actual demand, usually lasted less than 15 min; and (2) such operation was typically at less than rated speed, which resulted in reduced lube oil pressure.

NRC Information Notice (IN) 94-84, Air Entrapment in Terry Turbine Lubricating Oil System, was issued to address this problem. It documented this event and a similar one for the turbine-driven auxiliary feedwater system at Sequoyah 1. This IN noted that the turbine vendor had observed similar problems with some of the turbines during factory test runs or startup testing. A modification used by the manufacturer was to increase the bearing drain line size from 1 to 1.5 in.

E.10.3 Basis for Selection as An Impractical to Analyze Event

The RCIC turbine's ability to fully function had been impaired since initial criticality. The system had been determined to be operable most of the time based on its ability to pass surveillance and post-maintenance testing as well as to function in response to plant trips and losses of offsite power. However, the RCIC system had never been run for the long mission times assumed in accident sequence models. Since no data exists concerning the expected run times with the RCIC turbine in this condition, this event is considered impractical to analyze.

E.11 LER No. 295/94-011

Event Description: Violation of 10CFR50, Appendix R Analysis Separation Criteria

Date of Event: July 14, 1994

Plant: Zion 1

E.11.1 Summary

A deficiency in the Appendix R fire analysis was found that had the potential to disable the 0 emergency diesel generator (EDG) and the 1A and 1B centrifugal charging pumps.

E.11.2 Event Description

The 0 EDG is capable of supplying power to both Units 1 and 2. During preparation for work to replace Thermo Lag associated with the 0 EDG, it was noted that an adjacent cable was not fire-wrapped. This did not conform to Appendix R requirements. The unwrapped conduit provides power to a Unit 2 bus and is on the 0 EDG side of a Unit 2 bus feeder breaker. Since the cable is unprotected, it has a much greater likelihood of failing in a fire. This would render the 0 EDG inoperable since no protective device exists between the EDG output and the cable. The 1B centrifugal pump receives power from the 0 EDG, and the power cable for the 1A pump is routed through the same fire zone.

During the fire scenario of concern for this event, a loss-of-offsite power occurs in conjunction with the fire. With the disabling of both trains of the chemical and volume control system due to the loss of the two charging pumps, seal injection to the reactor coolant pumps (RCPs) would be unavailable, and an RCP seal LOCA could occur.

No immediate corrective action was necessary since the area had been under continuous fire watch since 1992 due to the use of Thermo Lag in the area.

E.11.3 Basis for Selection as An Impractical to Analyze Event

During a postulated fire in the fire zone, multiple trains of equipment could be lost, which would lead to a seal LOCA. However, the probability of fire in the fire zone of interest, the progression of the fire, and possible mitigating activities cannot be easily quantified. Therefore, this event is impractical to analyze.

E.12 LER No. 382/94-004

Event Description: Both Component Cooling Water Heat Exchangers Potentially Degraded

Date of Event: March 7, 1994

Plant: Waterford 3

E.12.1 Summary

The component cooling water (CCW) heat exchanger A was found to be degraded after performance testing. This condition was caused by biological fouling.

E.12.2 Event Description

During a refueling outage, performance testing of the A CCW heat exchanger was conducted in response to Generic Letter 89-13 requirements. The results of the testing revealed that the heat exchanger performance was degraded. The CCW system is designed to provide cooling water to safety-related components at a maximum temperature of 115°F under accident conditions. The extrapolated test results would result in a CCW outlet temperature of 117.2°F. Inspection with a boroscope of both CCW heat exchangers revealed deposits and microbiological activity on the outside diameter of the heat exchanger tubes. Both heat exchangers were chemically cleaned.

E.12.3 Basis for Selection as An Impractical to Analyze Event

Potentially, both CCW heat exchangers did not provide the required cooling. However, since the B CCW heat exchanger was not tested prior to its chemical cleaning, its actual condition due to the biological fouling is indeterminate. As a result, this event can not be analyzed.

E.13 LER No. 454/94-003

Event Description: Auxiliary Feedwater Isolation Valves Potentially Exposed to Harsh Environment

Date of Event: March 14, 1994

Plant: Byron 1 and 2

E.13.1 Summary

The removal of the flood seal openings (FSOs) between the main steam tunnel and the auxiliary feedwater (AFW) tunnel could expose AFW isolation valves to a harsh environment, a condition for which they are not analyzed.

E.13.2 Event Description

The FSO plates provide a barrier for the AFW from the environment created in the event of a main steamline break (MSLB) in the main steam safety valve room or steam pipe tunnel. They also ensure a watertight environment in the AFW tunnel in the event of turbine building flooding due to a circulating water pipe break. In part due to the barrier provided by the FSO plates, the environment in the AFW tunnel is considered mild, and the AFW isolation valves are not in the equipment qualification (EQ) program. However, the plates had been removed periodically since 1985 for maintenance activities during plant operations as allowed by plant administrative procedures. No basis for this removal of the FSO was documented.

If a MSLB or turbine building flooding occurred with the FSO removed, the potential existed for not being able to isolate a steam generator using the isolation valves in the AFW tunnel.

E.13.3 Basis for Selection as An Impractical to Analyze Event

Information concerning the potential for valve failure under flooding, high-temperature, or high-humidity conditions, and the frequency of initiating events that could impact these values is unavailable. This makes quantification of this event impractical.

Appendix F:

Containment-Related Events

F.1 Containment-Related Events

One reactor plant operational event for 1994 was selected as a containment-related event. Such events involve unavailability of a containment function, such as containment isolation, containment cooling, containment spray, or postaccident hydrogen control. Containment-related events are not currently considered precursor events as defined by the Accident Sequence Precursor (ASP) Program; however, information concerning historic failures that could result in reduced containment performance justifies their inclusion in the report. Containment models have not been developed as part of the ASP Program. The event identified for 1994 is shown in Table F.1

A summary and event description are provided for this event.

Table F.1. Events identified as containment-related

Docket/LER No.	Description	Plant Name	Page
336/94-040	Design Error Allows Unfiltered Release Path	Millstone 2	F.2-1

F.2 LER No. 336/94-040

Event Description:	Design Error Allows Unfiltered Release Path
Date of Event:	December 6, 1994
Plant:	Millstone Point 2

F.2.1 Summary

On December 6, 1994, with the plant defueled, it was determined that a release path existed that allowed a direct discharge to atmosphere without charcoal filtration.

F.2.2 Event Description

A system engineer reviewing a work package identified that a nonsafety-related system provided an untreated flow path from the enclosure building (containment) to the atmosphere. A hydrogen analyzer cabinet and sample hood exhaust fan were found to take suction on the enclosure building and discharge approximately 1000 cfm out the unit's main exhaust stack. Although the flow path did have HEPA filters, no charcoal adsorbers were in the flow path. An analysis concluded that 10CFR100.11 limits would be exceeded in the case of a major accident involving the release of appreciable quantities of the core's fission products.

F.2.3 Analysis Results

This event was not modeled as an accident sequence precursor since it is a containment-related event.

Appendix G:

"Interesting" Events

G.1 "Interesting" Events

Nine reactor plant operational events for 1994 were selected as "interesting" events. These events are documented in this section. "Interesting" events are not normally precursor events as defined by the Accident Sequence Precursor Program; however, they provide insight into unusual failure modes with the potential to compromise continued core cooling. The events identified for 1994 are shown in Table G.1.

A summary, event description, and any additional event-related information are provided for these events.

Table G.1. Index of "Interesting" events

Docket/LER No.	Description	Plant name	Page
245/94-015	Testing Error Drains Reactor to Drywell Spray While Plant Shutdown	Millstone 1	G.2-1
269/94-004	Past Unavailability of the Emergency Condenser Circulating Water and Low-Pressure Service Water Systems	Oconee 1	G.3-1
272/94-007	Reactor Trip, Two Safety Injection Actuations, and Solid Pressurizer Operation	Salem 1	G.4-1
275/94-020	Dual Reactor Trip Due to Grid Disturbances	Diablo Canyon 1 & 2	G.5-1
295/94-003	No Containment Pressure Indication on Startup	Zion 1	G.6-1
298/94-010	Difficulty Establishing Shutdown Cooling	Cooper	G.7-1
324/94-008	Plant-Centered Loss-of-Offsite Power	Brunswick 2	G.8-1
366/94-003	Loss of Shutdown Cooling	Hatch 2	G.9-1
529/94-002	Refueling Water Storage Tank Flood Caused Reactor Coolant Pump Trip and Reactor Trip	Palo Verde 2	G.10-1

G.2 LER No. 245/94-015

Event Description: Testing Error Drains Reactor to Drywell Spray While Plant is Shut Down

Date of Event: April 10, 1994

Plant: Millstone 1

G.2.1 Summary

During testing on day 85 of a plant outage, the shutdown cooling (SDC) system was inadvertently aligned to the drywell spray system. Approximately 12,000 gal of reactor coolant inventory was sprayed into the drywell before operators identified and isolated the leakage pathway.

G.2.2 Event Description

On April 10, 1994, Millstone Unit 1 was in day 85 of an extended outage when testing was begun on the low-pressure coolant injection (LPCI) system logic. With the LPCI pump breakers racked out, LPCI valve 1-LP-10B, train B outboard containment isolation valve, was opened. The SDC system at Millstone, unlike many boiling water reactor (BWR) plants, shares some piping with the LPCI system but employs dedicated SDC pumps instead of relying on the LPCI pumps. SDC discharge is piped into the B train LPCI injection line, just downstream of the 10B valve. When the 10B valve was opened, the B LPCI train was pressurized by the SDC system. The A LPCI train was pressurized as well through the normally open cross-connect between the LPCI trains.

Subsequently, LPCI drywell spray valves 1-LP-15A and 1-LP-16A were opened. This directly aligned the SDC system to the A train LPCI drywell spr.y system. About 3 min later, a drywell sump hi–hi level alarm was received in the control room. At that time, operators observed that reactor vessel level had declined from about +85 in. on the "flood-up" (wide-range) level gauge to about 40 to 50 in. and was decreasing rapidly. Approximately 2 min later, operators closed the LPCI valves and terminated the transfer of reactor coolant to the drywell sprays. At that point, the reactor level was about +6 in. on the wide-range level gauge or about +20 in. on the narrow-range gauges. It was estimated that approximately 12,000 gal was lost from the reactor coolant system at 2200 gpm during the 5.5-min event.

Had reactor level dropped an additional 12 in., which would have occurred approximately 30 s later, the low-level Group III isolation would have been initiated. Among other things, the Group III isolation signal provides for isolation of all SDC motor-operated valves, which would have automatically terminated the event. If the blowdown path had not been successfully isolated and the level continued dropping, an emergency core cooling system start signal would have been provided to the inoperable LPCI pumps, as well as to the core spray (CS) system, which was operable but set in "pull-to-lock." The CS system is capable of providing 3600 gpm from each of its two pumps. Had reactor level dropped further, to about -118 in., core uncovery would have occurred. It was estimated that core uncovery would have occurred approximately 13 min from the start of the event.

G.2.3 Basis for Selection as An "Interesting" Event

Automatic isolation of the drain down should occur when the vessel level reaches 132 in. above the top of the active fuel. This would require the closure of one of the three motor-operated valves upon receipt of a Group III isolation signal. If the isolation did not occur, makeup via the CS pumps would be possible. The LPCI pumps were unavailable since their breakers were racked out. If neither of these actions is successful, the vessel will be drained to the top of the active fuel in about 10 min. The drain down will continue until the SDC pumps lose adequate suction head.

G.2.4 Factors of Interest

This event involved an intersystem LOCA at shutdown. This event is similar in nature to the Wolf Creek event described in Appendix D. However, due to the slower transfer rate and the lower decay heat rate in this event, this event is an "Interesting" event and not a precursor.

G.3 LER No. 269/94-004

Event Description: Past Unavailability of the Emergency Condensor Circulating Water and Low-Pressure Service Water Systems

Date of Event: July 26, 1994

Plant: Oconee 1

G.3.1 Summary

On July 13, 1994, during planning for valve maintenance that would take the elevated water storage tank (EWST) out of service, the system engineering group was asked to determine the applicable limiting conditions for operation (LCO). This determination found that the low-pressure service water (LPSW) system, a postaccident core cooling system, could be rendered inoperable. This inoperability would occur if the lake level was more than 2 ft below the full pond level and a loss-of-offsite power (LOOP) event occurred while the EWST was out of service. The emergency condenser circulating water (ECCW) system would not maintain siphon flow under these conditions. Subsequent investigations revealed that the LPSW system was also vulnerable on other occasions due to the Unit 1 main feeder bus (MFB) being out of service longer than 72 h.

G.3.2 Event Description

It was determined that sealing water supplied from the EWST to the condenser circulating water (CCW) was necessary to prevent loss of ECCW siphon flow when lake level is less than 798.13 ft (about 2 ft below full pond level) during a LOOP event.

The CCW system supplies the LPSW system through the CCW crossover header. The ECCW is part of the CCW and performs two separate functions. One of these is to recirculate CCW to the intake canal following the loss of Lake Keowee (dam failure). The second function is an unassisted siphon during LOOP. This siphon supplies suction for the LPSW system and provides cooling water flow though the condenser. The LPSW system provides cooling for components in the turbine building, the auxiliary building (AB), and the reactor building (RB). LPSW also cools engineering safeguards equipment in the AB and RB and is required by technical specifications for these functions.

An evaluation to support repair work revealed that a lake level of 798.13 ft or greater was sufficient to provide gravity flow for suction supply to the LPSW. However, if the lake level is less than 798.13 ft and the EWST is unavailable during a LOOP, the ECCW may not maintain siphon flow due to assumed air in leakage through the CCW pump seals, thus rendering the LPSW pumps inoperable.

