Precursors to Potential Severe Core Damage Accidents: 1997

A Status Report

Prepared by
R. J. Belles, J. W. Cletcher, D. A. Copinger,
B. W. Dolan, J. W. Minarick, M. D. Muhlheim

Oak Ridge National Laboratory

Prepared for
U.S. Nuclear Regulatory Commission

RECEIVED
DEC 20 1999
OSTI

DISTRIBUTION OF THIS DOCUMENT IS UNLIMITED *ph*

MASTER

AVAILABILITY NOTICE

Availability of Reference Materials Cited in NRC Publications

NRC publications in the NUREG series, NRC regulations, and *Title 10, Energy*, of the *Code of Federal Regulations*, may be purchased from one of the following sources:

1. The Superintendent of Documents
U.S. Government Printing Office
P.O. Box 37082
Washington, DC 20402-9328
<http://www.access.gpo.gov/su_docs>
202-512-1800
2. The National Technical Information Service
Springfield, VA 22161-0002
<<http://www.ntis.gov/ordernow>>
703-487-4650

The NUREG series comprises (1) technical and administrative reports, including those prepared for international agreements, (2) brochures, (3) proceedings of conferences and workshops, (4) adjudications and other issuances of the Commission and Atomic Safety and Licensing Boards, and (5) books.

A single copy of each NRC draft report is available free, to the extent of supply, upon written request as follows:

Address: Office of the Chief Information Officer
Reproduction and Distribution
Services Section
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001
E-mail: <GRW1@NRC.GOV>
Facsimile: 301-415-2289

A portion of NRC regulatory and technical information is available at NRC's World Wide Web site:

<<http://www.nrc.gov>>

All NRC documents released to the public are available for inspection or copying for a fee, in paper, microfiche, or, in some cases, diskette, from the Public Document Room (PDR):

NRC Public Document Room
2121 L Street, N.W., Lower Level
Washington, DC 20555-0001
<<http://www.nrc.gov/NRC/PDR/pdr1.htm>>
1-800-397-4209 or locally 202-634-3273

Microfiche of most NRC documents made publicly available since January 1981 may be found in the Local Public Document Rooms (LPDRs) located in the vicinity of nuclear power plants. The locations of the LPDRs may be obtained from the PDR (see previous paragraph) or through:

<<http://www.nrc.gov/NRC/NUREGS/SR1350/V9/lpdr/html>>

Publicly released documents include, to name a few, NUREG-series reports; *Federal Register* notices; applicant, licensee, and vendor documents and correspondence; NRC correspondence and internal memoranda; bulletins and information notices; inspection and investigation reports; licensee event reports; and Commission papers and their attachments.

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. Such documents as theses, dissertations, foreign reports and translations, and non-NRC conference proceedings may be purchased from their sponsoring organization.

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. These standards are available in the library for reference 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—

American National Standards Institute
11 West 42nd Street
New York, NY 10036-8002
<<http://www.ansi.org>>
212-642-4900

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, 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.

DISCLAIMER

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

DISCLAIMER

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

Precursors to Potential Severe Core Damage Accidents: 1997

A Status Report

Manuscript Completed: October 1998
Date Published: November 1998

Prepared by
R. J. Belles, J. W. Cletcher, D. A. Copinger,
B. W. Dolan*, J. W. Minarick*, M. D. Muhlheim

Oak Ridge National Laboratory
Managed by Lockheed Martin Energy Research Corp.
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 Job Code B0435

---

*Science Applications International Corporation, Oak Ridge, TN 37831

PREVIOUS REPORTS IN THE 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-182/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. A. Forester, J. W. Minarick, H. K. Schriener, B. W. Dolan, D. B. Mitchell, D. W. Whitehead, and J. J. Jansen, Sandia Natl. Lab. and Science Applications International Corp., *Precursors to Potential Severe Core Damage Accidents: 1982-83, A Status Report*, USNRC Report NUREG/CR-4674, Vol. 24 (SAND97-0807), April 1997.
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: 1985, A Status Report*, USNRC Report NUREG/CR-4674 (ORNL/NOAC-232, Vols. 1 and 2), December 1986.
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: 1986, A Status Report*, USNRC Report NUREG/CR-4674 (ORNL/NOAC-232, Vols. 5 and 6), May 1988.
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: 1987, A Status Report*, USNRC Report NUREG/CR-4674 (ORNL/NOAC-232, Vols. 7 and 8), July 1989.
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: 1988, A Status Report*, USNRC Report NUREG/CR-4674 (ORNL/NOAC-232, Vols. 9 and 10), February 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: 1989, A Status Report*, USNRC Report NUREG/CR-4674 (ORNL/NOAC-232, Vols. 11 and 12), August 1990.

-
10. 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.
  11. 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.
  12. 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.
  13. L. N. Vanden Heuvel, J. W. Cletcher, D. A. Copinger, J. W. Minarick, and B. W. Dolan, 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.
  14. R. J. Belles, J. W. Cletcher, D. A. Copinger, B. W. Dolan, J. W. Minarick, and L. N. Vanden Heuvel, Lockheed Martin Energy Systems, Inc., Oak Ridge Natl. Lab.; and Science Applications International Corp., *Precursors to Potential Severe Core Damage Accidents: 1994, A Status Report*, USNRC Report NUREG/CR-4674 (ORNL/NOAC-232, Vols. 21 and 22), December 1995.
  15. R. J. Belles, J. W. Cletcher, D. A. Copinger, B. W. Dolan, J. W. Minarick, and M. D. Muhlheim, Lockheed Martin Energy Research, Inc., Oak Ridge Natl. Lab.; and Science Applications International Corp., *Precursors to Potential Severe Core Damage Accidents: 1995, A Status Report*, USNRC Report NUREG/CR-4674 (ORNL/NOAC-232, Vol. 23), April 1997.
  16. R. J. Belles, J. W. Cletcher, D. A. Copinger, B. W. Dolan, J. W. Minarick, and M. D. Muhlheim, Lockheed Martin Energy Research, Inc., Oak Ridge Natl. Lab.; and Science Applications International Corp., *Precursors to Potential Severe Core Damage Accidents: 1996, A Status Report*, USNRC Report NUREG/CR-4674 (ORNL/NOAC-232, Vol. 25), December 1997.

Abstract

This report describes the five operational events in 1997 that affected five commercial light-water reactors (LWRs) and that are considered to be precursors to potential severe core damage accidents. 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 first computer-screening the 1997 licensee event reports from commercial LWRs to identify those events that could be precursors. Candidate precursors were 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 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 1969–1996 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 the events.

Contents

	Previous Reports in Series	i
	Abstract	iii
	List of Figures	vii
	List of Tables	vii
	Preface	ix
	Foreword	xi
	Acknowledgments	xiii
	List of Acronyms	xv
1.	Introduction	1-1
	1.1 Background	1-1
	1.2 Current Process	1-1
2.	Selection Criteria and Quantification	2-1
	2.1 Accident Sequence Precursor Selection Criteria	2-1
	2.1.1 Precursors	2-1
	2.1.2 Potentially Significant Events Considered Impractical to Analyze	2-4
	2.1.3 Containment-Related Events	2-5
	2.1.4 "Interesting" Events	2-5
	2.2 Precursor Quantification	2-5
	2.3 Review of Precursor Documentation	2-6
	2.4 Precursor Documentation Format	2-8
	2.5 Potential Sources of Error	2-8
3.	Results	3-1
	3.1 Tabulation of Precursors	3-2
	3.1.1 Potentially Significant Events That Were Impractical to Analyze	3-2
	3.1.2 Containment-Related Events	3-5
	3.1.3 "Interesting" Events	3-5
	3.2 Number of Precursors Identified	3-5
	3.3 Important Precursors	3-6
	3.4 Insights	3-8
	3.5 Conclusion	3-17
4.	Glossary	4-1
5.	References	5-1

Appendix A: ASP Calculational Methodology	A.1-1
Appendix B: At-Power Precursors for 1997	B.1-1
Appendix C: Shutdown Precursors for 1997	C.1-1
Appendix D: "Impractical" Events	D.1-1
Appendix E: Containment-Related Events	E.1-1
Appendix F: "Interesting" Events	F.1-1
Appendix G: Resolution of Comments for 1997 Precursor Analyses	G.1-1

List of Figures

Figure	Page
Fig. 2.1 ASP analysis process	2-2
Fig. 2.2 ASP review process	2-7
Fig. 3.1 CCDP results by year for 10^{-6} to 10^{-5}	3-7
Fig. 3.2 CCDP results by year for 10^{-5} to 10^{-4}	3-7
Fig. 3.3 CCDP results by year for 10^{-4} to 10^{-3}	3-7
Fig. 3.4 CCDP results by year for 10^{-3} to 1.0	3-7
Fig. 3.5 Percentage of events resulting from unavailabilities	3-9
Fig. 3.6 Percentage of important precursors by year	3-10
Fig. 3.7 Percentage of precursors occurring at BWRs	3-11
Fig. 3.8 Percentage of precursors at multiunit sites	3-12
Fig. 3.9 Number of AFW/EFW-related precursors	3-13
Fig. 3.10 Percentage of electric-power-related precursors	3-14
Fig. 3.11 Number of LOOP-related precursors per year	3-15
Fig. 3.12 Total number of precursors by year	3-16

List of Tables

Table 3.1 At-Power Precursors Involving Initiating Events Sorted by Plant	3-3
Table 3.2 At-Power Precursors Involving Unavailabilities Sorted by Plant	3-3
Table 3.3 At-Power Precursors Involving Initiating Events Sorted by CCDP	3-4
Table 3.4 At-Power Precursors Involving Unavailabilities Sorted by Importance	3-4
Table 3.5 Potentially Significant Events Considered Impractical to Analyze	3-5
Table 3.6 Index of "Interesting" Events	3-5
Table 3.7 Number of Precursors by Year	3-6
Table 3.8 Number of Precursors by Event Type	3-8
Table 3.9 Precursors not Typically Modeled in PRAs or IPEs	3-8
Table 3.10 Precursors with a CCDP $\geq 10^{-3}$	3-10

PREFACE

The Accident Sequence Precursor (ASP) Program was established at the Nuclear Operations Analysis Center (NOAC) 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. Sixteen reports documenting the review of operational events for precursors have been published in this program (see Sect. 5.0, Refs. 1-16). These reports describe events that occurred from 1969 through 1996, including the recently published review of 1982 and 1983 event analyses. They have been completed on a yearly basis since 1986.

The current effort was undertaken on behalf of the Office for Analysis and Evaluation of Operational Data (AEOD) of the Nuclear Regulatory Commission (NRC). The NRC Project Manager is Dr. 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 1997 is a continuation of the assessment undertaken in the previous reports for operational events that occurred in 1969-1996.

The preliminary analyses of the 1997 events were sent for review to NRC staff and to licensees for those plants for which potential precursors were identified. This method is similar to the review process used for the 1992-1996 events. Similar to the 1994-1996 event analyses, the 1997 analyses 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 had been included normally in past ASP analyses of events. Therefore, comparing and trending analysis results from prior years is more difficult because some analysis results before 1992 likely would have been different if additional information had been solicited from the licensees and incorporated.

For 1997 the total number of precursors identified is about one-half that in the past several years. The same models were used for the analysis of 1997 events as were used in the analysis of 1994-1996 events. These models utilize ASP class-based event trees and plant-specific linked fault trees. Because these models were introduced in 1994, care must be used when comparing results from 1994-1997 with results 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 for PRA-related information.

Gary T. Mays, Head
Operational Performance Technology
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 1997 operational experience data by the Nuclear Regulatory Commission's (NRC'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, degradation 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 that were most significant in terms of the potential for inadequate core cooling and core damage. In addition, the program has the following secondary objectives to (1) categorize the precursors for plant-specific and generic implications, (2) provide a measure that can be used to trend nuclear plant core damage risk, and (3) provide a partial check on PRA-predicted dominant core damage scenarios.

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 the established practice, the preliminary ASP analyses of 1997 events 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 a 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 precursors were reviewed, and the conditional core damage probability calculations were revised where appropriate. The objective of the review process was to provide as realistic an analysis of the significance of the event as possible. Once all comments received from the review of the preliminary analyses had been resolved, the final analyses were transmitted to the licensees and made publicly available at that time. 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 (5) identified for 1997 is about one-half the total in each of the last 2 years (14 in 1996; 10 in 1995). All of the precursors for 1997 occurred at pressurized-water reactors, and none of them had a conditional core damage probability (CCDP) $\geq 10^{-4}$. Therefore, for 1997 operational events, there is no discussion section detailing attributes of the "important" (CCDP $\geq 10^{-4}$) precursors in this report.

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 NRC's Office for Analysis and Evaluation of Operational Data (AEOD). The AEOD project manager, Dr. P. D. O'Reilly, was instrumental in obtaining timely comments from the NRC staff and licensees and providing guidance on technical issues. We would like to especially thank Donnie Whitehead and Don Mitchell of Sandia National Laboratories and Stuart Lewis of SAROS, Inc. for providing independent technical review of each analysis. We would also like to thank the Project Managers from the NRC's Office of Nuclear Reactor Regulation for their efforts in receiving comments from the licensees. 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 (ORNL)

G. T. Mays
W. P. Poore

Nuclear Regulatory Commission

S. E. Mays
P. D. O'Reilly
D. M. Rasmuson

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

A. G. Andrews
L. B. Dockery
D. S. Queener
D. G. Sharp
L. W. Xiques

List of Acronyms

ac	alternating current
ACB	air circuit breaker
AEOD	Analysis and Evaluation of Operational Data
AFPC	augmented FPC mode II
AFW	auxiliary feedwater
AIT	augmented inspection team
ASP	Accident Sequence Precursor (Program)
BOP	balance of plant
BWR	boiling-water reactor
BWST	borated water storage tank
B&W	Babcock and Wilcox
CAR	containment air recirculation
CCDP	conditional core damage probability
CCF	common-cause failure
cd	core damage
CDP	core damage probability
CPS	Clinton Power Station
CRD	control rod drive system
CS	carbon steel
CSAS	containment spray actuation signal
CWS	circulating water system
DBA	design basis accident
dc	direct current
DHR	decay heat removal
ECCS	emergency core cooling system
EDG	emergency diesel generator
EFW	emergency feedwater
EOP	emergency operating procedure
EPRI	Electric Power Research Institute
ERAT	emergency reserve auxiliary transformer
ESF	engineered safety feature
ESFAS	engineered safety feature actuation signal
ESW	emergency service water
FPC	fuel pool cooling
FPL	Florida Power and Light
FSAR	final safety analysis report
GL	generic letter
HPI	high-pressure injection
HPSI	high-pressure safety injection
IIT	Incident Investigation Team
INEEL	Idaho National Engineering and Environmental Laboratory