The evaluation found that the EWST had been taken out of service during 1985 and 1990 while lake level was less than 798.13 ft. In 1985, between August and November, the EWST was removed from service to be painted, and lake level was 8 ft below full pond level. In 1990, at various times between July and September, the EWST was removed from service for valve maintenance. During these periods, the ECCW and LPSW had been technically inoperable.

The HPSW system provides a source of fire protection, bearing lubrication, sealing, and cooling water to various equipment for all three Oconee units. Its pumps are powered from the Unit 1 MFBs. In the event of a LOOP, the HPSW via the EWST automatically supplies cooling water to the turbine-driven emergency feedwater pump (TDEFW) and its oil cooler and maintains CCW pump seal water and pump cooling. If one of the Unit 1 MFBs is taken out of service for maintenance during an outage, then HPSW would be vulnerable to a single failure, rending the system inoperable. This potential effect on the CCW and LPSW for all three units had not been recognized, and the appropriate LCO had not been entered. The LPSW system was determined to have been inoperable in the past.

G.3.3 Basis for Selection as An "Interesting" Event

This event was not modeled as an accident sequence precursor. The principal difficulty in such an analysis would be the need to model the plant's 1985 and 1990 configurations. Also, the actual lengths of time for when the LPSW had been inoperable due to the potential loss of suction to the system's pumps from the removal of the EWST or one of the two Unit 1 MFBs are not readily available.

G.3.4 Factors of Interest

This event involves the potential inoperability of numerous safety-related systems for approximately 6 months.

G.4 LER No. 272/94-007

Event Description: Reactor Trip, Two Safety Injection Actuations, and Solid Pressurizer Operation

Date of Event: April 7, 1994

Plant: Salem 1

G.4.1 Summary

Salem 1 was reducing power in preparation for taking the main turbine off-line because of circulating water (CW) system problems caused by large quantities of river marsh grass and debris that were clogging the intake structure. Following an unexpected reactor trip, two safety injections were automatically initiated. The first, caused by a main steam pressure pulse, resulted in the pressurizer filling completely with water (solid condition) in a shorter than expected period of time. The second was caused by a rapid decrease in reactor system pressure when a secondary safety valve opened with the pressurizer solid. The pressurizer power-operated relief valves (PORVs) actuated over 300 times during the event and passed a significant quantity of water. Once safety injection was terminated, the operators reestablished a bubble in the pressurizer. The operators were unaware of a yellow path procedure to restore a pressurizer bubble and instead relied on support from Technical Support Center personnel outside of direct EOP guidance.

G.4.2 Event Description

Salem 1 was operating at reduced power on April 7, 1994, because seasonal river marsh grass and debris were severely affecting the CW intake structure. A load reduction was in progress to take the main turbine off-line following the clogging of several traveling screens and numerous CW pump trips. Reactor power was reduced to 7% by inserting control rods and by increasing the boron concentration in the reactor coolant system.

Initially, during the downpower maneuver, operators reduced turbine power ahead of reactor power, and the resulting power mismatch caused a slightly higher than normal reactor coolant system (RCS) temperature. At 1043 hours, the nuclear shift supervisor (NSS) directed the operator controlling reactor power to go to the electrical distribution panel and begin shifting plant loads to offsite power sources. At the time, the control room crew believed the plant was stable; however, they failed to recognize that reactor power was still decreasing due to the delayed effect of the boron that had been added. This led to a reversal of the power mismatch and a decreasing RCS temperature.

At 1045 hours, the NSS identified the resulting overcooling condition, went to the reactor control panel, and began withdrawing control rods to raise RCS temperature. Then he turned over rod control operation to the original operator. This operator continued to withdraw the control rods, and reactor power increased from approximately 7% to 25% of full power. Since the reactor had dropped below 10% power, the power range high-neutron flux low-setpoint trip had automatically reinstated, establishing a 25% power reactor trip setpoint. At 1047 hours, reactor power reached this level and the reactor tripped.

Almost immediately following the reactor trip, an automatic safety injection (SI) signal actuated. The SI occurred only on the train A logic and was caused by high steam flow coincident with low RCS temperature. The licensee later determined that the high-steam flow signal was the result of a short-duration pressure pulse created in the main steam lines by the closing of the turbine stop valves when the turbine tripped. Because of the short duration of the pressure pulse, only SI train A actuated, and a number of components had to be manually placed in their SI positions. This included some of the main steam isolation valves (MSIVs) and main feedwater isolation valves, which were closed from the control room. The main feedwater (MFW) pumps were also manually tripped. SI train A was reset with its automatic actuation in the "blocked" position. SI train B actuation logic remained armed.

Once the MSIVs were closed, the primary coolant system continued to heat up because of decay heat and the running reactor coolant pumps. This caused steam generator (SG) pressure to increase. Due to a design problem in the valve controllers for the main steam atmospheric relief valves, these valves did not automatically open to control SG pressure, nor did the secondary nuclear operator manually open the valves as required to prevent lifting the SG safety relief valves (the operator was occupied with the many manual valve repositionings required after the single-train SI actuation).

As a result of the primary heatup and the water added by the SI, the pressurizer filled to solid or near-solid conditions, and the PORVs periodically opened to control primary pressure. Shortly before 1126 hours, SG pressure increased to the safety valve lift setpoint in the No. 11 SG. The opening of two SG safety valves caused a primary system cooldown and, due to the solid water state of the primary system, primary system pressure rapidly decreased. At 1126 hours, primary pressure decreased to the SI setpoint of 1755 psig. Since train B of the SI logic remained armed, a second automatic SI was actuated by that train of logic. The operators had also identified the decreasing RCS pressure and manually initiated SI moments after the automatic actuation.

At 1149 hours, the pressurizer relief tank (PRT) rupture disk ruptured to relieve the increasing tank pressure that resulted from the volume of primary inventory discharged through the PORVs. The PORVs actuated over 300 times to relieve water to the PRT (PORV PR1 cycled 109 times and PORV PR2 cycled 202 times based on "valve not fully closed" indication). Following the event both PORVs were inspected. New stainless steel valve internals had been installed in 1993; these internals had no service life other than testing prior to the event. PORV PR2 exhibited galling of the stem where it passed through the bonnet and severe wear and scrapes along part of the plug and cage. PORV PR1 did not exhibit stem wear, although there was some wear to the plug and cage, and there was a possible cut in the valve seat. Both valves had an axial crack on both sides of the antirotation pin. Damaged parts were to be replaced prior to the unit's returning to power. There was no indication that any primary safety valve lifted during the event.

The operators were faced with the task of cooling down the plant from normal operating temperature and pressure without having a steam bubble in the pressurizer to accommodate pressure fluctuations. Once SI was terminated, operators controlled primary pressure through a combination of charging and letdown using the chemical and volume control system. Significant variations in RCS pressure in response to minor temperature changes were prevented by keeping the reactor coolant pumps (RCPs) running and by recovering a bubble in the pressurizer prior to initiating a plant cooldown (with the RCPs tripped, a one-degree change in temperature could have resulted in a 100 psi change in RCS pressure).

At 1316 hours, the licensee voluntarily declared an Alert to ensure the actuation of the Technical Support Center (TSC) to provide the operators with any technical assistance that might be required as they cooled down the plant. By 1410 hours, the TSC had been staffed, and at 1511 hours the operators restored a bubble in the pressurizer.

Guidance for reestablishing a steam space in the pressurizer for pressure control was available to the operators by use of the Critical Safety Function Coolant Inventory Status Tree yellow path "Response to High Pressurizer Level." However, this was not used. The operators were unaware of a yellow path to establish a pressurizer bubble. Instead, the operators continued through the Emergency Operating Procedure (EOP) for SI termination and, with technical support from the TSC, reestablished the steam space in the pressurizer outside of direct EOP guidance.

The Salem and Hope Creek service water systems were unaffected by the river debris that clogged the Salem CW intake structure.

Additional information concerning this event is provided in Augmented Inspection Team (AIT) Report 50-272-94-80 dated June 24, 1994 (Ref. 2).

G.4.3 Additional Event-Related Information

The Salem charging system includes three pumps: two centrifugal charging pumps and one positive displacement pump. The shutoff head of the centrifugal pumps is 2670 psig, well above the PORV setpoint of 2330 psig.

The AIT report for the event noted that the Salem Final Safety Analysis Report (FSAR) analyses include an allowance of 20 min to reset SI following inadvertent actuations. Westinghouse Electric Corporation (the Nuclear Steam Supply System vendor) analyses assume a shorter, 10-min operator response time. A June 30, 1993, letter from Westinghouse to the licensee noted that potentially nonconservative assumptions had been used in the licensing analysis of the Inadvertent Operation of the Emergency Core cooling System (ECCS) at Power accident, and that a water solid condition could occur in less than the 10-min operator action time assumed by Westinghouse to identify the event and terminate the source of fluid increasing the RCS inventory. Reference 2 concluded that the Westinghouse-assumed 10-min time period may need to be reexamined in light of this event. The Salem operators took about 17 min to terminate safety injection following the first SI and 12 min to terminate safety injection following the second SI. The pressurizer became water solid during the event, although the plant operators responded appropriately to the inadvertent SI actuations in accordance with approved EOPs.

G.4.4 Basis for Selection as An "Interesting" Event

The event was not modeled as an accident sequence precursor, primarily due to the difficulty associated with the development of a PRA model for plant response following a solid pressurizer condition. No existing analyses that address solid operation were identified, and the complete development of such a model is beyond the scope of the ASP program.

G.4.5 Factors of Interest

The event involves the occurrence of a solid pressurizer condition in a shorter than expected time period following a spurious SI. Although the Salem operators responded expeditiously to the SI in accordance with the EOPs, they could not prevent the pressurizer going solid.

The PORVs were repeatedly challenged once the pressurizer was solid, which increased the likelihood of their sticking open and resulting in a transient-induced LOCA (galling and unexpected wear were observed during the valve inspection following the event).

If the reactor coolant pumps had been secured by the operators, large fluctuations in RCS pressure could have occurred following minor temperature changes. This could have resulted in the formation of voids in unusual parts of the system, including the SG U-tubes, with a resulting loss of natural circulation.

The operators were faced with the difficult task of controlling the plant once the pressurizer was solid. They were unaware that a Critical Safety Function Coolant Inventory Status Tree yellow path, "Response to High Pressurizer Level," existed for Salem and did not use it to establish a pressurizer bubble. Instead, the operators continued through the EOP for SI termination and reestablished the pressurizer bubble outside of direct EOP guidance.

G.4.6 References

1. LER 272/94-007, Revision 1, "Reactor Trip from 25% Power/Two Safety Injections, Manually Initiated Mainstream Isolation, and Discretionary Declaration of Alert," May 10, 1994.
2. NRC Augmented Inspection Team (AIT) Report No. 50-272/94-80 and 50-311/94-80, June 24, 1994.

G.5 LER No. 275/94-020

Event Description: Dual Reactor Trip Due to Grid Disturbances

Date of Event: December 14, 1994

Plant: Diablo Canyon 1 & 2

G.5.1 Summary

On December 14, 1994, both Diablo Canyon units tripped due to a grid disturbance.

G.5.2 Event Description

At 1226 hours on December 14, 1994, both Diablo Canyon reactors tripped due to an undervoltage condition on the buses supplying the reactor coolant pumps (RCP). This undervoltage condition was due to a grid disturbance that started in Idaho and affected most western states and Canadian provinces. The reactor trip is anticipatory and designed to minimize the effects of the expected trip of the unit's RCPs. In this event, the voltage on the buses supplying power to the RCPs did not decrease enough to actually cause the RCPs to trip, and they continued to operate throughout the transient. Except for minor equipment anomalies, this was an uncomplicated trip.

G.5.3 Basis for Selection as An "Interesting" Event

This event is bounded by the normal trip since no significant equipment failures occurred.

G.5.4 Factors of Interest

The cause of the trip (large-scale grid disturbance) was unusual; however, the trip response was nominal.

G.6 LER No. 295/94-003

Event Description: No Containment Pressure Indication on Startup

Date of Event: March 23, 1994

Plant: Zion 1

G.6.1 Summary

On March 23, 1994, during the reactor startup following a 6-month refueling outage, containment pressure indications did not change during a containment vent. Investigation revealed that the sensing lines on all of the safety-related containment pressure transmitters were capped inside containment.

G.6.2 Event Description

During the reactor startup, the lack of containment pressure changes during containment venting resulted in verification of the valve lineups and draining of the vent lines. After these actions had no effect, further investigation discovered pipe caps on the instrument sensing lines on the inside of the containment penetrations. The pipe caps were found to have been installed four days before on March 19, 1994, while the plant was in cold shutdown, but the condition was discovered when the plant was in the startup mode. The pipe caps caused the containment pressure engineered safety features actuation logic, narrow- and wide-range indicators, and recorder to be inoperable during this period. The cause of the event was the lack of labeling on containment penetrations inside the containment. Additionally, the work to cap open containment penetration lines was deficient in planning and execution.

Although the ECCS high-containment pressure functions were not available, the remaining actuation systems and ECCS systems were available, and the core decay heat was minimal.

G.6.3 Basis for Selection as An "Interesting" Event

This event was not modeled as an accident sequence precursor due to the short time period during which the plant response to accidents would have been impacted and the availability of alternate actuation signals for safety injection.

G.6.4 Factors of Interest

This event is an example of a common-mode failure that resulted in the disabling of all the instrumentation for a safety-related process variable.

G.7 LER No. 298/94-010

Event Description: Difficulty Establishing Shutdown Cooling

Date of Event: May 26, 1994

Plant: Cooper Station

G.7.1 Summary

On May 26, 1994, while attempting to place the residual heat removal (RHR) system in the shutdown cooling (SDC) mode, the SDC isolation valves automatically closed three times on high-pressure signals. The cause was found to be leakage though the B RHR pump minimum flow valve to the suppression pool (torus).

G.7.2 Event Description

Prior to the first isolation occurring, heatup and flushing of the B RHR loop piping was in progress in preparation for placing the B loop in the SDC mode of operation. When the RHR SDC suction valves were opened, an isolation occurred with indications of a pressure perturbation, and reactor pressure vessel level dropped approximately 4.5 in. A walkdown of the accessible RHR piping revealed no damage to the RHR system. The cause of the pressure perturbation was assumed to be a steam void from the heated water (~250°F), which had been static for more than 2 h. This led the plant personnel to be aware of the potential for a second isolation and the assumed need to reset the isolation and reopen the valves as soon as possible if a second isolation did occur.

When the isolation logic was reset and the RHR SDC suction valves reopened, a second isolation did occur. Another pressure perturbation occurred, and the RPV level decreased 13.5 in. Nine minutes later, after resetting the isolation logic and reopening the valves, the same thing happened again with RPV level decreasing 16.5 in. The cognizant system engineer subsequently noted audible leakage through the B RHR pump minimum flow valve to the suppression pool. In an unrelated investigation, it had been noted that suppression pool level had been slowly increasing since around the time the flushing and heatup for the SDC mode had begun. The B RHR pump minimum flow valve was manually closed and declared inoperable. RHR SDC mode was subsequently placed in service.

The failure of the minimum flow valve to fully close was due to foreign material on one of the valve's torque switch contacts. Although the RHR suffered no damage from the water hammer induced by the steam voids created when the RHR lines refilled, the potential existed due to the failure of engineering and operations personnel to develop actions to eliminate the steam void and ensure that the piping was properly filled and pressurized.

G.7.3 Basis for Selection as An "Interesting" Event

This event was not modeled as an accident sequence precursor since limited equipment failures occurred and SDC was subsequently initiated.

G.7.4 Factors of Interest

This event is of interest due to the multiple, repeated, unnecessary challenges to plant systems while shut down with high-decay loads.

G.8 LER No. 324/94-008

Event Description: Plant-Centered Loss-of-Offsite Power

Date of Event: May 21, 1994

Plant: Brunswick, Unit 2

G.8.1 Summary

On May 21, 1994, with Brunswick Unit 2 in a refueling outage, the system dispatcher notified the Brunswick control room that maintenance had been completed on the Whiteville 230-kV line. Prior to returning the line to service, testing had to be conducted on the circuit breakers. Testing of the Whiteville breakers would involve opening three breakers in the Brunswick switchyard. At 1509 hours, the dispatcher opened the wrong breakers. This caused a loss-of-offsite power (LOOP) to Brunswick Unit 2, while Unit 1 remained powered from offsite sources. All four emergency diesel generators (EDGs) started, and loads automatically sequenced onto the buses for EDGs 3 and 4. With the exception of the reactor building ventilation system, all other engineered safety features responded as required. Offsite power was restored 2 min later at 1511 hours. By 1618 hours, the plant buses were realigned back to their normal supplies and the EDGs were shut down.

If this switchyard testing had been performed at power, the same results would have been obtained; Unit 2 would experience a LOOP. A similar event (LER 324/89-009) occurred at Brunswick Unit 2 in 1989 with the plant at 76% power. On June 17, 1989, troubleshooting activities related to a startup auxiliary transformer (SAT) ground caused the SAT to trip. Due to the loss of power to the recirculation pumps, the plant was manually tripped. This resulted in a LOOP event at Brunswick Unit 2. Corrective actions for the 1989 event did not indicate that maintenance and troubleshooting of the SAT would be restricted to when the Brunswick units were shut down. Therefore, it was concluded that this event could also occur at power.

G.8.2 Event Description

Brunswick Unit 2 was in a refueling outage on May 21, 1994. The system dispatcher notified the Brunswick control room that maintenance had been completed on the Whiteville 230-kV line. He also informed them that testing would be required on the circuit breakers prior to restoring them to service. The Unit 2 SAT was being supplied from switchyard bus 2B. Testing of the Whiteville breakers would involve opening one breaker on switchyard bus 2B (breaker 28B) and two breakers on switchyard bus 2A (breakers 27A and 30A). At 1509 hours, the dispatcher opened breaker 28B as required. Then, instead of opening breakers 27A and 30A, he opened breakers 27B and 30B. This resulted in a LOOP to Unit 2. All four Brunswick EDGs started, and loads automatically sequenced onto the buses for EDGs 3 and 4. The reactor protection system motor generators A and B tripped. The spent fuel pool cooling pumps and supplemental spent fuel pool cooling pumps tripped. The 2A nuclear service water pump automatically started. The reactor building ventilation system isolated, and the standby gas treatment (SBGT) system automatically started. The reactor building ventilation system inboard dampers did not automatically isolate due to a relay failure in the SBGT control relay logic.

Brunswick notified the dispatcher that there had been an automatic start of the EDGs. The dispatcher realized that he had opened the B circuit breakers instead of the A circuit breakers. At 1511 hours, the B circuit breakers were closed, and power was restored to the SAT. By 1618 hours, the plant buses were realigned back to their normal supplies, and the EDGs were shut down. By 1828 hours, switching operations were completed, and the 230-kV buses were in their normal configuration.

G.8.3 Additional Event-Related Information

There are 4 EDGs at Brunswick. EDGs 1 and 2 normally provide emergency power for Unit 1, and EDGs 3 and 4 normally provide emergency power for Unit 2. However, the emergency buses from each unit can be cross-tied. Thus, emergency power for Unit 2 could be supplied from the Unit 1 buses via offsite power sources or EDGs 1 and 2.

Each of the four emergency buses is designed to power one residual heat removal (RHR) pump for each unit, and the five service water pumps are powered such that at least one is available from the opposite unit's emergency buses. Thus, the unit that loses offsite power has RHR capability that is powered from a separate switchyard and is not dependent on the postulated loss of the unit's emergency buses.

During power operations the SAT feeds the reactor recirculating pumps, and the unit auxiliary transformer (UAT) feeds all other plant loads. The UAT is supplied by the main generator. Therefore, any loss of power to the SAT would cause the recirculation pumps to trip. This, in turn, would require the operators to manually trip the reactor. Once the reactor is tripped, the main generator would trip and the UAT would be lost. This would result in a plant LOOP.

G.8.4 Basis for Selection as An "Interesting" Event

A similar event (LER 324/89-009) occurred at Brunswick Unit 2 in 1989. On June 17, 1989, with the plant at 76% power, troubleshooting activities related to an SAT ground caused the SAT to trip. Due to the loss of power to the recirculation pumps, the plant was manually tripped. This resulted in a LOOP event at Brunswick Unit 2. Corrective actions for the 1989 event did not indicate that maintenance and troubleshooting of the SAT would be restricted to when the Brunswick Units were shut down. The ASP analysis of LER 324/89-009 is documented in *Precursors to Potential Severe Core Damage Accidents: 1989 A Status Report*, NUREG/CR-4674, Vol. 12.

Any loss of power to the plant from the SAT would cause the recirculation pumps to trip. This, in turn, would require the operators to trip the reactor. Once the reactor is tripped, the main generator would trip, and the UAT would be lost. This would result in a plant LOOP.

G.9 LER No. 366/94-003

Event Description: Loss of Shutdown Cooling

Date of Event: March 17, 1994

Plant: Hatch 2

G.9.1 Summary

On March 17, 1994, 34 h after the start of a refueling outage, the operating loop of shutdown cooling (SDC) for Hatch Unit 2 was isolated by a control circuit fault. Approximately 1 h and 20 min elapsed before the standby loop was placed in service. The reactor coolant temperature rose from 168°F at the start of the event to saturation temperature when localized boiling occurred. Reactor pressure peaked at 9 psig despite an open half-inch vent line. A similar event occurred at Peach Bottom Unit 2 and is briefly described in the event description .

G.9.2 Event Description

Hatch 2 was in cold shutdown with decay heat removal provided by SDC loop B on March 17, 1994, at 1131 hours, 34 h after shutdown for a refueling outage. An engineer was tracing the route of a wiring bundle and inadvertently caused an exposed bare wire strand to contact the metal wire raceway. The subsequent circuit ground caused the spurious activation of certain primary containment isolation system (PCIS) functions. This included the closure of the SDC loop B discharge valve, which terminated SDC.

Reactor coolant system (RCS) temperature was approximately 168°F when SDC was lost. Due to a failure of a process computer low-flow alarm, it took 9 min (1140 hours) for the operators to recognize that SDC loop B was not providing any flow through the core. When operators attempted to reopen the SDC loop B discharge valve, it opened and immediately closed due to the locked-in, spurious PCIS signal. Operators then shut down the operating residual heat removal (RHR) pump and began trying to diagnose the problem with the assistance of the engineer who introduced the fault.

The operators entered the "Loss of Shutdown Cooling" procedure and raised reactor water level from 37 to 57 in. to promote natural circulation. Temperature was monitored at the inlet to the reactor water cleanup (RWCU) system. It remained steady over the first 30 min of the event. This was probably due to the effect of adding cold makeup water to raise the reactor water level and the effect of monitoring temperature within the RWCU system, which takes a suction from the bottom of the reactor vessel. If temperature approaches 212°F, the procedure directs that an alternate cooling path be established. Pressure was also used as an indication of the rising core temperature. However, the pressure indication used was a 0- to 1200-psig gauge marked in 20-psig increments. This was inadequate to observe a small pressure increase. RHR loop A was available for SDC, but this was not pursued while the temperature apparently remained stable. Instead, efforts were concentrated on discovering the reason for the spurious PCIS signal.

Thirty minutes after the initiation of the PCIS signal (1202 hours), temperature at the inlet to the RWCU system began to rise. This prompted operators to begin to line-up RHR loop A for SDC. Some delay was encountered while a temporary procedure change was processed to allow the operators to waive the normal system flush before placing loop A in service. RWCU inlet temperature rose to 185°F, and reactor pressure rose to 9 psig before SDC loop A was placed in service, 80 min after the spurious PCIS signal interrupted flow from SDC loop B. RWCU inlet temperature ultimately rose to 195°F before it began to decrease. Throughout the event, a half-inch reactor vessel vent line was open. However, this did not provide enough cross-sectional area to prevent the reactor vessel from pressurizing. Analysis by the nuclear steam supply system vendor indicated that the bulk temperature remained less than 212°F; however, localized boiling did occur.

By 1325 hours, a blown fuse in the PCIS initiation circuitry had been found and replaced. Subsequently, the PCIS signal was reset, and the SDC loop B discharge valve was cycled to ensure its operability. Therefore, SDC loop B was restored to standby status at 1325 hours, 1.75 h after the discovery that no SDC flow existed (1140 hours).

A similar event occurred at Peach Bottom 2, near the end of a refueling outage. The B reactor recirculation pump (RRP) was secured to limit the heat input. This placed the plant in a natural circulation mode with the reactor head vent open. Operators planned to test run the A RRP while flushing SDC loop B. However, the operators were unsuccessful in starting the A RRP. Reactor head flange temperature and RWCU inlet temperature were to be monitored every 15 min. The operator observed the RWCU inlet temperature decrease steadily and failed to recognize the increasing reactor head flange temperature until reactor pressure increased 1 psig. Flange temperature had reached 230°F, and bulk temperature was 205°F when SDC loop B was restarted 4 h after initially securing the B RRP.

G.9.3 Factors of Interest

Both these events are interesting due to the time required before beginning to restore SDC. In the Hatch event, high decay heat loads existed just 34 h after shutdown; however, operators waited to see an indication of increasing temperatures before commencing efforts to restore a SDC loop. This time delay was further increased while processing a procedure change. In the Peach Bottom event, operators watched the incorrect temperature indication for several hours and chose not to question continually decreasing temperatures even though they were knowledgeable of decay heat generation in the core.

Both events are also interesting due to the inadequate instrumentation monitored during the events. In both events, RWCU system temperatures were monitored when other indications were available. In the Hatch event, a pressure instrument calibrated in 20-psig increments was monitored when a much smaller pressure change was expected. Pressure indication at a much finer resolution was available via the plant computer.

G.10 LER No. 529/94-002

Event Description:	Refueling Water Storage Tank Flood Caused Reactor Coolant Pump Trip and Reactor Trip
Date of Event:	May 28, 1994
Plant:	Palo Verde 2

G.10.1 Summary

On May 28, 1994, water from the refueling water storage tank (RWST) had gravity-drained through a containment spray (CS) isolation valve after maintenance was performed on the wrong logic train. The water sprayed into containment via the auxiliary CS nozzles. This resulted in a reactor coolant pump (RCP) trip when water from the CS system entered an RCP termination box and caused a short circuit. This caused the reactor to trip.

G.10.2 Event Description

Maintenance troubleshooting and replacement of a relay in the A train engineered safety features actuation system (ESFAS) was authorized. The relay of interest controlled the CS isolation valve. The A train relay cabinet was deenergized in preparation for work by the maintenance technicians, but the technicians incorrectly worked on the B train relay cabinet. When the incorrect relay was removed, the B train CS isolation valve opened as designed, without actuating any control room alarms. The opening of this valve created a flow path that allowed borated water to gravity-drain from the RWST into containment through the auxiliary CS nozzles.