---

IPE	Individual Plant Examination
IRRAS	Integrated Reliability and Risk Analysis System
kV	kilovolts
LBLOCA	large-break loss of coolant accident
LCO	limiting conditions of operation
LDST	letdown storage tank
LER	licensee event report
LOCA	loss-of-coolant accident
LOFW	loss of main feedwater
LOOP	loss of offsite power
LPI	low-pressure injection
LPR	low-pressure recirculation
LPSI	low-pressure safety injection
LWR	light-water reactors
MDP	motor-driven pump
MFW	main feedwater
MGL	Multiple Greek Letter
MLOCA	medium-break loss-of-coolant accident
MOV	motor-operated valve
MSLB	main steam line break
MT	main transformer
MU	makeup
NOAC	Nuclear Operations Analysis Center
NPSH	net positive suction head
NRC	Nuclear Regulatory Commission
OD	outside diameter
OOS	out of service
ORNL	Oak Ridge National Laboratory
PCIS	primary containment isolation system
PI	performance indicator
PM	preventive maintenance
PNPS	Pilgrim Nuclear Power Station
PORV	power-operated relief valve
PRA	probabilistic risk assessment
PWR	pressurized-water reactor
RAS	recirculation actuation signal
RAT	reserve auxiliary transformer
RB	reactor building
RBCCWP	reactor building closed cooling water pump
RCIC	reactor core isolation cooling
RCP	reactor coolant pump
RCS	reactor coolant system
RFO	refueling outage
RHR	residual heat removal
RT	radiographic testing (Oconee 2)

RT	reactor trip (in general)
RWB	radwaste building
RWST	refueling water storage tank
RWT	refueling water tank
SBO	station blackout
SBODG	station blackout diesel generator
SCSS	Sequence Coding and Search System
SDC	shutdown cooling
SG	steam generator
SGTR	steam generator tube rupture
SIT	special investigation team
SKI	Swedish Nuclear Power Inspectorate
SLOCA	small-break loss-of-coolant accident
SNL	Sandia National Laboratories
SS	stainless steel
SSF	safe shutdown facility
SSWP	salt service water pump
SUT	startup transformer
SW	socket weld
TDP	turbine-driven pump
TMI 1	Three Mile Island, Unit 1
TRANS	transient
TRC	time-reliability correlation
TS	Technical Specifications
TW	through-wall
UAT	unit auxiliary transformer
UE	unusual event
UT	ultrasonic testing

1. Introduction

The Accident Sequence Precursor (ASP) Program involves the systematic review and evaluation of operational events or conditions that have occurred at licensed U.S. commercial 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 in later status reports.²⁻¹⁶ This report details the review and evaluation of operational events that occurred in 1997. The requirements for licensee event reports (LERs) is given in the Title 10 of the Code of Federal Regulations, Part 50.73; reporting guidance is described in NUREG-1022, *Licensee Event Report System, Description of System and Guidelines for Reporting*.¹⁷⁻¹⁹

1.1 Background

The ASP Program owes its genesis to the Risk Assessment Review Group,²⁰ 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." [Ref. 21]. Evaluations done for the 1969-1981 period were the first efforts in this type of analysis.

Accident sequences of interest are those that, if additional failures had occurred, would have resulted in inadequate core cooling that could have caused severe core damage. For example, a postulated loss-of-coolant accident (LOCA) with a reported failure of a high-pressure injection (HPI) system may be examined or studied. In this example, the precursor would be the HPI system failure.

Events considered to be potential precursors are analyzed, and a conditional probability of core damage is calculated. This probability is estimated by mapping failures observed during the event onto ASP core damage 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 Chap. 2. Completed precursor analyses were transmitted for review by the responsible licensees, the Nuclear Regulatory Commission (NRC) staff, and an independent NRC contractor. All comments were evaluated, and the analyses were revised as appropriate.

The ASP Program uses the NRC's Sequence Coding and Search System (SCSS) data base to identify most LERs that are reviewed for potential precursors. The SCSS data base contained 1861 LERs for 1997. The ASP computer search algorithm selected 797 of these for engineering review as potential precursors. Of the nine events that the NRC identified from other sources for engineering review, one event was not selected by the computer search. As a result 798 events were selected for review. Of these 798 events, 48 LERs (55 including revisions) were determined to be potentially significant. Of these 48, 31 LERs were rejected after detailed analysis, 2 LERs were determined to be impractical to analyze, and 8 LERs (5 events) were

Introduction

---

documented as "interesting" events. Review and analysis of the events described in the remaining seven LERs led to the identification of five precursors for 1997. The results of these analyses are shown in Tables 3.1-3.4.

In addition to the events selected as accident sequence precursors, events involving loss of containment function and others that are considered serious but are not modeled in the ASP Program were identified during the 1997 LER review. These events are also documented in this report.

Chapter 2 describes the selection and analysis process used for the review of 1997 events. Chapter 3 provides a tabulation of the precursors, a summary of the more important precursors, and insights gained from the analyses and results. Chapter 4 provides a glossary of terms, and Chapter 5 provides the list of references. The remainder of this report is divided into seven appendices: Appendix A describes the ASP calculational methodology, Appendix B describes the at-power precursors, Appendix C describes the basis for selection as a shutdown precursor, Appendix D contains the potentially significant events considered impractical to analyze, Appendix E describes the requirements for an event to be considered a "containment-related" event, Appendix F contains "interesting" events, and Appendix G contains the resolution of comments on the preliminary 1997 ASP analyses.

2. Selection Criteria and Quantification

2.1 Accident Sequence Precursor Selection Criteria

The 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 LOCA, and steam generator tube rupture (SGTR) [pressurized-water reactors (PWRs) only]. These four initiators are primarily associated with loss of core cooling. ASP Program staff members examine LERs and other event documentation to determine the impact that operational events have on potential core damage sequences associated with these initiators. (Operational events are occasionally identified that impact other initiators, such as a large-break LOCA. Unique models are developed to address these events.)

2.1.1 Precursors

This section describes the steps used to identify events requiring analysis. Figure 2.1 illustrates this process.

A computerized search of the SCSS data base at the Nuclear Operations Analysis Center (NOAC) of the Oak Ridge National Laboratory (ORNL) 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 for core damage-related initiating events. A review of 4 years of precursor data and 1 year of LERs determined that this computerized search successfully identifies almost all precursors within a subset of approximately one-third to one-half of all LERs.

LERs 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 NRC designated other events for inclusion in the review process.

Those events selected underwent one- or two-engineer review to determine if the reported event should be examined in greater detail. Events that, in the judgment of the initial reviewing engineer, clearly fail to satisfy the ASP criteria for analysis as a potential precursor are not subject to another evaluation. All other events are reviewed by two engineers to determine if they meet the ASP criteria for detailed analysis before the decision is made to reject or analyze the event. This initial review is a bounding review, meant to capture events that in any way appear to deserve detailed review and to eliminate events that are clearly unimportant. This process involves eliminating events that satisfy predefined criteria for rejection and accepting all others as potentially significant and requiring analysis.

Selection Criteria and Quantification

Fig. 2.1. ASP analysis process.

LERs were eliminated from further consideration as precursors if they involved only one of the following:

- a component failure with no loss of redundancy,
- a short-term loss of redundancy in only one system,
- an event that occurred prior to initial criticality,
- design or qualification error that is small relative to what is predicted (e.g., an error of a few percent in an actuation setpoint),
- an event bounded by a reactor trip or an 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 analyses were not limited to the LERs; also used were final safety analysis reports (FSARs) and their amendments, individual plant examinations (IPEs), and other information related to the event of interest, which are available at ORNL and NRC.

The detailed analysis 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.

Selection Criteria and Quantification

3. If the event or failure was identified while the plant was not at power, then the event was first assessed to determine whether it could have impacted at-power operation. If the event could have impacted at-power operation, its impact was assessed. If the event could only occur at cold shutdown or refueling shutdown, then its impact on continued decay heat removal during shutdown was assessed.

For each actual occurrence or postulated initiating event associated with an operational event reported in an LER, 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). Events of low significance are thus excluded, allowing attention to be focused on the more important events. This approach is consistent with the approach used to define 1987–1996 precursors, but differs from that of earlier ASP reports, which addressed all events meeting the precursor selection criteria regardless of conditional core damage probability.

Five operational events with conditional probabilities of subsequent severe core damage $\geq 1.0 \times 10^{-6}$ were identified as accident sequence precursors. Five events were analyzed as at-power events and are documented in Appendix B; because no events were analyzed as shutdown events, a description of the basis of what constitutes a shutdown event is documented in Appendix C.

While review of LERs identified by this process is expected to identify almost all precursors, it is possible that a few precursors exist within the set of unreviewed LERs. Some potential precursors that would have been found if all 1997 LERs had been reviewed may not have been identified. Because of this, it should not be assumed that the set of 1988–1997 precursors is consistent with precursors identified in 1984–1987.

2.1.2 Potentially Significant Events Considered Impractical to Analyze

In some cases, events are impractical to analyze because of lack of information or inability to reasonably model 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. Such events are thought to be capable of impacting core damage sequences. However, the events usually involve component degradations in which the extent of the degradation cannot be determined or the impact of the degradation on plant response cannot be ascertained.

Two of the 1997 LERs were identified as potentially significant but impractical to analyze.

For many events classified as impractical to analyze, an assumption that the affected component or function was unavailable over a 1-year period (as would be done using a bounding analysis) would result in the conclusion that a very significant condition existed. This conclusion would not be supported by the specifics of the event as reported in the LER or by the limited engineering evaluation performed in the ASP Program. A description of the basis for an event to be considered impractical to analyze, as well as a description of the two events considered impractical to analyze, is provided in Appendix D.

2.1.3 Containment-Related Events

Events involving loss of containment functions—such as containment cooling, containment spray, containment isolation (direct paths to the environment only), or hydrogen control—are classified as “containment-related” events. The review of the 1997 LERs identified no containment-related events; however, Appendix E provides the basis for events considered containment-related.

2.1.4 “Interesting” Events

Events that provide insight into unusual failure modes with the potential to compromise continued core cooling but are not considered to be precursors are documented as “interesting” events. The review of the 1997 LERs resulted in five events (documented in eight LERs) being classified as interesting. These events are documented in Appendix F.

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 probability is estimated by mapping failures observed during the event onto the ASP accident sequence models (event trees and linked fault trees modified to reflect the event), which depict potential paths to severe core damage, and calculating a conditional probability of core damage. The effect of a precursor on event tree branches is assessed by reviewing the operational event specifics against system design information. This information is used to modify the ASP model (typically the fault trees). 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. Details of the event modeling process and calculational results can be found in Appendix A of this report.

The calculational approach used for the analysis of 1997 events was similar to that used for the 1994–1996 events. Linked fault tree models were used instead of the earlier event-tree-based models. The use of linked fault trees allows the impact of individual component failures to be more correctly addressed; this could only be approximated in the earlier models. As with the 1994–1996 events, the conditional core damage probability (CCDP) during the time period in which the failures were observed was used to rank the initiating event assessments. The importance measure, the difference between the CCDP and the nominal core damage probability (CDP) for the same period of time, was used to rank the unavailability assessments. Pre-1994 assessments used the importance measure to rank events.

For most events 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, the nominal plant response during the time period dominates the results. In these cases, the CCDP can be considerably higher than the importance measure (the impact of such a condition on plant response is relatively minor). By only looking at the CCDP for such an event, its significance may be overestimated. Therefore, for condition assessments, the CCDP, the CDP, and the difference between these values (i.e., the importance) are provided.

Selection Criteria and Quantification

The frequencies and failure probabilities used in the calculations are derived in part from data obtained across the population of LWRs. An attempt has been made to make the frequencies and failure probabilities plant-specific. However, this effort is not complete. Because of this, the conditional probabilities determined for each precursor cannot be rigorously associated with the probability of severe core damage resulting from the actual event at the specific reactor plant where it occurred.

The evaluation of precursors in this report considers and, where appropriate, gives credit for additional equipment or recovery procedures at the plants. Accordingly, the evaluations for 1994–1997 are not directly comparable to the results for prior years. Examples of additional equipment and recovery procedures addressed since the 1994 analyses, when information was available, include use of supplemental emergency diesel generators (EDGs) for station blackout mitigation and alternate systems for steam generator (SG) and reactor coolant system (RCS) makeup.

2.3 Review of Precursor Documentation

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

After completion of the initial analyses of the precursors, 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. Comments were received for all of the preliminary precursors from all the responsible licensees.

As with the 1993–1996 events, the 1997 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 NRC and SNL for final comments, and revised again, if necessary.

In some cases the analysis results were affected as a result of comments received. In general, this was the result of incorporation of plant-specific equipment or strategies for mitigating events. Incorporation of these factors for a subset of the analyses reduces the validity of ranking the events by CCDP. Consistent incorporation of these mitigation strategies across all of the events could affect the CCDP of some events and may affect the ranking of the events.

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 G.

Fig. 2.2. ASP review process.

2.4 Precursor Documentation Format

The at-power precursors are contained in Appendix B; the basis for shutdown precursors is contained in Appendix C. 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 the analysis results. A figure indicating the dominant core damage sequence postulated for each event is also included.

The CCDP calculation for each precursor is documented. The tables associated with each specific event analysis include selected basic event probabilities; sequence logic, probabilities, and importance; system names for higher probability sequences; and selected cut sets for higher probability sequences.

2.5 Potential Sources of Error

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

1. *Evaluation of only a subset of 1997 LERs.* For 1969–1981 and 1984–1987, all LERs reported during the year were evaluated for precursors. For 1982–1983 and 1988–1997, 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.
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 LER for initial review can be somewhat judgmental. Events selected in the study were more serious than most. Hence, the majority of the LERs 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.
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 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 may not adequately reflect all of the important differences such

as the lack of support system models and station blackout issues. Modeling improvements that address these problems are being pursued in the ASP Program.

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 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 plant-class features included in the ASP event tree models were addressed in the 1997 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 Appendix A. 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. Programmatic constraints have prevented substantial efforts in estimating actual recovery probabilities. The values currently used are based on a review of recovery actions during historic events and also include consideration of human error during recovery. These values have been reviewed both within and outside the ASP Program. While it is acknowledged that substantial uncertainty exists, these values are thought adequate for ranking purposes, which is one of the goals of the current precursor calculations. (The primary goal is to provide a realistic estimate of the risk.) This assessment is supported by the sensitivity and uncertainty calculations documented in the 1980-1981 report.² These calculations demonstrated only a small impact on the relative ranking of events from changes in the numeric values.
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 LER. See Ref. 2 for a more comprehensive discussion of test interval assumptions.

3. Results

This chapter summarizes the results of the review and evaluation of 1997 operational events. The primary result of the ASP Program is the identification of operational events with CCDPs $\geq 1.0 \times 10^{-6}$ 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 LOFW with a degraded mitigating system. Five of the events that occurred during 1997 were determined to have a CCDP $\geq 10^{-6}$ and were transmitted to the respective licensees for review and comment. These events are documented as precursors in App. B.

Direct comparison of results with those of earlier years is not possible without substantial effort to reconcile analysis differences. The major differences in the selection and modeling of events, which were implemented for event assessments for 1984, 1988, 1992, and 1994, are discussed below.