Some of the borated water entered an RCP penetration termination box that contained the 1B RCP 13.8-kV power leads. The water caused a short circuit, which tripped the 1B RCP. The RCP trip caused a reactor trip on low departure from nucleate boiling ratio (DNBR), which is the expected plant response. The plant response to the reactor trip was nominal.

Approximately 7000 gal of borated water drained from the RWST over a 2-h period. This represents about a 1% level change in the RWST level, which is not noticeable on the RWST level instrumentation. High containment sump levels and increasing containment humidity caused by the leakage were being investigated by the plant staff. After verifying that the source of water was not from the primary coolant system, a containment entry to identify the source of the leakage was in progress when the reactor trip occurred. The CS isolation valve was closed after the flow path through the CS nozzles was visually identified.

Components within the area affected by the borated water from the auxiliary CS nozzles were inspected and repaired as necessary.

G.10.3 Basis for Selection as An "Interesting" Event

This event was not modeled as an accident sequence precursor since the response to the reactor trip was uncomplicated.

G.10.4 Factors of Interest

The initiation of the reactor trip due to activation of the CS system caused by maintenance activities is unusual.

Appendix H:

Resolution of Comments on the Preliminary 1994 ASP Analyses

H.1 Introduction

This appendix contains the comments received from the applicable licensees and the Nuclear Regulatory Commission (NRC) staff for each of the potential precursors. The comments for each potential precursor are listed and discussed in docket number order, where the docket number refers to the plant that reported the problem. Comments are further separated into licensee and NRC comments. Only comments considered pertinent to the accident sequence precursor analysis are addressed. Due to the length of the comments received, they are paraphrased in this appendix. Comments simply pointing out grammatical or spelling errors were addressed in the revision of the analyses but are not listed or addressed in this appendix. The reanalysis of the potential precursors resulted in the elimination of some events from the final set of precursors contained in Appendices C and D of this report. These events are noted in Table H.1.

Table H.1. List of comments on preliminary ASP analyses

Event No.	Plant	Event description	Page
LERs 213/94-004, -005, -007, -013; IR 213/94-03	Haddam Neck	Power-Operated Relief Valves and Vital 480-V ac Bus Degraded	H.2-1
LER 237/94-018	Dresden 2	Motor Control Center Trips Due to Improper Breaker Settings	H.3-1
LER 237/94-021	Dresden 2	Long-Term Unavailability of High Pressure Coolant Injection	H.4-1
LER 245/94-015*	Millstone 1	Testing Error Drains Reactor to Drywell Spray While Plant is Shut Down	H.5-1
LER 250/94-005	Turkey Point 3 and 4	Load Sequencers Periodically Inoperable	H.6-1
LER 266/94-002	Point Beach 1	Both Diesel Generators Inoperable	H.7-1
LER 272/94-007*	Salem 1	Reactor Trip, Two Safety Injection Actuations, and Solid Pressurizer Operation	H.8-1
LER 304/94-002	Zion 2	Unavailability of Turbine-Driven Auxiliary Feedwater Pump and Emergency Diesel Generator	H.9-1
LER 318/94-001	Calvert Cliffs 2	Trip, Loss of 13.8-kV Bus, and Short-Term Saltwater Cooling System Unavailability	H.10-1
LER 324/94-008*	Brunswick 2	Plant-Centered Loss of Offsite Power	H.11-1
LER 366/94-003*	Hatch 2	Loss of Shutdown Cooling	H.12-1
LER 458/94-023	River Bend	Scram, Main Turbine-Generator Fails to Trip, Reactor Core Cooling Isolation Cooling, and Control Rod Drive System Unavailable	H.13-1
IR 482/94-18	Wolf Creek	Reactor Coolant System Blows Down to Refueling Water Storage Tank During Hot Shutdown	H.14-1
LER 498/94-012*	South Texas 1	Emergency Diesel Generator 11 and Turbine-Driven Auxiliary Feedwater Pump 14 Simultaneously Inoperable	H.15-1
IRs 499/94-13, -16*	South Texas 2	Emergency Diesel Generator 22 Long-Term Unavailability	H.16-1

*This event eliminated from set of final precursors.

H.2 LER Nos. 213/94-004, -005, -007, -013, Inspection Report 213/94-03

Event Description: Power-Operated Relief Valves and Vital 480-V ac Bus Degraded

Date of Event: February 16 and 19, 1994

Plant: Haddam Neck

H.2.1 Licensee Comments

Reference: Letter from J. F. Opeka, Northeast Utilities Service Co., to U.S. NRC, dated July 19, 1995, NUSC letter B15299

Comment 1: The ASP models fail to properly credit the use of the "A" charging pump for mitigating the effect of reactor coolant pump (RCP) seal induced loss-of-coolant accident (LOCA), given motor control center 5 (MCC-5) failure.

Response 1: Use of the charging system is credited in the ASP analysis. In the event of a loss-of-offsite power (LOOP) and loss of MCC-5, the charging pumps will trip. Because MCC-5 powers the instrument air system, instrument air will not be available to control charging and seal injection flows unless MCC-5 is recovered. Current Haddam Neck procedures direct operators to simultaneously attempt recovery of MCC-5 and to reestablish charging flow.

In the event labeled "MCC-5 Recovered Before Seal LOCA," the ASP model considers the likelihood that MCC-5 will be recovered or that charging will be independently restored prior to occurrence of seal LOCA. This is discussed in Section C.2.4.3 of the analysis. A single operator nonrecovery probability is believed to be appropriate for the combined activities because they are competing actions undertaken at approximately the same time and success of either is assumed to prevent seal failure.

Given that a seal LOCA occurs, a source of high-pressure injection (HPI) is assumed to be required to prevent core damage. The failure probabilities used for the HPI function in seal LOCA sequences for this event reflect dominant operator nonrecovery probability values, while equipment failure contributions are neglected. The ASP HPI and high-pressure recirculation (HPR) system models do consider the charging pumps as redundant sources of HPI.

The wording of the modeling assumptions section has been revised to clarify this point.

Comment 2: The last sentence of the fourth paragraph of Event Description section (of the preliminary analysis), which indicates that "The PORV air-operator diaphragms are believed to have been damaged during the 1993 refueling outage." should be revised. The damage to the valves consisted of improperly installed diaphragms. This caused no physically or functionally observable degradation at first. The degradation took place over a period of time. It is impossible to determine exactly when that degradation progressed to this point of inoperability, but it is reasonable to assume that it occurred well after the start of the cycle. In addition, the problem affecting the power-operated relief valves (PORVs) had a significant impact only on their ability to operate long term as for feed and bleed. For a short-term operation, such as relieving an overpressure condition, they would have functioned properly.

Response 2: The sentence has been revised to say, "As a result of their incorrect installation, the PORV air-operator diaphragms were damaged and subject to leakage at an unknown time after they were replaced during the 1993 refueling outage." However, the analysis still assumes that the valves were failed for feed-and-bleed from the end of the refueling outage until the problem was discovered. The installation errors caused the eventual degradation of the valves until the point where they were no longer functional for feed-and-bleed. The point at which the valves were no longer operable cannot be determined. It was conservatively assumed that the valves were inoperable since the end of the refueling outage.

The air-operator diaphragm damage and attendant air leakage were assumed not to affect PORV availability for overpressure relief.

Comment 3: The second sentence of the sixth paragraph of the Event Description section (of the preliminary analysis) reads as follows: "containment spray, reactor coolant (RC) system loop isolation, at least one PORV block valve." It is recommended that the words "at least" be deleted since only one PORV block valve was at that time powered by MCC-5 and the words "at least" imply more.

Response 3: The words "at least" were deleted.

Comment 4: In the first paragraph of the Modeling Assumptions section (of the preliminary analysis), second line, CYAPCO suggests deleting the word "must." The ability to cycle the valves four times is an arbitrary design requirement.

Response 4: The word "must" was deleted.

Comment 5: It appears from the loss-of-offsite power event tree and the data tables that the SRVs were assumed to open with probability 1.0 given a LOOP and the PORVs unavailable. This is quite conservative. It then appears that a conditional probability of sticking open (given a challenge) of 3×10^{-2} per valve is used. Supplemental information provided by the licensee notes that based on best-estimate transient analyses, the pressurizer PORV set point would not be challenged on a LOOP event with auxiliary feedwater available. Therefore, the conditional probability of ever challenging the PORV/SRV given a LOOP is not 1.0 but some small fraction thereof. This factor does not appear in the ASP modeling. If so, LOOP sequence 8, case 2-2, accounting for some 19% of the CDP (in the preliminary analysis), would decrease somewhat. If 3×10^{-2} represents the combined probability of SRV challenge and sticking open, then the modeling is correct. But PPR-SRV-00-PRV1 in Table 12 should be clarified.

Response 5: The ASP models currently assume the probability of PORV lift given LOOP is 1.0 for this plant class. This value is acknowledged to be conservative and will be revised on a plant-class basis in a later model revision. While some PRAs have assumed a lift rate of 1.0, others have used values in the range of 0.1. The potential impact of the use of a reduced PORV challenge rate following LOOP was explored during the resolution of these comments and was determined to have a minor impact on analysis results; (it does not affect the dominant sequences) therefore, the value used in the preliminary analysis was retained. Note that while the PORV lift rate may be conservative, the combined lift and failure to reseat probability, which is the probability of a transient-induced LOCA, is realistic based on the next-to-the-last sentence in the summarized licensee comments.

Event PPR-SRV-00-PR1 does represent the probability that the PORV/SRV fails to reseat, given that it was challenged.

Comment 6: As noted under general comments above, the ASP model does not credit the use of the "A" charging pump (powered by "B" electrical division equipment) to mitigate the consequences of a small LOCA, including an RCP seal induced LOCA. Best estimate LOCA analyses confirm the adequacy of one charging pump to mitigate small breaks of up to about 0.02 ft^2. The LOCA analysis supports the conclusion that one centrifugal charging pump can mitigate a RCP seal failure-induced LOCA.

Given failure of MCC-5 and induced RCP seal LOCA, it is possible to restart the charging pump and mitigate the consequences of the seal-LOCA after confirming adequate electrical power.

Response 6: As described above, the ASP model for the event does credit recovery of charging and seal injection as a means of preventing seal LOCA. Given that a seal LOCA occurs, recovery of a source of HPI is assumed to be required to prevent core damage. The failure probabilities used for the HPI function in seal LOCA sequences for this event reflect dominant operator nonrecovery probability values, and equipment failure contributions are neglected. The ASP HPI and HPR system models do consider the charging pumps as a redundant source of HPI.

Comment 7: Missing from Table 3 are transients and high-energy line breaks (feedline and steamline) where significant credit is taken for feed and bleed. The impact can only be quantified using a detailed model such as the IPE. Hence, the 1.4×10^{-4} value in the preliminary ASP is reasonably correct, although about one-half the sequences are not accurate. These models should be corrected if for no other reason than future use of the IRRAS may result in incorrect analysis.

Response 7: The ASP models consider complicated trips and LOFWs, LOOPs, small LOCAs, and SGTRs. Plant-specific initiating events such as high-energy line breaks, in which the location of potentially impacted components can play an important role, cannot be considered unless detailed special interaction information is provided by the licensee in the LER. Such analyses are usually beyond the scope of the analysis effort.

Comment 8: Finally, the value of 0.2 for MFW-SYS-TRIP, main feedwater (MFW) system trips, is a reasonable number if it is used as a modifier of the transient initiating frequency. The MFW recovery value of 0.34 would not, in general, be appropriate for a plant design such as the Haddam Neck plant where the MFW pumps are motor-driven, and very reliable, are not tripped on safety injection or high containment pressure, and are easily restarted. All transients are lumped together as a single initiator, this modeling approximation is adequate.

Response 8: The value 0.2 for MFW-SYS-TRIP reflects the probability that the feedwater system is unavailable, given that an initiator has occurred.

The ASP models assume average probabilities for MFW recovery, given that feedwater is postulated to be lost. Values that reflect event specifics are utilized in cases where an actual LOFW is observed.

H.2.2 NRC Comments

None.

H.3 LER No. 237/94-018

Event Description: Motor Control Center Trips Due to Improper Breaker Settings

Date of Event: June 8, 1994

Plant: Dresden 2

H.3.1 Licensee Comments

Reference: Memo from P. D. O'Reilly, U.S. NRC, to file, September 8, 1995.

Comment 1: The Additional Event-Related Information section is limited to a discussion of ac and dc power sources and does not discuss the isolation condenser (IC) or its operation during a loss-of-offsite power (LOOP). Information concerning the IC was provided by the licensee.

Response 1: The Additional Event-Related Information section was revised to describe the IC and its makeup water source.

Comment 2: The modeling of the LOOP sequences in the preliminary analysis is overly conservative because the analysis does not credit the IC system for extended station blackout (SBO) events (events in which offsite power is not recovered prior to battery depletion). Although the response tree given in the preliminary analysis appears to include an IC node, it follows the HPCI node. The tree appears to be incorrectly based on an implicit assumption that the IC would be used only if offsite power were recovered but HPCI failed.

Enhancements to procedure DGA-13, "Loss of 125 VDC Battery Chargeıs with Simultaneous Loss of Auxiliary Electric Power," effective August 17, 1993, detail operator actions to prevent isolation of the IC due to battery depletion. After that date the Dresden IPE credits operator action to maintain the IC available following battery depletion, which significantly reduces the importance of extended SBO sequences. Therefore, the model used in the preliminary ASP analysis should not be applied to conditions after August 17, 1993.

Response 2: It is acknowledged that the current ASP model incorrectly addresses the potential use of the IC for long-term core cooling following HPCI success. This does not impact the analysis of this event and will be corrected the next time the models are revised. The current model also does not address the potential for a recirculation pump seal LOCA following a station blackout. This will be addressed during further model development.

All ASP models assume core damage will occur if offsite power is not recovered by the time the batteries deplete. At that time all instrumentation would be lost, as would control power for breaker, turbine-driven pump, and dc valve operation. Components and instrumentation would change state and cease functioning when component-specific voltages are reached during the gradual loss of dc power (these voltages are usually more conservative than manufacturers' specifications and are often temperature dependent); the plant state would be unpredictable. Potential recovery after this time, although possible, is extremely difficult to address and is beyond the scope of the analysis.

Comment 3: The condition involving the trip setting for the MCC 28-3 breaker began in March 1993, as discussed in the LER. Since changes to procedure DGA-13 became effective August 17, 1993 (see comment 2), a more realistic duration for the event would be approximately 5.5 months.

Response 3: See the response to comment 2. Since the ASP models assume core damage occurs once the batteries deplete, the duration utilized in the preliminary analysis is considered appropriate.

Comment 4: The preliminary ASP analysis estimated a probability of 0.21 of failing to recover offsite power prior to battery depletion after 4 h. This estimate appears to be based on data in NUREG-1032 and an assumption that the station has a single switchyard. The estimate in the preliminary analysis is overly conservative, however, because Dresden has two switchyards. The Dresden IPE also uses a 6-h mission time instead of the 4-h battery depletion time used in the preliminary ASP analysis. The probability of failing to recover offsite power at 6 h is estimated to be 0.0205 in the Dresden IPE (information concerning the approach used to estimate the nonrecovery probability was provided by the licensee).

Response 4: The likelihood of failing to recover offsite power in the ASP models is estimated using data from NUREG-1032. The plant-centered, grid, and severe-weather groups and their recovery groups are the same as those used in the Dresden IPE. The ASP model assumes an extreme severe-weather group SS3, however, which is considered reasonable for Dresden's location. The ASP analyses distinguish the different types of LOOPs (plant-centered, grid-related, etc.) and estimate LOOP frequencies and nonrecovery probabilities for each type in terms of Weibull distributions developed from data in Appendix A of NUREG-1032 for each type of LOOP instead of from cluster data. This allows different types of LOOPs observed in the operating experience to be specifically addressed. The ASP LOOP models estimate a LOOP nonrecovery probability at 4 h for an "average" LOOP at Dresden (which considers all four LOOP types by weighting the four Weibull nonrecovery distributions based on the frequency of each type of LOOP) to be 0.0238, very close to and slightly smaller than the 0.0296 estimated at 4 h by the licensee based on cluster data. As described in the response to comment 2, the ASP models assume core damage will occur if offsite power is not recovered at the time the batteries deplete following a station blackout. Since the batteries will deplete in 4 h at Dresden, that value is appropriate for the analysis. It is acknowledged that if the recirculation pump seals remain intact, the IC may extend the time of core damage to beyond the battery depletion time. However, such considerations are beyond the scope of the current analysis.

Analysis Case 2b, the only case that significantly contributes to the results, considers dual-unit LOOPs (primarily grid- and weather-related LOOPs). For these LOOPs, the probability of failing to recover offsite power at 4 h is higher than for nominal (cluster data) LOOPs, since more easily recovered plant-centered LOOPs are excluded. However, the frequency of dual-unit LOOPs is also smaller because of the exclusion of the relatively higher frequency plant-centered LOOPs.

The LOOP nonrecovery probabilities used in the preliminary analysis are considered appropriate and have been retained.

H.3.2 NRC Comments

None.

H.4 LER No. 237/94-021

Event Description: Long-Term Unavailability of High Pressure Coolant Injection

Date of Event: August 4, 1994

Plant: Dresden Unit 2

H.4.1 Licensee Comments

Reference: Letter from Thomas P. Joyce, Commonwealth Edison Co. (ComEd), to the U.S. NRC, dated July 5, 1995, TPJLTR 95-0077

Comment 1: The preliminary NRC analysis assumed that the event made Unit 2 high pressure coolant injection (HPCI) unavailable for one month (i.e., 720 h). In fact, the Unit 2 HPCI operated at 2500 rpm for 5 min immediately prior to the subsequent failure. This should be considered a valid test. ComEd believes that the actual Unit 2 HPCI unavailability was probably 107 h. This 107-h period represents the time from the failure occurrence on August 4, 1994, until Unit 2 was shut down, when HPCI was no longer required.

Response 1: The Licensee Event Report (LER) indicated that HPCI turbine exhaust stop check valve 2-2301-74 was disassembled and inspected. The inspection revealed that the four tack welds had failed recently due to fatigue. The fatigue failure was suspected to have occurred during the most recent 5-min turbine run for the manual trip test portion of the monthly surveillance. During this period, the failure of the tack welds allowed the steam flow through the valve to rapidly start rotating the disk from the valve stem. This motion essentially elongates the valve stem, forcing it into a closed position, which then resulted in a high turbine exhaust pressure. It appears fortuitous that the manual shutdown occurred prior to the valve elongation, causing a high-pressure trip. The check valve would have likely worked itself closed if the manual trip test had lasted another minute or two, and the turbine would have tripped on high exhaust pressure at that point. Therefore, it was assumed that the HPCI turbine would have failed within minutes of being demanded if it had been required to perform its safety function subsequent to the last monthly surveillance. This period was assumed to be 720 h (30 d) prior to the observed failure. Because power operation continued for another 107 h, a more appropriate failure period of 827 h was used in the analysis.

Comment 2: The preliminary NRC analysis appears to be based on a generic boiling water reactor (BWR) probabilistic risk assessment (PRA) model. Use of a generic model is conservative for some accident scenarios and nonconservative for others. Idaho National Engineering Laboratory (INEL) has developed a Dresden model for use with the SAPHIRE code that is based on the Dresden IPE. This model should be used because it more accurately reflects Dresden plant response, especially concerning loss-of-offsite power (LOOP) sequences.

Response 2: The Dresden model used in the analysis is based on previous work by ORNL and was converted into a SAPHIRE-based model by INEL. This model was developed specifically for the ASP Program. It is intended to be similar to and consistent with the other plant models used by the ASP Program. The Dresden model referred to by the licensee was based on the Dresden IPE and converted into a SAPHIRE-based model by INEL. Due to the variety of methodologies and level of detail in the licensee-developed plant-specific IPEs and the limited review that the IPEs have received to date by the NRC, these models are not appropriate for use in the ASP Program. Plant-specific IPE insights may be incorporated into the ASP models following completion of the NRC IPE reviews.

Comment 3: The preliminary NRC analysis defines an "Importance" value for the event as the resulting increase in core damage probability. The "Importance" calculated in the preliminary NRC analysis is 2.1×10^{-6}. If the NRC analysis had used 107 h, the calculated event "Importance" would have been 3.1×10^{-7}. Results from the current ComEd PRA model for Dresden 2 gives an "Importance" of 7.0×10^{-7} for this event if 107 h of HPCI unavailability is used. The ComEd PRA model includes many more accident sequences and initiating events than were included in the preliminary NRC analysis.

Response 3: As explained in response 1, it appears more appropriate to use a failure period of 827 h. This yields an "Importance" of 2.6×10^{-6} from the NRC analysis. Utilizing the formula provided in the Dresden response and Dresden IPE values with an 827-h HPCI turbine unavailability period, the "Importance" is calculated at 5.4×10^{-6}.

H.4.2 NRC Comments

None.

H.5 LER No. 245/94-015

H.5.1 Licensee Comments

None.

H.5.2 NRC Comments

None.

H.6 LER No. 250/94-005

Event Description: Load Sequencers Periodically Inoperable

Date of Event: November 3, 1994

Plant: Turkey Point 3 and 4

H.6.1 Licensee Comments

Reference: Letter from T. F. Plunkett, Florida Power and Light, to the U.S. NRC, L-95-197, dated July 18, 1995, and supplemental information faxed on August 29, 1995, from Florida Power and Light to the U.S. NRC.

Comment 1: Because of the unique design of the high-head safety injection (HHSI) system at Turkey Point (four pumps shared by two units), a failure of two sequencers in an accident unit does not directly cause a loss of automatic HHSI capability; two sequencers on the other unit will provide automatic actuation capability. The HHSI pumps, along with the accumulators, will extend the time available for the operators to take recovery actions during a large-break loss-of-coolant accident (LOCA).

Response 1: The large-break LOCA model used in the analysis of this event, like the Turkey Point Individual Plant Examination (IPE), utilizes an early core heat removal success criterion of 1 of 2 residual heat removal (RHR) pumps (plus accumulators). The potential use of the HHSI pumps to support early core cooling for large-break LOCA is not addressed. Although HHSI pump success may delay core uncovery, no thermal-hydraulic analyses exist to support this proposition or to provide information on operator response timing.

Comment 2: By reviewing the information provided in NUREG/CR-4550 (7 to 10 min to recover from core uncovery) and the results from simulator drills for LOCA scenarios in which HHSI and low-head safety injection were successfully initiated by the operators within the first 2 min, Florida Power and Light (FPL) calculated an operator error probability of 0.06 for failing to manually initiate safety injection (SI) following a large-break LOCA (in later, faxed, information, an operator failure probability of 0.03 was estimated).

Response 2: The ASP models define the undesired end state "core damage" to occur following core uncovery. It is acknowledged that clad and fuel damage will occur at later times, depending on the criteria used to define "damage." The potential for recovery following core uncovery is not addressed in the models.

The times referred to in the comment by Florida Power and Light are provided in Appendix D.4 of the Surry PRA. Times to core uncovery (following a large-break LOCA) of 7.1 and 9.4 min are listed, based on data included in *Radionuclide Release Under Specific LWR Accident Conditions*, BMI-2104, July 1984. The BMI-2104 calculations assumed all safeguards are unavailable. The 7.1 min time is based on a 4-volume analysis and is presumably a better estimate than the 9.4 min developed using a 2-volume analysis.

The calculations were done using MARCH for the purpose of estimating accident source terms; the results of the thermal-hydraulic calculations used to estimate the time to core uncovery have large uncertainty. However, since no later large-break LOCA analyses were identified during resolution of this comment, the core uncovery time of 7.1 min included in BMI-2104 was used in this analysis. (It should be noted that Appendix D.4 also includes Figures D.4-1 and D.4-2, which provide curves of the time to core uncovery as a function of break size developed from a variety of timing estimates.

Based on these curves, the 7.1-min time to core uncovery corresponds to approximately a 6-in. break, the low end of large-break LOCA sizes. LOCAs of this size are more likely than larger ones.)

The table on p.13 of the LER provides the results of three simulator scenarios involving design basis accidents with failed sequencers. For the scenario applicable to this comment, a large-break LOCA, the response time for full safeguards actuation ranged from 1.5 to 3.25 min, with an average time of about 2 min. At least some of the simulator runs were completed after the problem with the sequencers was identified at Turkey Point, which may skew the results low. It is also likely that the simulator exercises did not represent the operator burden that would be expected following a large-break LOCA.

An estimate of the probability of the operators failing to manually recover SI was developed based on the simulator data provided in the LER, the 7.1 min available before core uncovery, as listed in BMI-2104, and lognormal time-reliability correlation as described in *Human Reliability Analysis* (E. M. Dougherty and J. R. Fragola, John Wiley and Sons, New York, 1988). The simulator data provided in the LER was assumed to represent unburdened response; its standard deviation was revised to reflect burdened response as described on p. 127. An operator failure probability of 0.095 is estimated using this approach.

The NUREG/CR-4550 PWR probabilistic risk assessments (PRAs) were also reviewed to determine what recovery credit was provided in those analyses. Documentation for the Zion and Sequoyah PRAs discuss manual initiation of LPI following a large-break LOCA. In those PRAs, a probability of 0.1 was used for failure to manually initiate ECCS pumps following sequencer failure. That value is consistent with the operator failure probability estimated here.

Comment 3: The ASP analysis used initiating event frequencies of 1.0×10^{-3} and 5.0×10^{-4} for a medium- and large-break LOCA, respectively. The Turkey Point IPE used the values 1.0×10^{-4} and 1.0×10^{-5} for these two frequencies. FPL believes the plant-specific IPE values should be used in the analysis (in later, faxed information FPL stated 1.0×10^{-4} was considered more appropriate than 5.0×10^{-4}).

Response 3: The frequencies for medium- and large-break LOCAs used in the Turkey Point IPE are significantly lower than the values used in almost all other IPEs, particularly for large-break LOCAs. For example, the following is a listing of medium- and large-break LOCA frequencies from five other IPEs:

Plant	Medium-break LOCA frequency	Large-break LOCA frequency
Diablo Canyon	4.6×10^{-4}	2.0×10^{-4}
Oconee	7.0×10^{-4}	7.0×10^{-4}
Salem	1.0×10^{-3}	5.0×10^{-4}
Sequoyah	2.6×10^{-4}	2.0×10^{-4}
St. Lucie	Not provided	2.7×10^{-4}

The above values are typical of the frequencies used for medium- and large-break LOCAs in IPEs and PRAs.

The frequencies for a medium-break LOCA are typically in the 10^{-4} range, instead of 1.0×10^{-3}, as used in the analysis. However, since the results for a medium-break LOCA do not dominate the overall results, the medium-break LOCA frequency was not revised. The initiating event frequency for a large-break LOCA was revised, however, to 2.7×10^{-4}, the same value as used in the St. Lucie IPE. This reflects a survey of 13 IPEs, in which the estimated frequency of a large-break LOCA ranged from 1.0×10^{-4} to 7.0×10^{-4}, with most values in the $2–5 \times 10^{-4}$ range. (The mean estimate 2.7×10^{-4} is equivalent to a median estimate of 1.0×10^{-4} with an error factor of 10 as used in the Reactor Safety Study.)