1984-1987 The revised LER rule, which went into effect in 1984, resulted in more LERs being selected for detailed review even though fewer LERs were reported. One requirement of the revised LER rule is the detailed reporting of all operational events involving reactor trip. This allowed reactor trips with degraded mitigating systems to be analyzed as precursors (previously, the plant state at the time a degraded system was discovered could not always be discerned in the LERs). The new LER rule also required additional detail for those events that are reported. Model changes included using event trees that were developed on a plant-class basis to more accurately reflect plant response following an initiating event. The models also included additional mitigating systems that could prevent core damage. The system failure probabilities were estimated using simplified train-based system models. These probabilities were checked against observed failures in the 1984-1985 period. Section 5 in NUREG/CR-4674, Vol. 3, provides additional details of these changes.⁴

1988-1992 Two major types of changes for 1988 resulted in differences between the 1988-1992 ASP Program efforts and those of earlier years. Prior to 1988, all LERs were reviewed by members of the project team. Starting in 1988, computerized searches of the SCSS data base identified those LERs that met the minimum selection criteria (e.g., failures in plant systems that provide protective functions for the plant for core damage-related initiating events). Hence, the project team evaluated only a portion of the LERs. This change, however, does not impact the number of precursors. Section 2.1.1 provides further details of the selection criteria. Model changes included: (1) revising the LOOP recovery model, (2) the explicit modeling of PWR reactor coolant pump seal LOCA sequences, and (3) the reassignment of core vulnerability sequences on earlier trees to either success or core damage sequences. The net effect of the last change was a significant reduction in the complexity of the event trees, with little impact on the relative significance estimated for each precursor. NUREG/CR-4674, Vol. 9, provides additional details of these changes.⁸

1992-1993 Beginning with 1992, each preliminary analysis was transmitted to the responsible licensee for review and comment. As a result of comments received from reviews by the licensees,

Results

---

the NRC staff, and the NRC's independent contractor, credit for additional equipment and recovery procedures that were added by the plants was incorporated into the analyses of the precursors. Examples include the use of supplemental EDGs for station blackout mitigation, alternate systems for SG and RCS makeup, and venting in boiling-water reactors (BWRs). Appendix A of NUREG/CR-4674, Vol. 17, documents the changes incorporated over the years.¹²

1994–present The use of plant-class event trees and linked plant-specific fault trees in precursor analyses began in 1994. The use of linked fault trees allows the impact of individual component failures to be more correctly addressed; this could only be approximated in the earlier models. In addition, the method for calculating the probability for condition assessments (events in which components are unavailable for a period of time during which the initiating event could have occurred) was modified. Additional discussion concerning the current analysis methods is given in Appendix A.

Because of the differences in analysis methods, only limited observations are provided here. Refer to the 1982–1983 precursor report³ for a discussion of observations for 1982–1983 results, the 1986 precursor report⁶ for a discussion of observations for 1984–1986 results, and to the 1987–1996 reports⁷⁻¹⁶ for the results of those years.

3.1 Tabulation of Precursors

The 1997 accident sequence precursors are listed in Tables 3.1–3.4. The following information is included on each table:

- Docket/LER number associated with the precursor (Event Identifier)
- Name of the plant where the precursor occurred (Plant)
- A brief description of the precursor (Description)
- Conditional probability of potential core damage associated with the precursor (CCDP)
- Date(s) of the precursor (Event Date)
- Plant type (Plant Type)
- Initiator associated with the precursor or unavailability if no initiator was involved (TRANS)

The tables are sorted as follows:

- Table 3.1 - At-power precursors involving initiating events sorted by plant
- Table 3.2 - At-power precursors involving unavailabilities sorted by plant
- Table 3.3 - At-power precursors involving initiating events sorted by CCDP
- Table 3.4 - At-power precursors involving unavailabilities sorted by importance

3.1.1 Potentially Significant Events That Were Impractical to Analyze

Two potentially significant events were considered impractical to analyze for 1997 (Table 3.5). Typically, this event category includes events that are impractical to analyze because of lack of information or inability to reasonably model the event within a PRA framework, considering the level of detail typically available

Table 3.1 At-Power Precursors Involving Initiating Events Sorted by Plant

Plant	Event identifier	Description	Plant type	Event date	CCDP	Event type
Oconee 2	LER 270/97-001	Unisolable RCS leak	PWR	4/21/97	2.2×10^{-5}	LOCA
TMI 1	LERs 289/97-007, -008, -010	Failure of both generator output breakers causes a LOOP	PWR	6/21/97	9.6×10^{-6}	LOOP

Table 3.2 At-Power Precursors Involving Unavailabilities Sorted by Plant

Plant	Event identifier	Description	Plant type	Event date	CCDP	Importance (CCDP - CDP)	Event type
Oconee 3	LER 287/97-003	Two HPI pumps were damaged because of a low water level in the letdown storage tank (LDST)	PWR	5/3/97	5.4×10^{-6}	4.3×10^{-6}	Unavailability
Maine Yankee	LER 309/97-004	RCS hot-leg recirculation valves subject to pressure locking because of post-LOCA thermal expansion of the trapped water	PWR	1/22/97	8.2×10^{-5}	1.3×10^{-5}	Unavailability
St. Lucie 1	LER 335/97-011	Nonconservative recirculation actuation signal (RAS) set point	PWR	11/2/97	3.4×10^{-5}	1.7×10^{-5}	Unavailability

Results

Table 3.3 At-Power Precursors Involving Initiating Events Sorted by CCDP

CCDP	Plant	Plant type	Event identifier	Description	Event date	Event type
2.2×10^{-5}	Oconee 2	PWR	LER 270/97-001	Unisolable RCS leak	4/21/97	LOCA
9.6×10^{-6}	TMI 1	PWR	LERs 289/97-007, -008, -010	Failure of both generator output breakers causes a LOOP	6/21/97	LOOP

Table 3.4 At-Power Precursors Involving Unavailabilities Sorted by Importance

Importance (CCDP - CDP)	CCDP	Plant	Plant type	Event identifier	Description	Event date	Event type
1.3×10^{-5}	8.2×10^{-5}	Maine Yankee	PWR	LER 309/97-004	RCS hot-leg recirculation valves subject to pressure locking because of post-LOCA thermal expansion of the trapped water	1/22/97	Unavailability
4.3×10^{-6}	5.4×10^{-6}	Oconee 3	PWR	LER 287/97-003	Two HPI pumps were damaged because of a low water level in the LDST	5/3/97	Unavailability
1.7×10^{-6}	3.4×10^{-5}	St. Lucie 1	PWR	LER 335/97-011	Non-conservative RAS set point	11/2/97	Unavailability

Table 3.5 Potentially Significant Events Considered Impractical to Analyze

Plant	Event description
Millstone 2	Nine of 89 containment penetrations are susceptible to thermally induced overpressurization
Millstone 2	The maximum allowable peak fuel element cladding temperature may be exceeded during a LOCA

3.1.2 Containment-Related Events

No containment-related events were identified for 1997. 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 the basis for events to be considered containment-related is given in Appendix E.

3.1.3 "Interesting" Events

Five "interesting" events were identified for 1997 (Table 3.6). This event category includes events that were not selected as precursors but that provided insight into unusual failure modes with the potential to compromise continued core cooling. Descriptions of these events are located in Appendix F.

Table 3.6 Index of "Interesting" Events

Plant	Event description
Oyster Creek	Generator exciter fire results in partial LOOP
Indian Point 2	A fault in a unit auxiliary transformer protective relay causes a loss of generator load
Pilgrim 1	LOOP occurs during shutdown
FitzPatrick	Fouling of the circulating water system traveling screens
Clinton	Normal power supply breaker for safety bus fails to open

3.2 Number of Precursors Identified

Five precursors with a CCDP greater than 1.0×10^{-6} affecting five units were identified in 1997 (i.e., none of the precursors that occurred at multiunit sites affected more than one unit). The distribution of precursors as a function of CCDP for 1987 through 1997 is shown in Table 3.7 and in Figs. 3.1–3.4.

Results

Table 3.7 Number of Precursors by Year

Year ^a	No. of reactor years ^b	$10^{-3} \leq \text{CCDP} < 1$	$10^{-4} \leq \text{CCDP} \leq 10^{-3}$	$10^{-5} \leq \text{CCDP} \leq 10^{-4}$	$10^{-6} \leq \text{CCDP} \leq 10^{-5}$	Total no. of precursors
1987	102.7	0	10	9	14	33
1988	107.1	0	7	14	11	32
1989	109.0	0	7	11	12	30
1990	110.5	0	6	11	11	28
1991	111.0	1	12	8	6	27
1992	110.4	0	7	7	13	27
1993	108.7	0	4	7	5	16
1994	109.0	1	1	4	3	9
1995	109.0	0	1	7	2	10
1996 ^c	110.1	1	2	4	7	14
1997	106.1	0	0	2	3	5

^aIn 1988, the ASP Program began using computerized searches to identify LERs that meet minimum selection criteria, revised the LOOP recovery model, and explicitly modeled PWR seal LOCA sequences. In 1992, additional equipment and procedures were incorporated into the plant models. In 1994, the project began using plant-class event trees and plant-specific fault trees. Consequently, a direct comparison of results is not possible without substantial effort to reconcile analysis differences.

^bThe number of reactor years, which is based on the total number of operating hours, dropped in 1997 because a number of plants shut down permanently during the year.

^cThe measure of significance for the unavailability assessments is the importance (see Sect. 2.2).

As described previously, differences in the ASP models and the analysis methods from year to year preclude a direct comparison between the number of precursors identified for different calendar years. In particular, the CCDPs estimated for some 1992–1997 precursors are lower than for equivalent precursors in earlier years because supplemental and plant-specific mitigating systems beyond those included in the pre-1992 ASP models were incorporated into the analyses. In addition, new modeling techniques were adopted for the analysis of the 1994–1997 precursors (e.g., plant-specific fault trees).

3.3 Important Precursors

Precursors with CCDPs $\geq 10^{-4}$ have traditionally been considered important in the ASP Program. For the first time in the history of the ASP Program, no precursors with a CCDP $\geq 10^{-4}$ were identified.

Fig. 3.2. CCDP results by year for 10^{-5} to 10^{-4} . Fig. 3.4. CCDP results by year for 10^{-3} to 1.0. Fig. 3.1. CCDP results by year for 10^{-6} to 10^{-5} . Fig. 3.3. CCDP results by year for 10^{-4} to 10^{-3} .

Results

3.4 Insights

The number of 1997 precursors involving initiators and unavailabilities of equipment is given in Table 3.8.

Table 3.8 Number of Precursors by Event Type

Event category	$10^{-3} \leq \text{CCDP} < 1$	$10^{-4} \leq \text{CCDP} \leq 10^{-3}$	$10^{-5} \leq \text{CCDP} \leq 10^{-4}$	$10^{-6} \leq \text{CCDP} \leq 10^{-5}$	Total
At-power unavailabilities			2	1	3
At-power initiators			1	1	2

A review of the analyses for all five precursors for 1997 and a comparison with analyses for previous years revealed the following insights and trends.

1. Most of the precursors are consistent with the failure combinations identified in PRAs/IPEs. A review of the last several years (1994–1997) shows that several precursors involved event initiators or conditions not typically modeled in PRAs or IPEs (Table 3.9).

Table 3.9 Precursors not Typically Modeled in PRAs or IPEs

Year	Plant(s)	Event description
1994	Wolf Creek	Blowdown of the RCS to the refueling water storage tank during hot shutdown
1996	Wolf Creek	Reactor trip with the loss of one train of emergency service water due to the formation of frazil ice on the circulating water traveling screens and the unavailability of the turbine-driven auxiliary feedwater (AFW) pump
1996	LaSalle 1 and 2	Fouling of the cooling water systems due to concrete sealant injected into the service water tunnel
1996	Haddam Neck	Inadequate residual heat removal pump net positive suction head following a large- or medium-break LOCA

2. Historically, the percentage of precursors is evenly split between initiating events and unavailabilities (Fig. 3.5). The initiating events of interest include LOOPs, LOFW events, LOCAs, SGTRs, and general plant transients. An example of an initiating event is an actual LOOP event with complications. Unavailability events involve a system or component being inoperable, typically for a long time. An example unavailability event would be the long-term unavailability of an EDG. General transients contribute ~75% to all initiating events.

Fig. 3.5 Percentage of precursors resulting from unavailabilities.

Results

3. For the first time in the history of the ASP Program, no important precursors (i.e., those with a $CCDP \geq 10^{-4}$) were identified. This compares with the ~25% precursors over the last 10 years considered to be important. In addition, precursors with a $CCDP \geq 10^{-3}$ occur rather infrequently and are unique events (i.e., no pattern for where, what, why, or how they occur) (Fig. 3.6). Those precursors with a $CCDP \geq 10^{-3}$ that have occurred since 1987 are listed in Table 3.10.

Fig. 3.6 Percentage of important precursors by year.

Table 3.10 Precursors with a $CCDP \geq 10^{-3}$

Year	Plant	Description
1991	Harris 1	High-head safety injection unavailable
1994	Wolf Creek	Blowdown of the RCS during hot shutdown
1996	Catawba 2	LOOP with one EDG unavailable

4. Historically, the number of precursors occurring at BWRs has been less than the percentage of BWRs in operation (Fig. 3.7). In the last several years, the percentage of precursors occurring at BWRs appears to be decreasing. For the first time in the history of the ASP Program, none of the precursors occurred at a BWR. NUREG-1560 (Ref. 22) indicates that BWR core damage frequencies estimated in the IPEs were less than the frequencies estimated for PWRs in most cases. This difference was attributed to the larger number of injection systems and the capability to more easily depressurize to allow use of low-pressure injection systems. The greater protection against core damage afforded by these plant features may explain, in part, the smaller number of BWR precursors than would be indicated by the fraction of units that are BWRs. For 1997, the fraction of operational events selected for detailed analysis that occurred at BWRs was also less (22%) than the fraction of units that are BWRs (38%). The reason for this has not been explored.

Fig. 3.7 Percentage of precursors occurring at BWRs.

Results

5. Eighty percent (4 out of 5) of the 1997 precursors occurred at multiunit sites (Fig. 3.8). The 10-year average for percentage of precursors at multiunit sites is 69%. The percentage of units located at multiunit sites is about 71%. Therefore, there does not appear to be any benefit or detriment associated with a multiunit site with respect to the overall occurrence rate of precursors.

Fig. 3.8 Percentage of precursors at multiunit sites.

6. Precursors involving the degradation of AFW/emergency feedwater (EFW) are typically large contributors to the number of precursors. None of the 1997 precursors, however, involved problems with AFW/EFW, either demand-related or long-term unavailabilities. (Long-term unavailabilities are infrequently observed and are typically discovered during testing.) This is the first time in the history of the ASP Program that none of the precursors involved any type of AFW or EFW problems. Fig. 3.9 shows the number of AFW and EFW-related precursors associated with unexpected demands. (Although not shown, one event in 1994 involved the potential unavailability of AFW at Zion.) Fig. 3.9 excludes, for example, a limited number of precursors identified during testing. It also shows the fitted trend with the associated uncertainty bounds on the mean value. The decreasing trend is statistically significant (p -value = 0.0001). The trend was estimated using a log-linear model (Ref. 23) and reactor years as an independent variable. The trend is still statistically significant (p -value = 0.037) when only the 1990 through 1997 data are considered. The decrease in the number of AFW-related precursors is primarily the result of the decrease in the number of unexpected AFW system demands in the later years of the time period.

Fig. 3.9 Number of AFW/EFW-related precursors.

Results

- Electric power-related events and conditions continue to be a significant fraction of the precursors (one of the five 1997 precursors involved problems with electrical equipment). This is less than in previous years (1993–1995), for which about 60% of the precursors involved electric-power-related issues (Fig. 3.10).

Fig. 3.10 Percentage of electric-power-related precursors.

8. Of the four LOOP events that occurred in 1997, only one was classified as a precursor (Fig. 3.11). This was a plant-centered LOOP at Three Mile Island, Unit 1, and was caused by the failure of both generator output breakers. (Another LOOP, which occurred at Pilgrim, was classified as an "interesting" event, and is discussed in Appendix F.4; the other two occurred at Indian Point 3 and at Browns Ferry 3. Both of latter two events were of relatively short duration and no complications were encountered in restoring offsite power. Consequently, the CCDP associated with each event did not exceed the precursor threshold, and neither met the criteria for an "interesting" event.) It should be noted that the LOOP recovery models were revised in 1988 and that credit for supplemental EDGs for station blackout mitigation was added in 1992. Interestingly, four LOOP events occurred in 1993 and 1996, while none occurred in 1994 and 1995. The last dual-unit LOOP was in 1996 (at Prairie Island). Plant-centered LOOPS are the most frequent and are typically caused by equipment faults and, to a lesser extent, human errors. Severe weather-related LOOPS have the longest duration. An extreme example is the weather-induced LOOP caused by Hurricane Andrew in 1992 at Turkey Point 3 and 4 that lasted over 6.5 days. Grid-based LOOPS are rare—the last grid-based LOOP event occurred in 1989 at Summer and lasted 1 h and 35 min.

Fig. 3.11 Number of LOOP-related precursors per year.

Results

9. The total number of precursors identified for 1997 is the lowest for the last 10 years (1987–1996) (Fig. 3.12). In fact, this is the lowest number of precursors since 1970. Some of this downward trend is because of the differences in the ASP analysis approach, including sending the preliminary analyses to the licensees for review and comment, which helped identify additional equipment and procedures available for mitigating the event (1992); and using plant-class event trees (1984) and plant-specific fault trees, which facilitated modeling of alternate equipment that could be used for recovery (1994). Also contributing to this downward trend are the reduction in the number of safety system actuations and the number of automatic scrams; both have decreased by a factor of 4 over the last 10 years (Ref. 22). Reducing the number of transients (about 40% of the precursors) as well as the number of challenges to safety systems will directly affect the number of precursors. Another factor influencing the number of precursors is Generic Letter (GL) 88-20 (Ref. 23). GL 88-20 required all licensees to evaluate their plant(s) for vulnerabilities to severe accidents. Through this program, licensees could address the most important plant-specific vulnerabilities, thereby reducing plant risk (60% of the IPEs were submitted between August 1990 and December 1992).

Fig. 3.12 Total number of precursors by year.

3.5 Conclusion

The total number of precursors identified for 1997 is the lowest since 1970. Some of this downward trend is because of the differences in the ASP analysis approach. Also contributing to this downward trend are the reduction in the number of safety system actuations and the number of automatic scrams; both have decreased by a factor of 4 over the last 10 years. Another factor influencing the number of precursors is the IPE program that required all licensees to evaluate their plant(s) for vulnerabilities to severe accidents.

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. An 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.

Base probability. The nominal failure probability for the basic event and is given in the ASP linked event tree-fault tree model for the plant.

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

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 the ASP Program, 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 are 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 LOCA.

Glossary

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. Event trees are typically used to model potential plant response to an initiating event on a system or functional level.

Failure. The inability to perform 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 separately accounted for in the analysis.

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 fault tree is a graphical representation of the logical combinations of basic events that can lead to an undesired event, such as a system failure.

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.

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 with those initiating events that could lead to severe core damage.

Licensee event reports. Those reports described in 10 CFR 50.73 and submitted to NRC by utilities who operate nuclear plants. LERs describe abnormal operating occurrences that generally involve violations of the plants' 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 10 CFR 50.73 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.

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 (ORNL/NSIC-182/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. A. Forester, J. W. Minarick, H. K. Schriener, B. W. Dolan, D. B. Mitchell, D. W. Whitehead, and J. J. Jansen, Sandia Natl. Lab. and Science Applications International Corp., *Precursors to Potential Severe Core Damage Accidents: 1982-83, A Status Report*, USNRC Report NUREG/CR-4674, Vol. 24 (SAND97-0807), April 1997.*
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: 1985, A Status Report*, USNRC Report NUREG/CR-4674 (ORNL/NOAC-232, Vols. 1 and 2), December 1986.*
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: 1986, A Status Report*, USNRC Report NUREG/CR-4674 (ORNL/NOAC-232, Vols. 5 and 6), May 1988.*
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: 1987, A Status Report*, USNRC Report NUREG/CR-4674 (ORNL/NOAC-232, Vols. 7 and 8), July 1989.*
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: 1988, A Status Report*, USNRC Report NUREG/CR-4674 (ORNL/NOAC-232, Vols. 9 and 10), February 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: 1989, A Status Report*, USNRC Report NUREG/CR-4674 (ORNL/NOAC-232, Vols. 11 and 12), August 1990.*
10. 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*

References

- Accidents: 1990, A Status Report*, USNRC Report NUREG/CR-4674 (ORNL/NOAC-232, Vols. 13 and 14), August 1991.*
11. 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), Sept. 1992.*
  12. 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.*
  13. L. N. Vanden Heuvel, J. W. Cletcher, D. A. Copinger, J. W. Minarick, and B. W. Dolan, 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.
  14. R. J. Belles, J. W. Cletcher, D. A. Copinger, B. W. Dolan, J. W. Minarick, and L. N. Vanden Heuvel, Lockheed Martin Energy Systems, Inc., Oak Ridge Natl. Lab.; and Science Applications International Corp., *Precursors to Potential Severe Core Damage Accidents: 1994, A Status Report*, USNRC Report NUREG/CR-4674 (ORNL/NOAC-232, Vols. 21 and 22), December 1995.
  15. R. J. Belles, J. W. Cletcher, D. A. Copinger, B. W. Dolan, J. W. Minarick, and M. D. Muhlheim, Lockheed Martin Energy Research, Inc., Oak Ridge Natl. Lab.; and Science Applications International Corp., *Precursors to Potential Severe Core Damage Accidents: 1995, A Status Report*, USNRC Report NUREG/CR-4674 (ORNL/NOAC-232), Vol. 23, April 1997.
  16. R. J. Belles, J. W. Cletcher, D. A. Copinger, B. W. Dolan, J. W. Minarick, and M. D. Muhlheim, Lockheed Martin Energy Research, Inc., Oak Ridge Natl. Lab.; and Science Applications International Corp., *Precursors to Potential Severe Core Damage Accidents: 1996, A Status Report*, USNRC Report NUREG/CR-4674 (ORNL/NOAC-232), Vol. 25, December 1997.
  17. U.S. Nuclear Regulatory Commission, *Licensee Event Report System, Description of System and Guidelines for Reporting*, USNRC Report NUREG-1022, September 1983.*
  18. U.S. Nuclear Regulatory Commission, *Licensee Event Report System, Description of System and Guidelines for Reporting*, USNRC Report NUREG-1022, Supplement 1, February 1984.*
  19. U.S. Nuclear Regulatory Commission, *Licensee Event Report System, Evaluation of First Year Results, and Recommendations for Improvements*, USNRC Report NUREG-1022, Supplement 2, September 1985.*
  20. U.S. Nuclear Regulatory Commission, *Risk Assessment Review Group Report*, USNRC Report NUREG/CR-0400, September 1978.*

21. 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.*
22. *Individual Plant Examination Program: Perspectives on Reactor Safety and Plant Performance*, USNRC Report NUREG-1560, December 1997.
23. J. P. Poloski et al., *Reliability Study: Auxiliary/Emergency Feedwater System, 1987-1995*, USNRC Report NUREG/CR-5500, Vol. 1, August 1998.
24. A. Mosleh and R. A. Bari, *Probabilistic Safety Assessment and Management (PSAM 4): Proceedings of the 4th International Conference on Probabilistic Safety Assessment and Management, 13-18 September 1998, New York City, USA*, Springer, 1998.
25. Generic Letter 88-20, "Individual Plant Examination for Severe Accident Vulnerabilities -10 CFR 50.54(f)."

---

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

Appendix A:
ASP Computational 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 Chap. 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.

Quantifying the significance of the events identified as precursors involves determining a conditional probability of subsequent core damage given the failures and other undesirable conditions (such as an initiating event or an unexpected relief valve challenge) that were 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 then translating the results of the review into a revised model for the plant that reflects the observed failures. The precursor's significance is then estimated by calculating a conditional probability of core damage given the observed failures. The probabilities of components observed to operate successfully or that were not challenged during the event are not modified. 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 1997 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 Ref. 1. The current ASP models are described in NUREG/CR-4674, Vol. 21 (i.e., the ASP Program's 1994 status report). 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 (SLOCA) 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 occurred, 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 a probability of 1.0 is used for the observed initiating event, 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. Each basic event typically 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 the failure of an operator to perform a required 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 can be 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.^a

In addition to revising the basic events associated with failed components, basic events related to the common-cause failure of similar components may also have to be revised to reflect the observed failures. If the failure could also have occurred in other similar components at the same time, then the common-cause failure probability is increased to represent this likelihood. If the failure could not simultaneously occur in other components (e.g., if a component was removed from service for preventive maintenance), then the common-cause failure probability is also revised, but only to reflect the "removal" of the unavailable component from the model. The Multiple Greek Letter (MGL) method is used to quantify the common-cause failure basic events (see Ref. 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 setting basic events impacted by the failure to "failed" (logical state "true"). 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."

---

^aPractical considerations in the solution of large linked fault trees, primarily the use of the Delete Term 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.

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

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 Ref. 4. The probability of in-control room operator error is described using a lognormal 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

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 outside the control room considers the time available for response and the nature of the failures (which prescribe the repair time).

Note that the actual likelihood of failing to recover from an event at a particular plant is difficult to assess and may vary substantially from values estimated using this approach. 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 previously 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.

Several simplified examples that illustrate the basics of the precursor calculational process follow. The intent of the examples is not to describe a detailed precursor analysis, but instead to provide a basic understanding of the process. The examples are presented in terms of event tree 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 Fig. A.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, the up branch represents success, and the down branch represents failure for each of the systems. (In an accident sequence model for an actual 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 ("I" 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 frequency of initiating event I, $\lambda(I)$ and the failure probabilities for A, B, C, and D [$p(A)$, $p(B)$, $p(C)$, and $p(D)$]. Assuming $\lambda(I) = 0.1 \text{ yr}^{-1}$ and $p(A|I) = 0.003$, $p(B|IA)^a = 0.01$, $p(C|I) = 0.05$, and $p(D|IC) = 0.1$, the frequency of core damage is determined by calculating the frequency of each of the three core damage sequences and adding the frequencies:

$$\begin{aligned}
 &0.1 \text{ yr}^{-1} \times (1 - 0.003) \times 0.05 \times 0.1 \text{ (sequence 3)} + \\
 &0.1 \text{ yr}^{-1} \times 0.003 \times (1 - 0.01) \times 0.05 \times 0.1 \text{ (sequence 6)} + \\
 &0.1 \text{ yr}^{-1} \times 0.003 \times 0.01 \text{ (sequence 7)} \\
 &= 4.99 \times 10^{-4} \text{ yr}^{-1} \text{ (sequence 3)} + 1.49 \times 10^{-5} \text{ yr}^{-1} \text{ (sequence 6)} + 3.00 \times 10^{-6} \text{ yr}^{-1} \text{ (sequence 7)} \\
 &= 5.03 \times 10^{-4} \text{ yr}^{-1}.
 \end{aligned}$$

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 previously and cannot be directly compared with it.

^aThe notation $P(B|IA)$ means the probability that B fails, given I occurred and A failed.

Table A.1. Rules for Precursor Calculation

<i>Event sequences requiring calculation.</i> 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 condition.
<i>Initiating event probability.</i> 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 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.
<i>Component failure probability estimation.</i> 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 that are not challenged during the event, a failure probability equal to the nominal component failure probability is utilized.
<i>Nonrecovery probability.</i> If an initiating event or a total system failure occurred as a part of the precursor, then 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.
<i>Failures in support systems.</i> 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. Such failures can be modeled through multiple calculations that address the impact of failure and success of the failed support system components. 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 included in the current ASP models.)

A.5.1 Example 1: Initiating Event Assessment

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

$$\begin{aligned}
 &1.0 \times (1 - 0.003) \times 0.05 \times 0.1 \text{ (sequence 3)} + \\
 &1.0 \times 0.003 \times (1 - 0.01) \times 0.05 \times 0.1 \text{ (sequence 6)} + \\
 &1.0 \times 0.003 \times 0.01 \text{ (sequence 7)} \\
 &= 5.03 \times 10^{-3}.
 \end{aligned}$$

If instead B was determined to have been failed at the time of initiating event I, its probability would have been set to 1.0. The conditional core damage probability for precursor IB would be calculated as

$$1.0 \times (1 - 0.003) \times 0.05 \times 0.1 \text{ (sequence 3)} + 1.0 \times 0.003 \times 1.0 \text{ (sequence 7)} = 7.99 \times 10^{-3}.$$

Because B is failed, sequence 6 cannot occur.

Fig. A.1 Hypothetical core damage model.

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 if the plant is at power for 70% of a year, then the frequency for I is estimated to be $0.1 \text{ yr}^{-1} / (8760 \text{ h/yr} \times 0.7) = 1.63 \times 10^{-5} \text{ h}^{-1}$.