Comment 4: The small-break LOCA analysis assumes that the plant is at power for 70% of a year. This factor was not included in the medium- and large-break LOCA analyses.

Response 4: The factor 0.70 is used to estimate the number of at-power hours in a year when converting initiating event frequencies from a yearly to an hourly basis. Initiating events used to estimate an initiating event frequency are assumed to occur at power. Since this event was analyzed for a 1-yr duration (6132 at-power hours), the net effect is the same as using the yearly frequency.

Comment 5: The sequencers start the diesel generators for LOCA, LOOP, and LOOP plus LOCA events. Because of this, "if required because of a LOOP" should be deleted from the second paragraph of the Event Description.

Response 5: The Event Description section has been revised to reflect this.

Comment 6: While the sequencers were vulnerable to failure from the time one of the affected test steps started until the start of the next step (a period of 1 h), the actual test step took approximately 10 s to complete. The wording in the second and fifth paragraphs of the Event Description, which currently describes each test step as requiring 1 h to complete, should be revised to reflect this.

Response 6: The Event Description has been revised to clarify the time required to complete each test step.

Comment 7: The calculation for the increase in core damage probability for medium- and large-break LOCAs should be clarified (proposed example calculations were provided).

Response 7: The calculational approach for medium- and large-break LOCAs has been clarified as suggested.

H.6.2 NRC Comments

None.

H.7 LER No. 266/94-002

Event Description: Both Diesel Generators Inoperable

Date of Event: February 8, 1994

Plant: Point Beach 1 and 2

H.7.1 Licensee Comments

Reference: Letter from Bob Link, Wisconsin Electric Power Company, to U.S. NRC, dated April 10, 1995, WEPCO Letter NRC-95-021

Comment 1: The preliminary analysis assumed a 1-h battery lifetime. Nonsafety batteries installed in 1993 reduced safety-related battery loading by half, increasing battery lifetime to 2 h.

Response 1: The analysis has been revised to consider a 2-h battery lifetime.

Comment 2: The preliminary ASP analysis conservatively assumes that for every occurrence of a loss-of-offsite power (LOOP) the pressurizer power-operated relief valves (PORVs) will open. Because of the reduced primary pressure at Point Beach, PORV lift following LOOP is considered unlikely. Point Beach thermal-hydraulic analyses and experience with one LOOP supports this. The lift probability during LOOP should be set conservatively at 0.05.

Response 2: The ASP models currently assume that the probability for PORV lift following LOOP is 1.0 for this plant class. This value is acknowledged to be conservative and will be revised on a plant-class basis in a later model revision. While some PRAs have assumed a lift rate of 1.0, others have used values in the range of 0.1. The potential impact of the use of a reduced PORV challenge rate following LOOP was explored during resolution of these comments and was determined to have a minor impact on analysis results (it does not affect the dominant sequences); therefore, the value used in the preliminary analysis was retained.

Comment 3: The preliminary ASP analysis assumes that the probability of failure of the auxiliary feedwater (AFW) turbine-driven pump is 1.5×10^{-1}. This is given under primary name AFW-TDP-FC-1A, "AFW turbine-driven pump fails." Recommend the probability of item AFW-TDP-FC-1A be set to 6.0×10^{-2}.

Response 3: The probability of turbine-driven AFW pump failure has been reevaluated. The value currently used in the ASP model is 3.3×10^{-2}.

Comment 4: The preliminary ASP analysis assumes the probability of failure of the operator to recover AFW during station blackout is 3.4×10^{-1}. As stated in the Point Beach Nuclear Plant (PBNP) Individual Plant Examination (IPE) submittal, the probability that an operator will fail to control steam generator flow with minimum steam generator level indication is 2.4×10^{-1}. Recommend the probability of item AFW-XHE-NOREC-EP be set to 2.4×10^{-1}.

Response 4: Basic event AFW-XHE-NOREC-EP addresses the probability that an initially failed AFW turbine-driven pump train will not be recovered in the short term, not the probability that the operators will fail to control AFW flow with minimum SG levels. The nonrecovery probability recognizes that some turbine-driven AFW pump failures are recoverable even following a station blackout. The value used is consistent with those used in other analyses. Since there is no operating experience pertaining to station blackouts, this value was developed based on recovery from turbine-driven pump failures following reactor trips.

H.7.2 NRC Comments

None.

H.8 LER No. 272/94-007

Event Description: Reactor Trip, Two Safety Injection Actuations, and Solid Pressurizer Operation

Date of Event: April 7, 1994

Plant: Salem 1

H.8.1 Licensee Comments

Reference: Letter from J. J. Hagan, Public Service Electric and Gas Company, to U.S. NRC, dated April 21, 1995.

Comment 1: The probability used in the analysis for failure to realign the AFW pump suction source to an alternate source upon CST depletion is cverly conservative. A plant-specific value for this action has been calculated to be 8.3×10^{-4}. The plant-specific value is considered appropriate since multiple alarms and procedural actions would have to fail in order for the alignment not to occur.

Response 1: Following completion of the preliminary analysis, this event was deleted from the set of precursors and included instead as an "interesting" event. Difficulties associated with the development of a risk model within the scope of the ASP program that could address potential plant response following the solid pressurizer condition observed during the event prevented a reasonable estimate of the significance cf the event.

H.8.2 NRC Comments

None.

H.9 LER No. 304/94-002

Event Description: Unavailability of Turbine-Driven Auxiliary Feedwater Pump and Emergency Diesel Generator

Date of Event: March 7, 1994

Plant: Zion Unit 2

H.9.1 Licensee Comments

Reference: Letter from T. W. Simpkin, Commonwealth Edison Company, to the U.S. NRC, dated May 19, 1995.

Comment 1: The description of the auxiliary feedwater system states that each motor-driven pump supplies two steam generators. Each of the two motor-driven pumps is capable of and normally aligned to supply water to all four steam generators individually.

Response 1: The description of the auxiliary feedwater systems was revised to state that the two motor-driven pumps supply all four steam generators.

Comment 2: The statement that the common diesel generator will align to only one unit at a time is inaccurate. This is true only in the event that a safety injection signal is present on either of the units. Absent a safety injection signal, the common diesel generator is capable of supplying power to the associated electrical bus of each unit simultaneously.

Response 2: The description was revised to state that if a safety injection signal is present, the common diesel generator will align to the unit with the safety injection signal. If a safety injection signal is absent, the common diesel generator is capable of supplying power to the associated electrical bus of each unit simultaneously.

Comment 3: Given the discovery of zebra mussels, it was assumed that the common-cause diesel generator failure should be set 25 times higher than normal. The LER makes it clear that the heat exchangers for the other two diesel generators had essentially zero zebra mussel buildup. In other words, there was no common-cause failure involved here. The common-cause terms should have been left at their normal values. Removing the common-cause increase in the Commonwealth Edison model yields only a small change in risk.

Response 3: The emergency power system is treated as a three-train system because of the common diesel. The nominal common-cause basic event for a three-train system is Q × β × γ. If the other trains were also exposed to the same failure mechanism that caused the failure of one train (i.e. the zebra mussels), then the common-cause basic event becomes β × γ or (0.27 × 0.1). This value is approximately 25 times greater than the original value. The common-cause failure probability used in the preliminary analysis has been retained. However, the reason for changing the common-cause failure probability was clarified.

Comment 4: It was assumed that the turbine-driven auxiliary feedwater pump was inoperable during the entire 15-day period of the diesel generator inoperability. Inspection and repeated subsequent testing of the pump revealed no identifiable cause for the overspeed trip. Since the failure was not repeatable and no cause could be found, one must conclude that it was some kind of random event, rather than an indicator of a defective pump. The pump was not broken; it just failed for unknown reasons on that particular start. Given a demand, the probability of the pump working would be much higher than the probability of it failing. Therefore, the assumption that the turbine-driven auxiliary feedwater pump was inoperable for 15 days is not justified.

Response 4: The turbine-driven auxiliary feedwater pump tripped on overspeed. Since this operation of the pump was the first demand since tne last surveillance of the pump, it was assumed that the pump would have tripped if the pump had been demanded during the period in which the emergency diesel generator was also unavailable. While it is not clear, either in the LER or in the comments provided by the licensee, that the pump operated normally on its next demand (the licensee states that no cause or problem could be found), it was assumed that operators could have readily reset the pump and subsequently started the pump. Therefore, the pump was modeled as unavailable with a nonrecovery probability of 0.04. This nonrecovery probability reflects the assumption that the pump is easily recoverable from the control room, that the recovery is routine, and that procedures existed at the time of the event to recover the pump.

H.9.2 NRC Comments

Reference: Memo from S. S. Lee, U.S. NRC, to P. D. O'Reilly, U.S. NRC, dated May 5, 1995.

Comment 1: Since the zebra mussel shells did not affect the other emergency diesel generators, why was the common-cause factored into the analysis? Secondly, even if there was a common-cause effect by the mussels, why was an increase factor of 25 chosen?

Response 1: An explanation was provided as part of the response to licensee comment 3.

Comment 2: Why were some of the base case values modified?

Response 2: The values were modified to reflect revised probabilities for certain basic events identified after the original model was developed. These changes do not reflect the circumstances of the event. Since these were corrections to the model and not modifications to reflect the circumstances of the event, they are not described in the event analysis.

H.10 LER No. 318/94-001

Event Description: Trip, Loss of 13.8-kV Bus, and Short-Term Saltwater Cooling System Unavailable

Date of Event: January 12, 1994

Plant: Calvert Cliffs 2

H.10.1 Licensee Comments

Reference: Letter from R. E. Denton, Baltimore Gas and Electric Company, to U.S. NRC, dated June 5, 1995

Comment 1: Additional information was provided concerning saltwater pump configurations and their power supplies. Alternate acronyms were proposed for the saltwater and service water systems.

Response 1: The Additional Event-Related Information section has been revised to include information on the configuration of the saltwater pumps and their power supplies. Acronyms have been consistently used throughout the analysis.

Comment 2: The conditional probabilities for sequences 1 and 6 (Case 2) could be reduced by considering, in addition to the recovery of bus 14, the recovery of saltwater (SW) header 12 by starting SW pump 13. This pump can be powered from bus 11 or 14.

Response 2: The analysis has been revised to consider the potential use of SW pump 13 powered from bus 11. Consideration of SW pump 13 impacts sequence 1, which addresses component failures, but not sequence 6, which concerns operator actions related to the restoration of SW cooling. Failure of such operator actions is estimated using a time-reliability correlation (TRC) model, which in this case would also address the use of SW pump 13 within the set of response actions.

Comment 3: Component cooling water (CCW) would still be circulating even if SW cooling flow was lost. This circulation would remove heat from the reactor coolant pump (RCP) and high-pressure safety injection (HPSI) pump seals until an equilibrium temperature is reached. This circulation is expected to reduce the heatup rate for these components and allow additional time for recovery.

Response 3: While circulating CCW may delay seal heatup and extend the time available for recovery, its impact cannot be practically estimated. The impact of continued CCW flow is one of the many issues contributing to the uncertainty in the RCP seal failure model (see the response to comment 4).

Comment 4: Calvert Cliffs RCP seals include four stages, each capable of holding full primary pressure. The failure probability estimated for the four seal stages is 3.7×10^{-4} for a loss of CCW (1.5×10^{-3} for all four RCPs). This value was developed in "Reactor Coolant Pump Seal Failure Probability Given a Loss of Seal Cooling," Combustion Engineering Owners Group (CEOG) Task 742, November 1992.

Response 4: The likelihood of RCP seal failure given a loss of CCW at Combustion Engineering (CE) plants has been the subject of considerable discussion both within the NRC and between the NRC and the CEOG, and at the present time the issue is unresolved. Individual Plant Examinations (IPEs) for CE plants typically utilize an RCP seal failure probability consistent with the referenced CEOG task report. The CEOG developed an estimate of the RCP seal failure probability by estimating the probability of stage failure based on historic data and then applying generic Multiple Greek Letter (MGL) values to estimate the probability that the remaining stages would fail. The IPE for Arkansas Nuclear One, Unit 2 (section 3.7.4), however, acknowledges that differing opinions on the likelihood of RCP seal failure exist and provides an alternate analysis with an assumed failure probability of 0.2 for the fourth seal stage.

Information on RCP seal design, operating experience, and related issues was provided by the CEOG in a meeting with the NRC on May 17, 1994 (memorandum from S. K. Shaukat to C. Z. Serpan, *CEOG/NRC Meeting on GI-23, "RCP Seal Failure,"* dated August 15, 1994).

The list of historic losses of RCP seal cooling and related tests presented by the CEOG was modified to reflect certain Brookhaven National Laboratory (BNL) comments and then used to develop a crude RCP seal failure model for this analysis. In particular, seven tests were deleted from the CEOG list, the number of pumps subjected to loss of RCP cooling was revised for two events, and in the December 19, 1984 loss of RCP cooling at St. Lucie 2, one stage was considered failed on each of two pumps. Since many questions remain unresolved and no process equivalent to that used to develop the Westinghouse RCP seal failure model during the NUREG-1150 effort was performed, large uncertainties exist in the model that was developed.