The expected number of core damage sequences in the 360-h period is

$$\begin{aligned} &1.63 \times 10^{-5} \text{ h}^{-1} \times 360 \text{ h} \times (1 - 0.003) \times 0.05 \times 0.1 \text{ (sequence 3)} + \\ &1.63 \times 10^{-5} \text{ h}^{-1} \times 360 \text{ h} \times 0.003 \times 1.0 \text{ (sequence 7)} \\ &= 4.69 \times 10^{-5}, \end{aligned}$$

and the probability of at least one core damage sequence is^a

$$1 - e^{-4.69 \times 10^{-5}} = 4.69 \times 10^{-5}.$$

As before, because 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 2.93×10^{-5} . This sequence is unrelated to the failure of B. The potential failure of systems C and D over the 360-h period still drives 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 (see Ref. 5). In this calculation, the increase in core damage probability over the 360-h period because of the failure of B is estimated:

$$p(\text{cd} | \text{B}) - p(\text{cd}) = \Delta \text{CDP}.$$

In this example the value is

$$4.69 \times 10^{-5} - 2.95 \times 10^{-5} = 1.74 \times 10^{-5},$$

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 previously referred to as the conditional core damage probability (CCDP) in 1993 and earlier annual precursor reports. For most conditions identified as precursors in the ASP Program, its value and the CCDP are numerically close, and

---

^aNote that this calculation assumes that failures are only detected when core damage occurs. This calculational approach, adopted in 1995, differs from previous years when it was assumed that a failed component would be detected when the first initiating event occurred. The current approach may overestimate the core damage probability for a long-duration condition that would be detected at the time of the initiating event, but has little impact on most analyses. (The earlier approach could underestimate the event significance for failures that would remain undetected following a nominal initiating event.)

the CCDP 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 CCDP can be significantly higher than the importance. 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 CCDP and the importance of the event.

A.6 References

1. *PRA Procedures Guide*, USNRC Report, NUREG/CR-2300, January 1983, Section 6.3.2.
2. *Systems Analysis Programs for Hands-on Integrated Reliability Evaluations (SAPHIRE) Version 5.0*, USNRC Report, NUREG/CR-6116, Vols. 1–10.
3. *Procedures for Treating Common-Cause Failures in Safety and Reliability Studies*, USNRC Report, 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*, USNRC Report, NUREG/CR-3385, July 1983.

Appendix B:
At-Power Precursors for 1997

B.1 At-Power Precursors

B.1.1 Accident Sequence Precursor Program Event Analyses for 1997

This appendix documents 1997 operational events selected as 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 data base maintained at the Nuclear Operations Analysis Center (NOAC), 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 Appendix A of this report.

B.1.2 Precursors Identified

Five precursors were identified among the 1997 events reviewed at the NOAC. Events were identified as precursors if they met one of the following precursor selection criteria and the conditional core damage probability (CCDP) 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 (LOOP) or small-break loss-of-coolant accident (SLOCA), or
4. the event involved a reactor trip or loss-of-feedwater with a degraded safety system.

The precursors identified are listed in Table B.1.

Table B.1 List of 1997 Precursors

Event Number	Plant	Event descriptions	Page
LER 270/97-001	Oconee 2	Unisolable reactor coolant system leak	B.2-1
LER 287/97-003	Oconee 3	Two high-pressure injection pumps were damaged because of a low water level in the letdown storage tank	B.3-1
LER 289/97-007, -008, and -010	TMI 1	Failure of both generator output breakers causes a LOOP	B.4-1
LER 309/97-004	Maine Yankee	Reactor coolant system hot-leg recirculation valves subject to pressure locking because of post-LOCA thermal expansion of the trapped water	B.5-1
LER 335/97-011	St. Lucie 1	Nonconservative recirculation actuation signal set point	B.6-1

B.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 sheet provides a description of the operational event, event-related plant design information, 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. This includes 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.

B.2 LER No. 270/97-001

Event Description: Unisolable reactor coolant system leak

Date of Event: April 21, 1997

Plant: Oconee 2

B.2.1 Event Summary

An unisolable 45.4 L/min (12-gal/min) leak developed in the reactor coolant system (RCS), high-pressure injection (HPI) nozzle, safe end-to-piping weld downstream of reactor coolant pump (RCP) 2A1 (Ref. 1). Unit 2 was shut down, and personnel removed and inspected the leaking pipe section. The leak was caused by a circumferential crack with through-wall penetration along 1.3 rad (77°) of the outer pipe surface. In addition, the nozzle thermal sleeve was loose and cracked, with portions missing from the end that extends into the RCS flow path. The piping failures were caused by high-cycle thermal fatigue that resulted from the mixing of makeup, warming, and RCS flows. The estimated conditional core damage probability (CCDP) associated with this event is 2.2×10^{-5} .

B.2.2 Event Description

At approximately 2245 on April 21, 1997, with Unit 2 at 100% power, changes were noted in the rate at which the water level in the letdown storage tank (LDST) was decreasing while the reactor building (RB) sump level was increasing. RB radiation monitor alarms followed. At 2300 the RCS leak rate was estimated to be 8.9 L/min (2.36 gal/min). Personnel entered the RB at 0215, determined that a leak did exist, but could not identify the source.

The shutdown of Unit 2 began at 0352, with the intention to reduce power to 15%. Because reducing the power level reduces the radiation levels in the RB, personnel could then perform a more detailed inspection of the leak area with the main turbine remaining on-line. At 0900, a more accurate leak rate calculation was performed with power stabilized at 20%. This calculation indicated that the leak rate had increased from 8.9 L/min (2.36 gal/min) at 2300 to 23.6 L/min (6.25 gal/min) at 0940. By 1048 it had increased above 30.3 L/min (8 gal/min).

At 1217, during another RB entry, the leak location was identified as being in the vicinity of 2HP-127, the block valve closest to the injection nozzle on the 2A1 RCP cold leg (Fig. B.2.1). The decision was made to proceed to cold shutdown. The turbine generator was taken off-line at 1250, and the reactor was tripped at 1448 on April 22, 1997. The leak rate peaked at approximately 45.4 L/min (12 gal/min) at 1750 and then began to decrease as RCS pressure was reduced as the shutdown continued.

The leak was found to be in an unisolable section of piping at the weld between the HPI piping and injection nozzle safe end. The unit was placed in a reduced inventory condition, and the pipe from the safe end to the block valve was cut out for examination (a temporary cap was then welded to the safe end, and the RCS water

level was raised). This examination determined that the leaking weld was caused by a 6.3 rad (360°) inside circumferential crack that penetrated, at a minimum, 24% of the pipe wall. The flaw depth increased and became through-wall over 1.3 rad (77°) of the outer circumference, as shown in Fig. B.2.2. The nozzle thermal sleeve was also found to be loose and cracked, with portions missing from the end that extends into the RCS flow. Cracking (~20% through-wall) was also found in the pipe in the vicinity of the warming line nozzle. Video examination, ultrasonic testing (UT), and radiographic testing (RT) of the welds and thermal sleeves in the other HPI nozzles showed no indications of cracking, loosening, or other signs of degradation.

The licensee concluded that the piping failures were caused by high-cycle thermal fatigue, as a result of thermal mixing of the warming line, makeup flow, and RCS flow. Thermal mixing occurred in the thermal sleeve, safe end, and piping because of varying operational conditions, including low makeup flow through the thermal sleeve. This caused cracking in the pipe, pipe-to-safe end weld, and safe end and contributed to the thermal sleeve failure. Vibration may have also contributed to the final failure once the crack was essentially through the pipe wall.

Following several earlier industry events involving cracked thermal sleeves and nozzle safe ends (described in the following section), Oconee adopted an augmented inspection plan to periodically check piping near the pipe-to-safe end welds (on Units 2 and 3) and the thermal sleeves (on all units). A review of the inspection schedules indicated that these inspections had been performed on Unit 2 in May 1996. However, the licensee determined that the inspection program failed to include UT of the piping near the pipe-to-safe end weld. Because of this, the weld that was cracked and leaking had not been inspected since 1982. The criteria for reviewing safe end radiographs were also poorly defined.

A reassessment of all radiographs of the thermal sleeves performed since 1983 determined that there had been no RT on the thermal sleeves at Unit 1 since 1989. However, a review of radiographs taken between 1983 and 1989 indicated no degradation of any of the thermal sleeves at Unit 1. Unit 1 was shut down on June 14, 1997, and its HPI nozzles and thermal sleeves were examined. The Oconee 1 thermal sleeves are of a different design, utilizing two concentric sleeves instead of the single sleeves used in the nozzles at Units 2 and 3. No unacceptable indications were found in the Unit 1 nozzles and sleeves.

Because the reassessment of Unit 3 radiographs indicated that the 3A1 thermal sleeve was potentially degraded, Unit 3 was shut down for inspection on May 1, 1997. Cladding cracks were found in the 3A1 thermal sleeve. UT of the other Unit 3 nozzles found no rejectable indications. Both the 2A1 and 3A1 nozzles were restored by installation of new safe ends, thermal sleeves, and associated piping.

B.2.3 Additional Event-Related Information

At Oconee, the HPI system provides both normal RCS makeup and RCP seal injection, as well as HPI for small-break loss-of-coolant accident (SLOCA) mitigation. During normal operation, the HPI system A header supplies makeup [typically 57–76 L/min (15–20 gal/min)] from the LDST through each of two lines to the RCS. These lines are equipped with “warming” lines that provide a minimum flow of 11.4 L/min (3 gal/min). The B HPI header is for emergency injection only and has no warming lines.

The injection lines terminate at injection nozzle assemblies located on each of the cold legs downstream of the RCPs. Each nozzle assembly (Fig. B.2.3) consists of an Inconel-clad carbon steel nozzle to which a stainless steel safe end is welded. The HPI piping is welded to the other end of the safe end. Inside the safe end is a stainless steel thermal sleeve, which extends into the RCS flow path. The function of the thermal sleeve is to minimize thermal shock and stresses on the nozzle by transporting the relatively cold HPI water [38 to 49°C (100 to 120°F)] into the main flow path. There it mixes with the 291°C (555°F) RCS cold-leg water. Without the thermal sleeve, the HPI water would directly contact the nozzle, resulting in unacceptable stresses in the nozzle material.

Additional information concerning this event is provided in NRC Information Notice 97-46 (Ref. 2). Problems similar to this event occurred in 1982 at Crystal River 3 and Oconee and in 1988 at Farley and Davis Besse. These events are described in NRC Information Notice 82-09 (Ref. 3), Generic Letter 85-20 (Ref. 4), and NRC Bulletin 88-08 (Ref. 5). Generic Letter 85-20 adopted recommended corrective actions developed by the Babcock and Wilcox (B&W) Owner's Group following the 1982 problems at Crystal River 3 and Oconee.

B.2.4 Modeling Assumptions

This event was modeled as a potential SLOCA at the 2A1 cold-leg HPI nozzle. In the actual event the pipe crack developed slowly and began to leak. This leakage was detected, and the plant was shut down while the injection line remained substantially intact. It is possible, however, that the crack could have developed differently, resulting in catastrophic failure of the injection line before detection.

The probability of such a "rupture before leak", which would result in a LOCA, was developed using service-based piping reliability data developed by the Swedish Nuclear Power Inspectorate (SKI).⁶ The probability of pipe rupture represents the likelihood that a defect could have progressed to a rupture. The conditional probability of an HPI line rupture was estimated using data related to thermal-fatigue-induced piping failures included in the recently developed SKI piping failure database.^{6,7} The SKI database currently includes over 2300 pipe failure records that represent about 4300 reactor-years of operating experience. For failures due to thermal fatigue, 20 cracks and leaks, but no ruptures, were observed in stainless steel piping 2.5 to 10 cm (1 to 4 in.) in diameter. Using Bayesian statistics with a noninformative prior^a, a conditional probability of rupture of 2.4×10^{-2} was estimated.^b Because no ruptures have been observed, this estimate may be conservative. However, several thermal fatigue-induced failures also included cyclic fatigue (vibration-induced fatigue) as a contributing factor (as noted in the Event Description, this may have been the case in

---

^aThe use of a noninformative prior is described on page 5-36 of the *PRA Procedures Guide*, NUREG/CR-2300, January 1983. A number of alternate estimators have been proposed for the case where no failures have been observed. See, for example, Section 5.5 of NUREG/CR-2300 and R. T. Bailey's article "Estimation from Zero-Failure Data" in *Risk Analysis*, Vol. 17, No. 3, June 1997.

^bAn alternative to the "data-driven" model that constitutes the SKI effort is the application of probabilistic fracture mechanics models. These models enable the calculation of failure probabilities assuming that piping is susceptible to anticipated degradation mechanisms especially those that develop over a long period. Reference 6 notes that under a similar set of boundary conditions, the two approaches tend to produce similar (i.e., the same order of magnitude) results.

this event as well). Among the 78 failures, 2 cyclic fatigue-related ruptures have been observed. This results in an estimated conditional probability of 3.2×10^{-2} , approximately the same as the 2.4×10^{-2} estimate for thermally induced fatigue. These values are consistent with the average number of piping failures that are ruptures as estimated in 1981 by Thomas (Ref. 8)^a and are about a factor of 4 smaller than the leak-before-break probability developed by the Electric Power Research Institute (EPRI) in 1992 (Ref. 9).^b

The strength of the HPI line piping and the proximity of the 2.5-cm (1-in.) warming line to the leaking weld would be expected to limit pipe movement and hence flow area, if a rupture had occurred (flow would also be limited by the thermal sleeve). This was reflected in the analysis by assuming that the potential break would be a SLOCA instead of the medium-break LOCA normally associated with a 6.4-cm (2.5-in.) break at Oconee.

Flow lost from an HPI line break is unavailable for RCS makeup. Orifices in each injection line provide for flow indication to allow the operators to redirect HPI flow between the two sets of injection lines so that a majority of the flow goes through the intact header into the RCS. The HPI system design also includes cross-connects to allow flow from the center HPI pump to be directed to the intact injection lines if the pump that normally supplies these lines (pump A in the case of a break in the 2A1 injection line) is unavailable. To address a potential HPI line break, the HPI and piggy-back cooling (high-pressure recirculation) fault trees were revised to require flow through the intact header in the event of such a break (a break in header A was modeled). In addition, the potential for the operators to realign pump B to inject through the B header was also added to the model.

The model was also revised to address use of rapid RCS depressurization and low-pressure injection (LPI) in the event that HPI were to fail. The Oconee *Individual Plant Examination* (IPE)¹⁰ states that the emergency operating procedures direct the operators to use secondary heat removal to depressurize the RCS until LPI flow is greater than 380 L/min (100 gal/min) per header. The probability of the operators failing to depressurize the RCS and initiating LPI was assumed to be 0.1, consistent with Ref. 10.

B.2.5 Analysis Results

The CCDP for a postulated SLOCA associated with the leaking 2A1 HPI nozzle weld is estimated to be 2.2×10^{-5} . The dominant sequence, sequence 3 in Fig. B.2.4, involves

- a postulated HPI line break (SLOCA) given the weld leak,
- successful reactor trip and secondary-side cooling,
- successful RCS depressurization to the decay heat removal (DHR) initiation pressure, and
- failure of DHR and piggy-back cooling.

---

^aReference 8 estimated that between 2 and 45% of piping failures were catastrophic, depending on the failure cause. On average, approximately 6% of all failures were estimated to be catastrophic. Unfortunately, piping failures caused by high-cycle fatigue were not separately enumerated. Three percent of low-cycle fatigue failures were estimated to be catastrophic, compared to 20% of vibration-related fatigue failures and 20% of failures associated with "thermal shock."

^bReference 9 estimated that the probability of break before leak varied from 0.09 to 0.11, depending on pipe size.

The dominant cut sets involve common-cause failures of the DHR heat exchangers and pumps.