No seal failures occurred following any of the losses of RCP seal cooling. The observation of no seal failures in 24 losses of seal cooling of greater than 60 min was used to estimate a pre-pump failure probability of 0.0208. Consistent with the NUREG-1150 model for Westinghouse seals, the seals were assumed to be vulnerable to seal failure if cooling was lost for more than 60 min, and any seal failure that was going to occur was assumed to have occurred by 90 min. This approach results in a cumulative seal failure probability for a four-pump plant like Calvert Cliffs of

$$F_{SL}(t) = \begin{cases} 0 & t \le 60 \\ 2.78 \propto 10^{-3}(t-60) & 60 < t \le 90 \\ 8.33 \times 10^{-2} & t > 90 \end{cases}$$

Although the stage failures that occurred on two stopped pumps at 30 min at St. Lucie may imply the 60-min minimum time to failure is optimistic, an assumption that additional time would exist before seal failure following a stage failure is considered reasonable.

The above distribution, which has a lower long-term RCP seal failure probability than the distribution assumed in the preliminary analysis, was used in the revised analysis of LER 318/94-001.

It should be noted that if the CEOG model is revised to include the additional St. Lucie stage failures and eliminate several tests that were nonrepresentative, a four-pump seal failure probability of 2.9×10^{-3} is estimated. Applying this value to the loss of CCW modeling approach described in the Calvert Cliffs IPE results in a similar core damage probability as estimated in the revised analysis.

H.10.2 NRC Comments

None.

H.11 LER No. 324/94-008

Event Description: Plant-Centered Loss-of-Offsite Power

Date of Event: May 21, 1994

Plant: Brunswick, Unit 2

H.11.1 Licensee Comments

Reference: Letter from R. P. Lopriore, Carolina Power & Light Company, to U.S. NRC, dated June 21, 1995.

Comment 1: The "Additional Event-Related Information" section does not include a discussion of the capability of the emergency bus configuration that provides for uninterrupted availability of one service water pump and two residual heat removal pumps on the unit experiencing the loss of offsite power (LOOP). Accident sequences 49 and 71 do not account for the availability of low pressure coolant injection (LPCI) and containment heat removal.

Response 1: A discussion of the emergency bus configuration was added to the appropriate section. The ability to cross-tie the emergency buses to the other unit before battery depletion results in a conditional core damage probability less than 1.0×10^{-6}. Thus, this event is no longer considered a precursor. Consideration of LPCI and containment heat removal in sequences 49 and 71 does not result in a significant change in the conditional core damage probability. Although this event was removed from the set of 1994 precursor events, it was included in Appendix G as an "Interesting" event, since it is similar to a precursor event from 1989.

Comment 2: The analysis includes all plant-centered LOOPs and their recovery times. This event is a subset of all plant-centered LOOPs and should be treated as such.

Response 2: The ASP Program has utilized the division of LOOPs that was developed in NUREG-1032. This consists of four categories: plant-centered, grid related, severe-weather related, and extreme severe-weather related. Division of the events into these four categories ensures that a proven and consistent methodology is utilized for these events.

H.11.2 NRC Comments

None.

H.12 LER No. 366/94-003

Event Description: Loss of Shutdown Cooling

Date of Event: March 17, 1994

Plant: Hatch 2

H.12.1 Licensee Comments

Reference: Letter from J. T. Beckham, Jr., Geoigia Power Company, to the U.S. NRC, dated July 21, 1995, HL-4889

Comment 1: Core damage would not occur as a result of a loss of shutdown cooling unless additional equipment failures occurred. Specifically, a mode change to hot standby conditions would not immediately cause core damage. All safety equipment, except steam-driven equipment [high pressure core spray (HPCS) and reactor core isolation cooling (RCIC)], was still available 34 h into the outage. Failure of suppression pool cooling would not result in core damage within 24 h. Several other methods for transferring heat from the suppression pool exist, which could have easily been attempted in that period. The shutdown model for this event, therefore, is not as extensive as it should be to accurately predict conditional core damage probability.

Response 1: Further consideration was given to the shutdown model concerning the plant response to a reactor pressure vessel heatup. With the head still in place and failing to reinitiate shutdown cooling (SDC), there appear to be two alternative paths to prevent core damage. First, the operator could open a safety relief valve (SRV) to rapidly remove energy and prevent vessel pressurization. This would require a means to dissipate the core heat and provide for a makeup source of water to the core area. Water could be injected via the residual heat removal (RHR), control rod drive (CRD), or low pressure core spray (LPCS) systems, which were all available at the time of the event. This was previously considered the only acceptable alternative to restarting SDC that would not lead to core damage. However, if vessel pressurization occurred and the SRV was not opened, additional mitigation strategies would still be available. Since only 34 h had passed since initiating the outage, all electrically powered safety equipment was readily available. A portion of the transient model, exclusive of steam-driven equipment, was incorporated into the loss of shutdown cooling (LSDC) model to more accurately reflect the possible recovery strategies. This allowed consideration of additional mitigation strategies including the use of automatic depressurization system (ADS), RHR, and containment cooling. The resulting conditional core damage probability resulting from the revised analysis is below the ASP Program cutoff for events identified as precursors (1×10^{-6}). The LSDC described in LER 366/94-003 has been removed from the set of 1994 accident sequence precursors. However, the event has been included in the report in Appendix G as an interesting event due to the difficulties experienced during the loss of shutdown cooling.

H.12.2 NRC Comments

None.

H.13 LER No. 458/94-023

Event Description: Scram, Main Turbine-Generator Fails to Trip, Reactor Core Isolation Cooling and Control Rod Drive Systems Unavailable

Date of Event: September 8, 1994

Plant: River Bend

H.13.1 Licensee Comments

Reference: Letter from James J. Fisicaro, Director Nuclear Safety, to U. S. NRC, dated June 9, 1995

Comment 1: Operations personnel could have recovered the feedwater system (FWS) if necessary to mitigate the event. This system failed due to the slow transfer of plant electrical loads to offsite power sources. All FWS pumps and valves were operable.

Response 1: The following time line is excerpted from the NRC's Augmented Inspection Team (AIT) report related to this event.

Time (h)	Time after trip	Event
0825	0 min	Reactor trip.
0845	+20 min	The control room supervisor asked the at-the-controls operator about the availability of the condensate and feedwater systems. They determined that the system needed to be vented prior to restarting the condensate pumps.
0905	+40 min	The nuclear equipment operators began locally venting the condensate system.
0938	+73 min	Nuclear equipment operators reported that valve MOV-CV0112 would not open to provide fill to the condensate system.
0948	+83 min	Nuclear equipment operators manually opened valve MOV-CV0112 and began filling and venting the condensate system.
1009	+104 min	Shift superintendent declared a notification of unusual event because only one source of high pressure water to the reactor was available, the event had the possibility to degrade, and additional support was needed to help return the condensate and feedwater systems to service.
1121	+176 min	Operators started feedwater pump 1A.
1217	+232 min	After verifying that the feedwater system was maintaining reactor vessel level, the operators secured the HPCS system.

A step in the feedwater system (FWS) abnormal procedure required the venting of the system under these circumstances regardless of whether system indications indicated the need for system venting. The emergency procedure for the FWS does not require the system to be vented. However, it is unclear when the emergency procedure would be used as opposed to the abnormal procedure used during this event. It is also unclear whether the system actually needed to be vented to ensure its operability under the conditions observed during this event. A high priority was placed on the restoration of the FWS, as its unavailability was, in part, the basis for declaring a Notification of Unusual Event.

A sensitivity calculation was performed to determine the impact of assuming the condensate and main feedwater systems were unrecoverable. If the nominal nonrecovery values are used, the conditional core damage probability for the event decreases by a factor of 2.2 to 8.0×10^{-6}.

Comment 2: Both trains of the control rod drive (CRD) system must be manually started for adequate initial reactor cooling. CRD is recoverable in this event. The operators could have manually opened the CRD flow control valves or changed the control valve control circuit fuses (which blew because of the slow transfer) in time to use CRD as an injection source in this event. Therefore, CRD should be modeled as available, with appropriate recovery factors.

Response 2: The following time line is excerpted from the NRC's Augmented Inspection Team (AIT) report related to this event.

Time (h)	Time after trip	Event
0825	0 min	Reactor trip.
1009	+104 min	Shift superintendent declared a notification of unusual event because only one source of high-pressure water to the reactor was available, the event had the possibility to degrade, and additional support was needed to help return the condensate and feedwater systems to service.
1100	+155 min	Operators identified that the CRD hydraulic system parameters were not reading correctly. The only available indication was pump current.
1155	+210 min	Operators replaced the blown fuse in CRD hydraulic system circuitry and returned the system to service.

From this, it would appear that the operators did not notice that the system was not functioning properly for over 2.5 h. Once the incorrect readings were noted, it took an additional 55 min to restore the system to operability. The operators were concerned with high-pressure injection systems as noted by the basis for the declaration of the notification of unusual event. It would seem unlikely that the CRD system could have been restored faster based on the number of tasks that needed to be accomplished (systems that needed to be restored) and the need for additional manpower. Therefore, modeling the system as inoperable and nonrecoverable in the time period required to maintain core cooling is appropriate.

Comment 3: Do the unavailability numbers for high-pressure core spray (HPCS), residual heat removal (RHR), automatic depressurization system (ADS), etc. include terms for maintenance unavailability? If so, the analysis should reflect that these systems were available and not out of service due to maintenance activities.

Response 3: Test and maintenance unavailabilities are not included in the values provided for the HPCS, RHR, and ADS systems. These systems were available during the event. As noted in Appendix A of this report, systems that were observed to fail during the event are modeled as failed (set to true). The failure probabilities for components that were observed to perform properly, or were not challenged during the event, were set to their nominal failure rates. Therefore, the probabilities used in the analysis for HPCS, RHR, and ADS reflect the nominal failure rates of the components.

Comment 4: For transient sequence 7, please note that RBS does not have an RHR containment spray subsystem. RBS [River Bend Station] has containment unit coolers that are independent of RHR, but dependent on normal/standby service water system. This is a plant-specific difference between RBS and the generic BWR/6 model.

Response 4: There are three 100% capacity containment cooler units, each consisting of a fan and associated air to water heat exchanger. Normally two of the units are running with cooling water supplied by the chilled water system. Under accident conditions, cooling water is supplied by the standby service water (SSW) system. There are three chiller pumps and four SSW pumps. The interaction between the SSW system and the chilled water system could not be determined from the information provided in the FSAR. The modeling of this system has little effect on the overall results for the event. Therefore, the containment spray subsystem was eliminated from the modeling. In effect, this models the containment unit coolers as components that are 100% reliable. This is somewhat nonconservative, but this simplification has little effect on the conditional core damage probability for this event.

Comment 5: RBS performed an analysis of core damage probability associated with this event. The analysis was performed using the RBS plant-specific PSA. Assumptions included (1) a transient initiator with loss of normal feedwater/condensate, loss of instrument air, and closure of the main steam isolation valves (MSIVs); (2) reactor core isolation cooling failed due to overspeed; (3) no loss-of-offsite power, no loss of reactor primary containment cooling water system (CCP), etc.; (4) emergency core cooling systems (ECCS) were not removed from service due to maintenance activities; (5) recovery from slow transfer is approximately equal to recovery of the power conversion system (PCS) modeled in NUREG/CR-4550, page 8–46; and (6) standby service water train A flow was sufficient to supply the necessary plant loads since adequate flow was available and operators were able to quickly open SSW pump A discharge valve. This assumption is supported by the use of RHR A for suppression pool cooling.

RBS re-quantified the appropriate transient sequences and added appropriate recovery factors. Based on the quantification, the probability of core damage given the above scram is 1.21×10^{-5} compared to the 6.0×10^{-5} value presented in the NRC letter.

Response 5: The ASP Program modeled the event in essentially the same manner as the licensee with the exception of the recovery values. The differences in these values are discussed in the response to comments 1, 2, and 3 above. The results obtained were similar to those obtained by the licensee. If the ASP models are modified to allow for recovery of the FWS and CRD systems, the conditional core damage probability is 2.2×10^{-5}. This is in good agreement with the value obtained by the licensee (1.2×10^{-5}).

H.13.2 NRC Comments

None.

H.14 Inspection Report 482/94-18

Event Description: Reactor Coolant System Blows Down to Refueling Water Storage Tank During Hot Shutdown

Date of Event: September 17, 1994

Plant: Wolf Creek

H.14.1 Licensee Comments

Reference: Letter from N. S. "Buzz" Carns, Wolf Creek Nuclear Operating Corp. (WCNOC), to U.S. NRC, dated July 26, 1995, WM-0118.

Comment 1: Two references in the preliminary analysis could be construed to imply that the operators did not initiate action to close valve EJHV-8716A until 66 s into the event. The 66 s included the time for diagnosis of the event, operator action to close the valve, and time for the valve to cycle from full open to full closed.

Response 1: The references have been clarified.

Comment 2: The first sentence in the Summary section should read, "the drain down event was initiated approximately 28 h following shutdown" instead of 24 h.

Response 2: The sentence has been clarified.

Comment 3: The Westinghouse analysis, using actual event conditions, indicates that core uncovery could have occurred in approximately 30 min (not the 25 min discussed throughout the preliminary analysis). The 25-min time used throughout the preliminary analysis should be changed to 30 min.

Response 3: This has been changed.

Comment 4: Sections 1 and 4 of the preliminary analysis both state that the conditional core damage probability (CCDP) for the event is 3.0×10^{-3}. This CCDP is about an order of magnitude greater than the preliminary CCDP estimated by WCNOC in the Incident Investigation Team (IIT) report for this event. In consideration for the difference between the two CCDP values, and due to the concerns recently identified by the NRC with the human reliability analysis methodology utilized by WCNOC in performing the individual plant examination, WCNOC requested NUS Corporation to perform an evaluation of the event using their human interactions methodology. NUS calculated the conditional core damage probability to be 3.5×10^{-4}. The assumptions and methodology used in the determination of the 3.5×10^{-4} conditional core damage probability value are documented in the NUS report, "Human Interactions Evaluation," dated July 1995, which is enclosed for your review.

Response 4: As discussed in the preliminary analysis, substantial uncertainties exist with respect to human reliability and other issues relevant to this event. However, a reanalysis of the event incorporating the SHARP method employed in the NUS analysis and other corrections suggested by Wolf Creek resulted in a conditional core damage probability estimate of 2.5×10^{-3}, as described in detail following the response to comment 5. This value is consistent with the conditional probability estimated in the ASP analysis.

Comment 5: The first sentence of Section 4, paragraph 5, states that after the RCS loops void at 5 min, RCS pressure would rapidly drop. However, the Westinghouse analysis of the draindown event (identified above) indicates that the RCS pressure would drop to saturation conditions within 30 to 60 s, after which the RCS pressure would slowly increase due to the absence of decay heat removal capability.

Response 5: Concerning the Westinghouse computer simulations, the referenced report says (p. 9, paragraph 2) [W]ithout operator recovery actions the vessel began to void within 2 to 3 min after event initiation and the RHR pump was predicted to fail about 30 s after the vessel began to void.

This was clarified in the analysis. It should be noted that the reduction in the assumed blowdown time interval from 5 min to 3 min impacts the conditional core damage probability estimated by the NUS application of the SHARP methodology.

Further Response to Comments 3–5:

To estimate the combined effects of comments 3–5, a calculation was performed utilizing the SHARP approach, assuming that 3 min was available for action ISO-S and 27 min for action ISO-L (see response to comment 5). Details of the SHARP-based methodology employed in the analysis can be found in the NUS report.

The SHARP method requires estimation of a cognitive/procedural error probability, P1. This involves identifying that a blowdown is occurring, identifying the blowdown source, and isolating the necessary valve. P1 is estimated based on the potential for misdiagnosis, clarity of procedures, plant interface difficulties, and lack of training, adequacy of time for correction of cognitive slips, and intuitiveness of required actions.

During the event, there were multiple clear indications that RCS inventory was being lost, including alarm annunciation and low-level indications on pressurizer level instrumentation. However, procedures did not permit a timely diagnosis of the event. The specifics of the event were not previously stressed in training. With available time for isolation of the blowdown path limited to 3 min instead of 5 min used in the NUS analysis, the time for correction of a cognitive slip was very short. Isolation of the blowdown was assumed to be an intuitively reasonable action.

Given that at least two of the variables determining P1 were negative (scenario not rehearsed in training and little time for correction of slips, as well as possible procedural weakness), P1 is defined to be greater than 10^{-4} and not more than 10^{-2}. In this analysis, P1 is assumed to be 10^{-3}, based on the two negative factors relevant at 3 min (the use of two negative factors is considered at most slightly conservative considering the possible procedural weakness; the assumption of one negative factor in the NUS analysis is considered optimistic).

The crew nonresponse probabilities, $P2_{3\ \mathrm{min}}$ and $P2_{27\ \mathrm{min}}$, can be calculated by the methods described in the NUS report:

$$P2_{3\ \mathrm{min}} = 1 - \Phi[\ln((150)/60)/0.6] = 0.063\ ;$$

$$P2_{27\ \mathrm{min}} = 1 - \Phi\ [\ln((1590/300)/0.8] = 0.019\ .$$

The manipulative error probabilities, P3, were retained from the NUS analysis:

$$P3_{3\ \mathrm{min}} = 3.0 \times 10^{-3}\ ;$$

$$P3_{27\ \mathrm{min}} = 1.5 \times 10^{-3}\ .$$

The human error probabilities for ISOL-S and ISOL-L can then be calculated:

$$\text{ISOL-S} = 1 \times 10^{-3} + 6.3 \times 10^{-2} + 3.0 \times 10^{-3} = 6.7 \times 10^{-2} ;$$

$$\text{ISOL-L} = 1 \times 10^{-3} + 1.9 \times 10^{-2} + 1.5 \times 10^{-3} = 2.2 \times 10^{-2} .$$

The NUS analysis developed the following algebraic equation describing the conditional core damage probability, summing sequences 3 and 4 from the event tree shown in Figure A.1-5 of the preliminary ASP analysis:

$$\text{CCDP} = [\text{ISO-S} \times (1 - \text{ISO-L}) \times \text{REFLUX}] + [\text{ISO-S} \times \text{ISO-L}] .$$

Observing that the P1 (cognitive) probability for event ISO-L is dependent between both human error events, the NUS analysis modified the equation:

$$\text{CCDP} = [(\text{ISO-S} - \text{P1}) \times (1 - (\text{ISO-L} - \text{P1})) \times \text{REFLUX}] + [(\text{ISO-S} - \text{P1}) \times (\text{ISO-L} - \text{P1})] + \text{P1} .$$

The values of P1, P2, and P3 obtained above can be substituted into this expression:

$$[(6.6\text{E-}2) \times (1 - 2.1\text{E-}2) \times 7.0\text{E-}4] + [(6.6\text{E-}2) \times (2.1\text{E-}2)] + 1.0\text{E-}3$$

$$= 4.5\text{E-}5 + 1.4\text{E-}3 + 1.0\text{E-}3$$

$$= 2.4\text{E-}3$$

to obtain a CCDP value which is consistent with the value obtained by other methods in the preliminary ASP analysis.

This value is consistent with the values developed using the TRC HRA model in the ASP analysis.

H.14.2 NRC Comments

None.

H.15 LER No. 498/94-012

Event Description: Emergency Diesel Generator 11 and Turbine-Driven Auxiliary Feedwater Pump 14 Simultaneously Inoperable

Date of Event: March 11, 1994

Plant: South Texas 1

H.15.1 Licensee Comments

Reference: Letter from T. H. Cloninger, Houston Lighting & Power, to the U.S. NRC, dated May 16, 1995, ST-HL-AE-5084.

Comment 1: (Summary) The event followed an extended shutdown of approximately 1 year, and decay heat levels were extremely low. Under these conditions, it would take over 24 h for the steam generators to dry out without any auxiliary feedwater. Also, at low decay heat levels, it is unlikely that the PORVs would lift. Therefore, more time should be allowed in the analysis for the recovery of electric power prior to assuming core damage will occur.

Response 1: The Accident Sequence Precursor (ASP) Program has typically reviewed shutdown events to determine if these events could have occurred with the unit at power. If so, the event is then screened for analysis as a possible precursor, using conventional ASP selection criteria. In this event, the combination of the emergency diesel generator (EDG) failure and the unavailability of the turbine-driven auxiliary feedwater (TDAFW) pump could have occurred with any power history and would then meet the selection criteria for analysis. However, given the extended shutdown power history prior to this event, translating this event to an at-power condition may be considered overly conservative.

Comment 2: (Summary) EDG 11 should not be modeled as guaranteed to fail for the entire 633-h period since there were six successful starts between the two related failures. This gives a failure-to-start probability during the period of interest of 2/8. The only period with a guaranteed failure of EDG 11 should be the 148-h period between the last successful start (February 23, 1994, at 0657 hours) and the second failure (March 1, 1994, at 1120 hours).

Response 2: It appears that the failure of the spring associated with the K1 relay was somewhat sporadic or was correctly (although temporarily) realigned during the maintenance following the initial EDG failure (February 3, 1994, at 0204 hours). Two of the six successful starts were not documented as valid tests; however, valid successful tests were performed before and after the TDAFW pump maintenance period (February 8, 1994, through February 13, 1994). So, it is reasonable to expect EDG 11 to have started and loaded as required during the TDAFW pump maintenance period. Therefore, the period that EDG 11 was unavailable and the period that the TDAFW pump was unavailable do not overlap. As a result, this event no longer meets the typical selection criteria for analysis by the ASP Program. The unavailabilities of the individual components were within the plant's technical specification requirements. Therefore, the event was not analyzed as a long-term single-train unavailability. As a result, the unavailability of EDG 11 and the TDAFW pump described in LER No. 498/94-012 has been removed from the set of 1994 accident sequence precursors.

H.15.2 NRC Comments

None.

H.16 Inspection Reports 499/94-13 and 499/94-16

Event Description: Emergency Diesel Generator 22 Long-Term Unavailability

Date of Event: March 2, 1994

Plant: South Texas 2

H.16.1 Licensee Comments

Reference: Letter from L. E. Martin, Houston Lighting and Power, to U.S. NRC, dated August 31, 1995, ST-HL-AE-5153.

Comment 1: Although the 4R piston was damaged, all indications are that it was still functioning at the time of the 18-month inspection. It is not known how long the piston skirt had been broken, but the damage had not progressed to the point of disabling the cylinder. Because the damage did not cause failure, there is nothing to indicate when it had occurred.

Comment 2: The broken piston would not necessarily cause engine failure, as it did not cause failure during the latest test. It would be accurate to say that the diesel was in a degraded condition and to postulate that the probability of failure was higher than average while this condition existed. But the failure probability was demonstrably not equal to one, as damage was found only by inspection of the piston, not by failure of the engine.

Comment 3: Houston Light and Power (HL&P) disagrees with the statement that the piston failure would not be detected unless EDG 22 was run. The piston failure was detected by a teardown inspection, and not by running the engine. In fact, in previous tests with the engine running, the cylinder gave normal test indications.

Comment 4: HL&P disagrees with the logic applied to speculate that the EDG 22 piston failure could have occurred at power. The unit was not at power, but was in a shutdown that had lasted for almost exactly 1 year. No fuel was in the core, and considering the low level of decay heat in the fuel pool, a loss of ac power would have had to last a long time to have any consequence.

Response: The failure of the EDG occurred following an extended shutdown period of approximately 1 year. The EDG was found in a degraded condition. The preliminary analysis assumed that further operation of the EDG would result in further degradation of the EDG and its eventual failure. Although the event occurred with the plant in a shutdown condition, the event was originally analyzed with the plant in an at-power condition. Previously, the ASP Program has reviewed conditions discovered with the plant in a shutdown condition to determine if the condition was unique to the shutdown condition. In other words, was there a specific factor involved in the event that would prevent it from occurring with the plant at power? If the answer to this question was no, then the event would have been analyzed as an at-power event regardless of whether the event actually affected at-power operation. Since the preliminary analysis of this event was completed, the ASP Program guidelines for analysis of this type of event has changed. Now, only those conditions identified with the plant shutdown that had the potential to affect at-power operations will be candidates for analysis as at-power events.

In the case of this event, it was assumed that the EDG had been tested throughout the extended shutdown period. As a result, it was assumed that the degradation of the EDG would not have affected the plant during its previous power operation (over 1 year previous to this event). Based on the change in the guidelines for reviewing this type of event, the event would now be analyzed as a shutdown event. As a result, the conditional core damage probability for the event falls below the precursor cutoff value (1×10^{-6}). Therefore, the event has been eliminated from the set of 1994 precursor events.

H.16.2 NRC Comments

None.

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-4674
ORNL/NOAC-232
Vol. 21

2. TITLE AND SUBTITLE

Precursors to Potential Severe Core Damage Accidents: 1994
A Status Report

Main Report and Appendices A-H

3. DATE REPORT PUBLISHED

MONTH	YEAR
December	1995

4. FIN OR GRANT NUMBER

B0435

5. AUTHOR(S)

R. J. Belles, J. W. Cletcher, D. A. Copinger, B. W. Dolan,*
J. W. Minarick,* L. N. Vanden Heuvel

6. TYPE OF REPORT

Technical

7. PERIOD COVERED (Inclusive Dates)

1994

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.)

Oak Ridge National Laboratory
Oak Ridge, TN 37831-8065

*Science Applications International
Corporation
Oak Ridge, TN 37831

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.)

Safety Programs Division
Office for Analysis and Evaluation of Operational Data
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

10. SUPPLEMENTARY NOTES

11. ABSTRACT (200 words or less)

Nine operational events that affected ten commercial light-water reactors (LWRs) during 1994 that are considered to be precursors to potential severe core damage are described. All of these events had conditional probabilities of subsequent core damage greater than or equal to 1.0×10^{-6}. These events were identified by computer-screening the 1994 licensee event reports from commercial LWRs to identify those that could be potential precursors. Candidate precursors were then selected and evaluated in a process similar to that used in previous assessments. Selected events underwent engineering evaluation that identified, analyzed, and documented the precursors. Other events designated by the Nuclear Regulatory Commission (NRC) also underwent a similar evaluation. Finally, documented precursors were submitted for review by licensees and NRC staff to ensure that the plant design and its response to the precursor were correctly characterized. This study is a continuation of earlier work, which evaluated 1969-1981 and 1984-1993 events. The report discusses the general rationale for this study, the selection and documentation of events as precursors, and the estimation of conditional probabilities of subsequent severe core damage for events. This document is bound in two volumes: Volume 21 contains the main report and Appendices A-H; Volume 22 contains Appendix I.

12. KEY WORDS/DESCRIPTORS (List words or phrases that will assist researchers in locating the report.)

Nuclear Power Plant, Accident Sequence Precursors, Risk Analysis, Event Trees, Core Damage Probability, Accident Sequences, Licensee Event Reports, Operational Events

13. AVAILABILITY STATEMENT

Unlimited

14. SECURITY CLASSIFICATION

(This Page)
Unclassified

(This Report)
Unclassified

15. NUMBER OF PAGES

16. PRICE

Printed
on recycled
paper

Federal Recycling Program