Substantial uncertainty is associated with the CCDP estimated for this event, primarily because of uncertainty in the conditional probability of pipe rupture. In addition to the uncertainty related to zero-event data described in Modeling Assumptions, Ref. 6 describes, among others, the following sources of uncertainty: coverage and completeness of the SKI data collection effort, data aggregation and exposure time estimation issues, identification of appropriate reliability attributes (e.g., pipe diameter, piping material) and influence factors (such as design and operating practices), plant-to-plant differences, and in-plant differences. In one probabilistic fracture mechanics study^a cited in Ref. 6, a 3 orders of magnitude difference existed in the conditional rupture probability for leaking 100 to 800 mm pipe ($10^{-4} \leq p \leq 10^{-1}$), depending on (1) the material, (2) whether the crack was in the base metal, or (3) if the crack was in a weld (as it was for this event). For stainless steel, the conditional probability for weld cracks was about 2 orders of magnitude higher than for cracks in base metal.

Definitions and probabilities for selected basic events are shown in Table B.2.1. The conditional probabilities associated with the highest probability sequences are shown in Table B.2.2. Table B.2.3 lists the sequence logic associated with the sequences listed in Table B.2.2. Table B.2.4 describes the system names associated with the dominant sequences. Minimal cut sets associated with the dominant sequences are shown in Table B.2.5.

During the Unit 3 shutdown to inspect its HPI nozzles and thermal sleeves, two of its three HPI pumps were damaged when they were operated with inadequate net positive suction head (NPSH). This resulted from a drained reference leg in the LDST instrumentation. The impact of the HPI pump failures as well as the potential for a combined RCS leak and HPI pump failure are addressed in the analysis of LER 287/97-003.

B.2.6 References

1. Licensee Event Report 270/97-001, "Unisolable Reactor Coolant Leak due to Inadequate Surveillance Program," May 21, 1997.
2. NRC Information Notice 97-46, "Unisolable Crack in High-Pressure Injection Piping," July 9, 1997.
3. NRC Information Notice 82-09, "Cracking in Piping to Makeup Coolant Lines at B&W Plants," March 31, 1982.
4. NRC Generic Letter 85-20, "Resolution of Generic Issue 69: High Pressure Injection/Makeup Nozzle Cracking in Babcock and Wilcox Plants," November 11, 1985.
5. NRC Bulletin 88-08, "Thermal Stresses in Piping Connected to Reactor Coolant Systems," June 22, 1988 (and supplements 1-3 dated June 24, 1988, August 4, 1988, and April 11, 1989, respectively).

---

^aProbabilistic Pipe Fracture Evaluations for Leak-Rate Detection Applications, NUREG/CR-6004, 1995.

6. R. Nyman, D. Hegedus, B. Tomic, and B. Lydell, *Reliability of Piping System Components, Framework for Estimating Failure Parameters from Service Data*, SKI Report 97:26, December 1997.
7. Personal communication, B. Lydell (RSA Technologies) and J. Minarick (SAIC), September 25, 1997.
8. H. M. Thomas, "Pipe and Vessel Failure Probability," *Reliability Engineering*, 2:83 (1981).
9. *Pipe Failures in U.S. Commercial Nuclear Power Plants*, EPRI TR-100380, July 1992.
10. Duke Power Company, *Oconee Nuclear Station IPE Submittal Report*, December 1990, p. 5.7-22, Rev 1.

Fig. B.2.1. Flow diagram of the emergency core cooling system at Oconee 2 (Source: Oconee 2 Final Safety Analysis Report).

Fig. B.2.2. Through-wall flow depth in pipe at Oconee 2 (Source: NRC Information Notice 97-46, "Unisolable Crack in High-Pressure Injection Piping," July 9, 1997). (TW is through-wall, OD is outside diameter, M/U flow is makeup flow, and RCS is reactor coolant system.)

Fig. B.2.3. Thermal sleeve 2A1, 2B1, 3A1, 3B1, and 3B2 (Source: NRC Information Notice 97-46, "Unisolable Crack in High-Pressure Injection Piping," July 9, 1997). (S.S. is stainless steel, C.S. is carbon steel, and SW is socket weld.)

Fig. B.2.4. Dominant core damage sequence for LER No. 270/97-001.

Table B.2.1. Definitions and Probabilities for Selected Basic Events for LER No. 270/97-001

Event name	Description	Base probability	Current probability	Type	Modified for this event
IE-LOOP	Initiating Event-Loss of Offsite Power	3.8 E-006	0.0 E+000		Yes
IE-MLOCA	Initiating Event-Medium Loss-of-Coolant Accident	8.2 E-008	0.0 E+000		Yes
IE-SGTR	Initiating Event-Steam Generator Tube Rupture	1.3 E-006	0.0 E+000		Yes
IE-SLOCA	Initiating Event-SLOCA	6.5 E-007	2.4 E-002		Yes
IE-TRANS	Initiating Event-Transient	7.8 E-004	0.0 E+000		Yes
DHR-HTX-CF-ALL	Common-Cause Failure (CCF) of the DHR Heat Exchangers	5.2 E-004	5.2 E-004		No
DHR-MDP-CF-ALL	CCF of all Motor-Driven DHR Pumps	2.1 E-004	2.1 E-004		No
DHR-MOV-CC-SUCA	DHR Suction Motor-Operated Valves (MOVs) LP-1 or LP-2 Fail	6.0 E-003	6.0 E-003		No
HPI-LINE-BREAK	Line Break in HPI Loop A	0.0 E+000	1.0 E+000	TRUE	Yes
HPI-MDP-CF-ABC	CCF (to Run) of the Motor-Driven HPI Pumps	6.1 E-006	6.1 E-006		No
HPI-MDP-CF-START	CCF (to Start) of the Motor-Driven HPI Pumps B and C	1.9 E-004	1.9 E-004		No
HPI-MDP-FC-B	HPI Train B Fails	3.9 E-003	3.9 E-003		No
HPI-MDP-FC-C	HPI Train C Fails	3.9 E-003	3.9 E-003		No
HPI-MOV-CC-409	HPI MOV HP409 Fails to Open	3.0 E-003	3.0 E-003		No
HPI-MOV-CC-SUCA	Isolation Valve in HPI Water Supply Path A Fails	4.2 E-003	4.2 E-003		No
HPI-MOV-CC-SUCB	Isolation Valve in HPI Water Supply Path B Fails	4.2 E-003	4.2 E-003		No
HPI-MOV-CF-SUCT	CCF of HPI Suction Isolation MOVs	2.1 E-004	2.1 E-004		No

**Table B.2.1. Definitions and Probabilities for Selected Basic Events for
LER No. 270/97-001 (Continued)**

Event name	Description	Base probability	Current probability	Type	Modified for this event
HPI-MOV-OO-115	MOV HP115 Fails to Close	3.0 E-003	3.0 E-003		No
HPR-MOV-CF-BWST	CCF of Isolation MOVs for the Borated Water Storage Tank (BWST)	7.7 E-005	7.7 E-005		No
LDST-LVL-LOW	Low Water Level in the LDST Fails the HPI Pumps	4.4 E-003	4.4 E-003		No
LPR-MOV-CF-BWST	CCF of BWST Isolation MOVs	8.6 E-005	8.6 E-005		No
LPR-SMP-FC-SUMP	Failures in the RB Sump	5.0 E-005	5.0 E-005		No
PBC-XHE-XM	Operator Fails to Initiate Piggy-Back Cooling	2.2 E-003	2.2 E-003		No
PCS-VCF-HW	Hardware Failures in the Secondary Systems	3.0 E-003	3.0 E-003		No
PCS-XHE-XM-CDOWN	Operator Fails to Initiate Cooldown	1.0 E-002	1.0 E-002		No
PCS-XHE-XM-FDEPR	Operator Fails to Initiate a Fast Depressurization for LPI	1.0 E-001	1.0 E-001		No

Table B.2.2. Sequence Conditional Probabilities for LER 270/97-001

Event tree name	Sequence number	Conditional core damage probability (CCDP)	Percent contribution
SLOCA	03	1.8 E-005	85.6
SLOCA	15	1.2 E-006	5.5
SLOCA	05	1.1 E-006	5.2
SLOCA	10	4.2 E-007	2.0
Total (all sequences)		2.2 E-005	

Table B.2.3. Sequence Logic for Dominant Sequences for LER 270/97-001

Event tree name	Sequence number	Logic
SLOCA	03	/RT, /EFW, /HPI, /COOLDOWN, DHR, PB-COOL
SLOCA	15	/RT, /EFW, HPI, FASTDEPR
SLOCA	05	/RT, /EFW, /HPI, COOLDOWN, /HPI-LATE, PB-COOL
SLOCA	10	/RT, /EFW, /HPI, COOLDOWN, HPI-LATE, FASTDEPR

Table B.2.4. System names for LER 270/97-001

System name	Logic
COOLDOWN	RCS Cooldown to DHR Pressure Using Turbine Bypass Valves, etc.
DHR	No or Insufficient Flow from the DHR System
EFW	No or Insufficient Flow from the Emergency Feedwater System
FASTDEPR	RCS Rapid Cooldown/Depressurization to LPI Pressure Using Turbine Bypass Valves, etc. (HPI Failed)
HPI	No or Insufficient Flow from the HPI System
HPI-LATE	HPI Fails Late
PB-COOL	No or Insufficient Flow from Piggy-Back Cooling
RT	Reactor Fails to Trip During a Transient

Table B.2.5. Conditional Cut Sets for Higher Probability Sequences for LER No. 270/97-001

Cut set number	Percent contribution	CCDP ^a	Cut sets ^b
SLOCA Sequence 03		1.8 E-005	
1	67.8	1.3 E-005	DHR-HTX-CF-ALL ^c
2	27.4	5.0 E-006	DHR-MDP-CF-ALL
3	1.7	3.2 E-007	DHR-MOV-CC-SUCA, PBC-XHE-XM
SLOCA Sequence 15		1.2 E-006	
1	42.9	5.0 E-007	HPI-MOV-CF-SUCT, PCS-XHE-XM-FDEPR
2	38.8	4.6 E-007	HPI-LINE-BREAK, HPI-MDP-CF-START ^d , PCS-XHE-XM-FDEPR
3	3.6	4.3 E-008	HPI-MOV-CC-SUCA, HPI-MOV-CC-SUCB, PCS-XHE-XM-FDEPR
4	3.1	3.7 E-008	HPI-LINE-BREAK, HPI-MDP-FC-B, HPI-MDP-FC-C, PCS-XHE-XM-FDEPR
5	2.4	2.8 E-008	HPI-LINE-BREAK, HPI-MOV-CC-409, HPI-MDP-FC-C, PCS-XHE-XM-FDEPR
6	2.4	2.8 E-008	HPI-LINE-BREAK, HPI-MOV-OO-115, HPI-MDP-FC-C, PCS-XHE-XM-FDEPR
7	1.3	1.5 E-008	HPI-MOV-CF-SUCT, PCS-VCF-HW
8	1.3	1.5 E-008	HPI-MDP-CF-ABC, PCS-XHE-XM-FDEPR
9	1.2	1.4 E-008	HPI-LINE-BREAK, HPI-MDP-CF-START, PCS-VCF-HW
SLOCA Sequence 05		1.1 E-006	
1	47.4	5.3 E-007	PCS-XHE-XM-CDOWN, PBC-XHE-XM
2	14.2	1.6 E-007	PCS-VCF-HW, PBC-XHE-XM
3	11.2	1.3 E-007	PCS-XHE-XM-CDOWN, DHR-HTX-CF-ALL
4	4.5	5.0 E-008	PCS-XHE-XM-CDOWN, DHR-MDP-CF-ALL
5	3.4	3.7 E-008	PCS-VCF-HW, DHR-HTX-CF-ALL
6	1.9	2.1 E-008	PCS-XHE-XM-CDOWN, LPR-MOV-CF-BWST

**Table B.2.5 Conditional Cut Sets for Higher Probability Sequences for
LER No. 270/97-001 (Continued)**

Cut set number	Percent contribution	CCDP ^a	Cut sets ^b
7	1.7	1.9 E-008	PCS-XHE-XM-CDOWN, HPR-MOV-CF-BWST
8	1.4	1.5 E-008	PCS-VCF-HW, DHR-MDP-CF-ALL
9	1.1	1.2 E-008	PCS-XHE-XM-CDOWN, LPR-SMP-FC-SUMP
SLOCA Sequence 10		4.2 E-007	
1	75.0	3.2 E-007	PCS-VCF-HW, LDST-LVL-LOW
2	25.0	1.1 E-007	PCS-XHE-XM-CDOWN, LDST-LVL-LOW, PCS-XHE-XM-FDEPR
Total (all sequences)		2.2 E-005	

^aThe conditional probability for each cut set is determined by multiplying the probability of the initiating event by the probabilities of the basic events in that minimal cut set. The probability of the initiating events are given in Table B.2.1 and begin with the designator "IE." The probabilities for the basic events also are given in Table B.2.1.

^bBasic event HPI-LINE-BREAK is a type TRUE event. This type of event is not normally included in the output of the fault tree reduction process, but has been added to aid in understanding the sequences to potential core damage associated with the event. This basic event was added to those cut sets that required HPI-LINE-BREAK for the cut set to occur.

^cComponents in the DHR system are shared with the LPI system. For example, the DHR motor-driven pumps are also the LPI pumps when providing LPI, or piggy-back cooling. Therefore, failure of the DHR pumps results in the failure of both DHR and PB-COOL in this sequence.

^dThis basic event represents the common-cause failure of HPI pumps B and C failing to start. At Oconee, one of the HPI pumps (pump A in this analysis) is always running to provide normal RCS makeup and seal injection; however, its flow is lost due to the HPI line break.

B.3 LER No. 287/97-003

Event Description: Two high-pressure injection pumps were damaged because of a low water level in the letdown storage tank

Date of Event: May 3, 1997

Plant: Oconee 3

B.3.1 Event Summary

Following a high-pressure injection (HPI) nozzle weld leak and thermal sleeve failure at Oconee 2, operators began shutting down Oconee 3 on May 1, 1997, so that personnel could inspect the HPI nozzles and thermal sleeves at that unit.¹ A low water level in the letdown storage tank (LDST), caused by the partial draining of the common reference leg in the tank level instrumentation, resulted in inadequate suction flow to the HPI pumps. Two of the three HPI pumps were damaged. All three HPI pumps were vulnerable to failure if a loss-of-coolant accident (LOCA) had occurred while the reference leg was drained. The estimated conditional core damage probability (CCDP) associated with this event for the 340-h period when the low water level in the reference leg would have impacted HPI pump operability is 5.4×10^{-6} . This is an increase of 4.3×10^{-6} over the nominal core damage probability (CDP) of 1.1×10^{-6} .

B.3.2 Event Description

On May 1, 1997, personnel at Oconee 3 started to shut down the reactor to inspect the HPI nozzles and thermal sleeves in response to an HPI nozzle weld leak and failed thermal sleeve at Oconee 2 (Ref. 2) and a reassessment of earlier Unit 3 radiographs that indicated the potential degradation of a Unit 3 thermal sleeve. By the morning of May 3, the decay heat removal (DHR) system had been placed in operation, reactor coolant system (RCS) temperature and pressure were at 115°C (240°F) and 1.9 MPa (270 psig), respectively, and a slow cooldown [5°C/h (10°F/h)] was in progress. HPI pump 3B was running, and pump 3A was in standby.

At 0913, control room alarm 3SA-2/C-2 indicated that the discharge pressure for the HPI pump was low. The alarm was cleared and then alarmed two more times during the next minute. HPI discharge pressure indicated ~14 MPa (2000 psig). While reactor coolant pump (RCP) seal injection flow indicated normal, the RCP seal injection control valve (3HP-31) position was observed to vary, and, in response, the operators placed the valve controller in "manual." At 0915, the 3A HPI pump autostarted on a low RCP seal injection flow signal. The control room operators stopped the 3A HPI pump within a minute, but when its control switch was placed in "automatic," it again started on low RCP seal injection flow.

The 3A HPI pump motor current was fluctuating at levels above normal (70–120 A), and the 3B pump motor current was about 10 A. The 3A pump was placed in the "run" mode, and the 3B pump was secured. Eight minutes after the initial low HPI discharge pressure alarm, both the RCP seal injection flow and HPI pump discharge pressure indicated low. The operators realigned the HPI pump suction flow path to the borated

water storage tank (BWST) by opening suction valve 3HP-24. The water level in the LDST began increasing, and the pump motor current for the 3A HPI pump motor stabilized at 10 A. At 0928, with HPI pump discharge pressure still low and no indication of RCP seal injection flow, operators closed BWST suction valve 3HP-24.

Two minutes later the operators observed that the LDST chart recorder had been indicating a constant level of 1.4 m (55.9 in.) for the last 1.75 h. The operators recognized that the HPI pump problems could be associated with erroneous LDST level indication, although the precise cause and nature of the problems were unknown. At 0931 the 3A HPI pump was secured, and valve 3HP-5 was closed to isolate RCS letdown. It was subsequently discovered that the 3A and 3B HPI pumps had been damaged when they were operated without an adequate suction source. Inadequate suction resulted from a low net positive suction head (NPSH) and possible hydrogen entrainment. The 3A and 3B pumps had operated with inadequate NPSH for about 15 min and 4 min, respectively.

RCS makeup and RCP seal injection were not immediately required, and a decision was made not to start the 3C HPI pump (if pump operation were required, the BWST could have been used as its suction source). A Notice of Unusual Event was declared at 1504 because of the expected delay in restoring RCS normal makeup. At 1515, the water level in the LDST level instrumentation common reference leg was found to be ~1.2 m (49 in.) instead of its normally filled level of > 2.5 m (100 in). The partially drained reference leg produced a high water level indication for the LDST. At the time that the HPI pumps were damaged, the tank level indicated 1.4 m (56 in.), but the tank was actually empty.

A small amount of boric acid buildup was noted around a test tee cap on the reference leg side of the No. 2 level transmitter. A subsequent laboratory examination concluded that the reference leg leak resulted from either (1) scratches on seating surfaces of the test tee and plug or (2) expansion of the tee nipple, probably from overtightening the cap sometime in the past. The licensee also noted that the reliance of the operators on the LDST low level alarm to cue LDST makeup, instead of LDST status monitoring to determine when makeup was needed, contributed to the HPI pump failures. The LDST low level alarm set point is 1.4 m (55-in.), 2.5 cm (1 in.) below the lowest tank level that could be indicated with the partially drained reference leg.

At ~2130, personnel began to develop procedures to flush, fill, vent, and start the 3C HPI pump without using the LDST. A contingency plan was also developed to support Unit 3 shutdown without any HPI pumps running, if necessary. Following approval of the procedures and contingency plan, the 3C HPI pump was successfully started at ~1140 on May 4, 1997, and the Unit 3 cooldown continued.

B.3.3 Additional Event-Related Information

The HPI system at Oconee provides both normal RCS makeup and RCP seal injection, as well as HPI for small- and medium-break LOCA mitigation. During normal operation, the HPI system "A" header, using either the 3A HPI pump or the 3B HPI pump, supplies RCS makeup and RCP seal injection [~300 L/min (80 gal/min) combined flow]. The LDST is used as a surge tank and normal (nonemergency) suction source for the HPI pumps. During operation, a hydrogen atmosphere is maintained in the LDST to promote oxygen scavenging. The "B" HPI header, supplied by the 3C HPI pump, is for emergency injection only. The HPI

pumps effectively share a common suction because the suction cross-connect valves are normally open (Fig. B.3.1).

Two channels of level indication are provided for the LDST. The operators can select either channel for display on a control room chart recorder. The level transmitters for the two channels utilize common process piping and a common reference leg that is vented back to the LDST.

Normally, the water level in the LDST ranges between 60 and 80 in. The low LDST level alarm set point is 1.4 m (55 in). When the LDST level is at 2.5 m (100 in.) (full) and the reference leg of the transmitter is full, there is zero differential pressure across the transmitter. This indicates a full tank. When LDST level indicates "0 m (0 in.)", about 2600 L (690 gal) remain in the tank. A continuous fill line, which would have maintained the reference leg filled, was included in the original LDST instrumentation design. The licensee did not consider the fill line to be a part of the instrumentation, and it was isolated at the time of the event.

The HPI pumps are normally isolated from the BWST by motor-operated valves (MOVs) HP-24 and -25. In the event of a safety system actuation, MOVs HP-24 and -25 open. The elevation head pressure in the BWST will overcome the pressure caused by the LDST level and hydrogen overpressure, opening check valves HP-101 and -102, closing the LDST outlet header check valve HP-97, and providing flow from the BWST to the HPI pumps. As the water level in the BWST drops, the available pressure from the LDST could exceed the available pressure from the BWST, allowing flow from the LDST when its check valve opens. The hydrogen gas in the LDST could then expand and fill the suction piping, resulting in damage to the HPI pumps. The procedural operating limit curve for LDST hydrogen pressure and volume is intended to ensure that LDST pressure does not exceed available BWST pressure, even as the water level in the BWST is drawn down during a LOCA. [A 1991 operational event at Oconee 1, 2, and 3 involving incorrect LDST hydrogen pressure/volume curves was analyzed as an accident sequence precursor (ASP).³]

The HPI pumps at Oconee are 24-stage vertical centrifugal pumps that develop 21-MPa (3000-psi) discharge pressure with a capacity of about 1900 L/min (500 gal/min) each. The pumps will typically only operate for 1-2 min without an adequate suction source before they are damaged.

Additional information concerning this event is included in an NRC Augmented Inspection Team report.⁴

B.3.4 Modeling Assumptions

If an initiating event involving a loss of RCS inventory occurred while the LDST was almost empty, all three HPI pumps could have failed as a result of hydrogen gas binding. This analysis assumes that the HPI system was vulnerable to failure as a result of the LDST common reference leg leak between February 22, 1997—when the LDST level instrumentation was calibrated, and May 3, 1997—when the two HPI pumps failed while shutting down. If an initiating event involving a loss of RCS inventory occurred during this time period, the potential for HPI pump failure would depend on the actual water levels that were reached in the LDST and BWST.

The potential effect of a loss of the HPI pumps following an initiating event without RCS inventory loss, such as the May 3, 1997, event when the low water level in the LDST was discovered, was not addressed in this

analysis. For such an event (or a postulated transient with successful primary relief valve closure, which was also not addressed in this analysis), the limited RCS makeup required could be provided by the safe shutdown facility (SSF) RCS makeup pump if all the HPI pumps were to fail.

This analysis assumed that the LDST reference leg was leaking continually. The LDST reference leg level was assumed to have decreased linearly with time, from 2.5 m (100 in.) (full) on February 22, 1997, to 1.2 m (49 in.) on May 3, 1997. Although the LDST is refilled to compensate for minor RCS leakage and to maintain the water level in the tank within the operational range, the gradual reduction in reference leg level resulted in an effective, albeit unrealized, reduction in tank level. Based on a simplified model of LDST level and pressure as a function of LDST reference leg level during BWST drawdown, the HPI pumps were estimated to be vulnerable to failure during (approximately) the final 20% of the time between February 22 and May 3, or 340 h. During this period, hydrogen gas would enter the pump suction piping and fail the HPI pumps if, following a LOCA, BWST level decreased to near the level at which switchover to high-pressure recirculation was required.

A new branch (HPI-LATE) was added to the event trees used in the ASP analysis to address the potential failure of HPI due to low water level in the LDST late in the injection phase. The fault tree associated with this branch consists of one basic event, LDST-LVL-LOW, that represents the probability that the water level in the LDST is unacceptably low. This basic event was set to TRUE during the 340-h period when the unacceptably low LDST water level existed. The ASP event trees for transients, loss of offsite power events, small-break LOCAs (SLOCAs), and steam generator tube ruptures (SGTRs) were also enhanced to address the potential use of rapid RCS depressurization and low-pressure injection (LPI) in the event that HPI failed and secondary-side cooling was available by adding branches to address fast depressurization, LPI, and low-pressure recirculation (LPR). The Oconee Individual Plant Examination (IPE) states that following an SLOCA with a loss of HPI, the emergency operating procedures direct the operators to use secondary heat removal systems to depressurize the RCS until LPI flow is greater than 380 L/min (100 gal/min) per header. The probability of the operators failing to depressurize the RCS and initiating LPI was assumed to be 0.1, consistent with Ref. 5 (pp. 5.7-22). Two operator actions associated with cooldown and depressurization are included in the SLOCA model. PCS-XHE-XM-CDOWN addresses the failure of the operators to cool down and depressurize the unit and initiate the residual heat removal (RHR) system following a SLOCA. This action is initiated early following the SLOCA. PCS-XHE-XM-FDEPR addresses the failure of the operators to depressurize to LPI pressure following a loss of HPI. In this event, this failure occurs close to the time when sump recirculation must be initiated, 4 to 6 h after the SLOCA. Because of this separation in time between the two actions, they were considered independent in this analysis.

If the water level in the BWST did not decrease to near the sump switchover level, then HPI pump operability would not be expected to be impacted. This could happen if, instead of proceeding to high-pressure recirculation, the operators successfully cooled down and depressurized the RCS during the injection phase and initiated DHR using the DHR system. This is the preferred response following an SLOCA because it avoids sump recirculation (the ASP models include this potential action). Limited BWST drawdown is expected in this case.^a

---

^aThis expectation is supported by the limited BWST drawdown that occurred following a 1325 L/min (350-gal/min) reactor coolant pump seal failure in 1980 at Arkansas Nuclear One, Unit 1 (Ref. 6).

HPI is also required to mitigate a medium-break LOCA (MLOCA) at Oconee (it is not required to mitigate a large-break LOCA). If an MLOCA occurred during the 340-h period when the LDST reference leg level was unacceptably low, the HPI pumps would have failed due to hydrogen entrainment before sump recirculation was initiated. The Oconee IPE (see Ref. 5, pp. 2.3-8 and -9, and Table D.2) notes that the time available before switchover to high-pressure recirculation (90 min) is too short to allow RCS depressurization to the point that LPI and LPR can be used if HPI were to fail early in this event. However, the IPE concluded that HPI failure around the time of switchover to sump recirculation could be mitigated by rapid depressurization to the point that LPR could be used.

The ASP Program typically considers the potential for core damage following four postulated initiating events in pressurized-water reactors: transient, loss of offsite power, SLOCA, and SGTR. Supercomponent-based linked fault tree models are available for each of these postulated initiating events. A linked fault tree model was developed to address the impact of a low water level in the LDST on an MLOCA. Consistent with the Oconee IPE, this model assumed that a reactor trip (RT), one train of HPI, and piggy-back cooling (high-pressure recirculation) are required for core cooling following an MLOCA; failure of HPI late in the injection phase was assumed to be mitigated through the use of rapid depressurization, LPI, and LPR. The fact that the event tree branch success criteria were the same as those used in the Oconee ASP model for an SLOCA allowed the existing fault trees to be used, in conjunction with the event tree shown in Fig. B.3.2, in describing MLOCA accident sequences. The event tree includes the following branches:

Initiating Event-MLOCA (MLOCA). The frequency of an MLOCA is estimated to be 5.0×10^{-4} /year [8.2×10^{-8} /h, assuming the unit is at power 70% of the time (6132 h)], based on a survey of medium-break frequencies performed in support of the analysis of Turkey Point LER No. 250/94-005 in the 1994 precursor report (see Appendix H to Ref. 7 for additional information).

Reactor Trip (RT). Failure of the reactor to trip is assumed to result in core damage following an MLOCA.

High-Pressure Injection (HPI). Failure of injection using the HPI system results in a loss of short-term RCS makeup and core damage following an MLOCA. Flow from one HPI pump is assumed to provide success.

HPI Fails Late (HPI-LATE). Failure of HPI system late in the injection phase results in the loss of RCS makeup and the requirement to rapidly depressurize the RCS to allow the use of LPI and LPR for core cooling. As described previously, this top event specifically addresses the potential failure of HPI due to low LDST level (other late injection phase failures, such as a common-cause failure of the HPI pumps to run, are imbedded within HPI). A failure probability of 1.0 is assumed for this branch when LDST level is unacceptably low.

RCS Fast Depressurization to LPI Pressure (FASTDEPR). Given a failure of HPI late in the injection phase, failure to rapidly depressurize the RCS to a pressure that would allow for adequate LPI flow results in a loss of RCS makeup and core damage.

Low Pressure Injection (LPI). Failure of LPI following successful RCS depressurization subsequent to a failure of HPI results in the loss of RCS makeup and core damage.

Piggy-Back Cooling (PB-COOL). Failure of piggy-back cooling results in a failure of long-term injection and DHR and is assumed to result in core damage. PB-COOL utilizes the DHR pumps, which take suction on the reactor building (RB) sump and provide water via the DHR heat exchangers to the suctions of the HPI pumps. Flow from one HPI pump (supplied by one DHR train) provides PB-COOL success.

Low-Pressure Recirculation (LPR). Failure of LPR following successful RCS depressurization subsequent to a failure of HPI results in a failure of long-term injection and DHR and is assumed to result in core damage. Like PB-COOL, LPR uses the DHR pumps, which take suction from the RB sump and provide water via the DHR heat exchangers to the RCS.

As with the other ASP linked fault tree models, the MLOCA model was solved using the Sapphire computer code to identify combinations of basic events (cut sets) that would result in core damage.

B.3.5 Analysis Results

The CCDP estimated for the potential HPI system unavailability because of the leaking LDST common reference leg is 5.4×10^{-6} . This is an increase of 4.3×10^{-6} over the nominal CDP of 1.1×10^{-6} for the 340-h period. The dominant sequence, highlighted as sequence 6 in Fig. B.3.2, contributes about 66% to the increase in the CCDP and involves

- a postulated MLOCA,
- successful RT,
- initial HPI success,
- failure of HPI late in the injection phase as a result of the low water level in the LDST, and
- failure to depressurize the RCS to allow the use of the LPI system for makeup.

Definitions and probabilities for selected basic events are shown in Table B.3.1. The conditional probabilities associated with the highest probability sequences are shown in Table B.3.2. Table B.3.3 lists the sequence logic associated with the sequences listed in Table B.3.2. Table B.3.4 describes the system names associated with the dominant sequences. Minimal cut sets associated with the dominant sequences are shown in Table B.3.5.

In addition to an assessment of the effect of a loss of HPI following a potential initiating event at Unit 3, a sensitivity analysis considered the effect if the Unit 3 LDST reference leg leak and the Unit 2 HPI nozzle weld leak (see the analysis of LER No. 270/97-001) had instead occurred at the same unit. As described in the analysis of LER No. 270/97-001, subsequent inspections of the thermal sleeve and injection line nozzles at Units 1 and 3 determined that Unit 3 was also affected by nozzle cracking. If the nozzle leak had occurred at Unit 3 at the same time as the low water level in the LDST (or if the low water level in the LDST had occurred at Unit 2 in conjunction with the observed leak), a CCDP of 2.8×10^{-4} would have been estimated.

B.3.6 References

1. Licensee Event Report 287/97-003, "High Pressure Injection System Inoperable due to Design Deficiency and Improper Work Practices," June 2, 1997.

2. Licensee Event Report 270/97-001, "Unisolable Reactor Coolant Leak due to Inadequate Surveillance Program," May 21, 1997.
3. J. W. Minarick et al., *Precursors to Potential Severe Core Damage Accidents: 1991, A Status Report*, USNRC Report NUREG/CR-4674, Vol. 16, September 1992, p B-47.
4. *NRC Augmented Inspection Team Report 269/97-06, 270/97-06, 287/97-06*, May 30, 1997.
5. Oconee Nuclear Station Units 1, 2, and 3, *IPE Submittal Report*, Rev. 1, December 1990.
6. W. B. Cottrell et al., *Precursors to Potential Severe Core Damage Accidents: 1980-1981, A Status Report*, USNRC Report NUREG/CR-3591, Vol. 2, February 1984, p. B-126.
7. R. J. Belles et al., *Precursors to Potential Severe Core Damage Accidents: 1994, A Status Report*, USNRC Report NUREG/CR-4674, Vol. 21, December 1995.

Fig. B.3.1. Flow diagram of the emergency core cooling system at Oconee 3 (Source: Oconee 3 Final Safety Analysis Report).

Fig. B.3.2. Dominant core damage sequence for LER No. 287/97-003.

Table B.3.1. Definitions and Probabilities for Selected Basic Events for LER No. 287/97-003

Event name	Description	Base probability	Current probability	Type	Modified for this event
IE-LOOP	Initiating Event-Loss of Offsite Power (LOOP)	2.8 E-006	2.8 E-006		No
IE-MLOCA	Initiating Event-MLOCA	8.1 E-008	8.1 E-008	NEW	Yes
IE-SGTR	Initiating Event-SGTR	1.3 E-006	1.3 E-006		No
IE-SLOCA	Initiating Event-SLOCA	6.5 E-007	6.5 E-007		No
IE-TRANS	Initiating Event-Transient	7.7 E-004	7.7 E-004		No
DHR-HTX-CF-ALL	Common-Cause Failure of the DHR Heat Exchangers	5.2 E-004	5.2 E-004		No
EFW-AOV-CF-FCV	Common-Cause Failure of the Emergency Feedwater (EFW) Flow-Control Valves	3.7 E-005	3.7 E-005		No
EFW-PMP-CF-ALL	Common-Cause Failure of the EFW Pumps	1.8 E-004	1.8 E-004		No
EFW-PSF-VF-MDP	Failure of the Upper Storage Tank Supply Line to the Motor-Driven Pumps (MDPs)	2.3 E-004	2.3 E-004		No
EFW-PSF-VF-SGA	Failure of the Flow Control Path to Steam Generator (SG) A	2.3 E-003	2.3 E-003		No
EFW-PSF-VF-SGB	Failure of the Flow Control Path to SG B	2.4 E-003	2.4 E-003		No
EFW-TDP-FC-TDP	Hardware Failures in the EFW Turbine-Driven Pump (TDP) Train	3.2 E-002	3.2 E-002		No
EFW-XHE-MDPSUP	Operator Fails to Switch Over the EFW MDPs to the Hotwell	1.0 E-003	1.0 E-003		No
EFW-XHE-NOREC	Operator Fails to Recover EFW	2.6 E-001	2.6 E-001		No
EFW-XHE-NOTHROT	Operator Fails to Throttle EFW Flow	5.0 E-003	5.0 E-003		No
EFW-XHE-TDPSUP	Operator Fails to Switchover the EFW TDPs to the Hotwell	5.0 E-002	5.0 E-002		No

**Table B.3.1. Definitions and Probabilities for Selected Basic Events for
LER No. 287/97-003 (continued)**

Event name	Description	Base probability	Current probability	Type	Modified for this event
EFW-XHE-THROT-L	Operator Fails to Throttle EFW Flow during a LOOP	5.0 E-003	5.0 E-003		No
LDST-LVL-LOW	Low Water Level in the LDST Fails the HPI Pumps	4.4 E-003	1.0 E+000	TRUE	Yes
LPR-XHE-XM	Operator Fails to Initiate LPR	1.0 E-002	1.0 E-002		No
MFW-SYS-TRIP	Main Feedwater (MFW) System Trips	2.0 E-001	2.0 E-001		No
MFW-XHE-NOREC	Operator Fails to Recover MFW	3.4 E-001	3.4 E-001		No
OPE-XHE-NOREC-6H	Operator Fails to Recover Offsite Power within 6 h	1.6 E-001	1.6 E-001		No
PCS-VCF-HW	Failure of Secondary System Hardware	3.0 E-003	3.0 E-003		No
PCS-XHE-XM-CDOWN	Operator Fails to Initiate Cooldown	1.0 E-002	1.0 E-002		No
PCS-XHE-XM-FDEPR	Operator Fails to Initiate Fast Depressurization for LPI	1.0 E-001	1.0 E-001	NEW	Yes
PCS-XHE-XO-SEC	Operators Fail to Establish Secondary Cooling	2.0 E-001	2.0 E-001		No
PCS-XHE-XO-SECL	Operators Fail to Establish Secondary Cooling during a LOOP	3.4 E-001	3.4 E-001		No
SSF-NO-START	SSF Fails to Operate	2.0 E-001	2.0 E-001		No

Table B.3.2. Sequence Conditional Probabilities for LER No. 287/97-003

Event tree name	Sequence number	Conditional core damage probability (CCDP)	Core damage probability (CDP)	Importance (CCDP-CDP)	Percent contribution ^a
MLOCA	6	2.9 E-006	1.3 E-008	2.8 E-006	65.6
SLOCA	10	8.9 E-007	3.9 E-009	8.8 E-007	20.4
MLOCA	4	2.7 E-007	1.2 E-009	2.7 E-007	6.2
LOOP	34	2.2 E-007	9.7 E-010	2.2 E-007	5.1
LOOP	39	7.2 E-008	3.1 E-010	7.1 E-008	1.7
SLOCA	33	6.1 E-008	2.7 E-010	6.1 E-008	1.4
TRANS	43	6.0 E-008	2.6 E-010	6.0 E-008	1.4
Total (all sequences)		5.4 E-006	1.1 E-006	4.3 E-006	

^aPercent contribution to the total importance.

Table B.3.3. Sequence Logic for Dominant Sequences for LER No. 287/97-003

Event tree name	Sequence number	Logic
MLOCA	6	/RT, /HPI, HPI-LATE, FASTDEPR
SLOCA	10	/RT, /EFW, /HPI, COOLDOWN, HPI-LATE, FASTDEPR
MLOCA	4	/RT, /HPI, HPI-LATE, /FASTDEPR, /LPI, LPR
LOOP	34	/RT-L, /EP, EFW-L, /PRVL-RES, SSF, /OP-6H, /HPI-C-L, SGCOOL, HPI-LATE
LOOP	39	/RT-L, /EP, EFW-L, /PRVL-RES, SSF, OP-6H, /HPI-C-L, SGCOOL-L, HPI-LATE
SLOCA	33	/RT, EFW, MFW, /SSF, /HPI, HPI-LATE
TRANS	43	/RT, EFW, MFW, SSF, /HPI-COOL, SGCOOL, HPI-LATE

Table B.3.4. System Names for LER No. 287/97-003

System name	Logic
COOLDOWN	RCS Cooldown to DHR Pressure Using Turbine-Bypass Valves, etc.
EFW	No or Insufficient EFW Flow
EFW-L	No or Insufficient EFW Flow during a LOOP
EP	Loss of all Emergency ac Power
FASTDEPR	RCS Cooldown to LPI Pressure Using Turbine-Bypass Valves, etc.
HPI	No or Insufficient HPI System Flow
HPI-C-L	Failure of HPI Cooling during a LOOP
HPI-COOL	Failure to Provide HPI Cooling
HPI-LATE	HPI Fails Late
LPI	No or Insufficient LPI
LPR	No or Insufficient LPR
MFV	Failure of the MFV System
OP-6H	Operator Fails to Recover Offsite Power Within 6 h
PRVL-RES	Power-Operated Relief Valves and Block Valves Fail to Reseat (Electric Power Succeeds)
RT	Reactor Fails to Trip during Transient
RT-L	Reactor Fails to Trip during LOOP
SGCOOL	Failure to Recover Secondary Cooling
SGCOOL-L	Failure to Recover Secondary Cooling when Offsite Power is Unavailable
SSF	SSF Fails to Operate

Table B.3.5. Conditional Cut Sets for Higher Probability Sequences for LER No. 287/97-003

Cut set number	Percent contribution	CCDP ^a	Cut sets ^b
MLOCA Sequence 6		2.9 E-006	
1	97.4	2.8 E-006	LDST-LVL-LOW, PCS-XHE-XM-FDEPR
2	2.9	8.5 E-008	LDST-LVL-LOW, PCS-PCF-HW
SLOCA Sequence 10		8.9 E-007	
1	75.0	6.8 E-007	LDST-LVL-LOW, PCS-PCF-HW
2	25.0	2.2 E-007	LDST-LVL-LOW, PCS-XHE-XM-CDOWN, PCS-XHE-XM-FDEPR
MLOCA Sequence 4		2.7 E-007	
1	92.0	2.5 E-007	LDST-LVL-LOW, /PCS-PCF-HW, /PCS-XHE-XM-FDEPR, LPR-XHE-XM
2	4.8	1.3 E-008	LDST-LVL-LOW, /PCS-PCF-HW, /PCS-XHE-XM-FDEPR, DHR-HTX-CF-ALL
LOOP Sequence 34		2.2 E-007	
1	98.4	2.2 E-007	EFW-XHE-THROT-L, SSF-NO-START, /OEP-XHE-NOREC-6H, LDST-LVL-LOW, PCS-XHE-XO-SEC
LOOP Sequence 39		7.2 E-008	
1	98.4	7.1 E-008	EFW-XHE-THROT-L, SSF-NO-START, OEP-XHE-NOREC-6H, LDST-LVL-LOW, PCS-XHE-XO-SECL
SLOCA Sequence 33		6.1 E-008	
1	98.4	6.1 E-008	EFW-XHE-NOTHROT, MFW-SYS-TRIP, MFW-XHE-NOREC, /SSF-NO-START, LDST-LVL-LOW
TRANS Sequence 43		6.0 E-008	
1	55.2	3.3 E-008	EFW-PMP-CF-ALL, EFW-XHE-NOREC, MFW-SYS-TRIP, MFW-XHE-NOREC, SSF-NO-START, LDST-LVL-LOW, PCS-XHE-XO-SEC
2	15.5	9.2 E-009	EFW-XHE-TDPSUP, EFW-XHE-MDPSUP, EFW-XHE-NOREC, MFW-SYS-TRIP, MFW-XHE-NOREC, SSF-NO-START, LDST-LVL-LOW, PCS-XHE-XO-SEC

**Table B.3.5. Conditional Cut Sets for Higher Probability Sequences for
LER No. 287/97-003 (Continued)**

Cut set number	Percent contribution	CCDP ^a	Cut sets ^b
3	11.5	6.8 E-009	EFW-AOV-CF-FCV, EFW-XHE-NOREC, MFW-SYS-TRIP, MFW-XHE-NOREC, SSF-NO-START, LDST-LVL-LOW, PCS-XHE-XO-SEC
4	9.9	6.1 E-009	EFW-TDP-FC-TDP, EFW-XHE-MDPSUP, EFW-XHE-NOREC, MFW-SYS-TRIP, MFW-XHE-NOREC, SSF-NO-START, LDST-LVL-LOW, PCS-XHE-XO-SEC
5	3.5	2.1 E-009	EFW-XHE-TDPSUP, EFW-PSF-VF-MDP, EFW-XHE-NOREC, MFW-SYS-TRIP, MFW-XHE-NOREC, SSF-NO-START, LDST-LVL-LOW, PCS-XHE-XO-SEC
6	2.3	1.4 E-009	EFW-TDP-FC-TDP, EFW-PSF-VF-MDP, EFW-XHE-NOREC, MFW-SYS-TRIP, MFW-XHE-NOREC, SSF-NO-START, LDST-LVL-LOW, PCS-XHE-XO-SEC
7	1.7	1.0 E-009	EFW-PSF-VF-SGA, EFW-PSF-VF-SGB, EFW-XHE-NOREC, MFW-SYS-TRIP, MFW-XHE-NOREC, SSF-NO-START, LDST-LVL-LOW, PCS-XHE-XO-SEC
Total (all sequences)		5.4 E-006	

^aThe CCDP is determined by multiplying the probability that the portion of the sequence that makes the precursor visible (e.g., the system with a failure is demanded) will occur during the duration of the event by the probabilities of the remaining basic events in the minimal cut set. This can be approximated by $1 - e^{-p}$, where p is determined by multiplying the expected number of initiators that occur during the duration of the event by the probabilities of the basic events in that minimal cut set. The expected number of initiators is given by λt , where λ is the frequency of the initiating event (given on a per-hour basis), and t is the duration time of the event (340 h). This approximation is conservative for precursors made visible by the initiating event. The frequencies of interest for this event are $\lambda_{MLOCA} = 8.15 \times 10^{-8}/h$, and $\lambda_{SLOCA} = 6.52 \times 10^{-7}/h$. The importance is determined by subtracting the CDP for the same period but with plant equipment assumed to be operating nominally.

^bBasic event LDST-LVL-LOW is a type TRUE event. This type of event is not normally included in the output of the fault tree reduction process but has been added to aid in understanding the sequences to potential core damage associated with the event.

B.4 LER Nos. 289/97-007, -008, -010

Event Description: Failure of both generator output breakers causes a LOOP

Date of Event: June 21, 1997

Plant: Three Mile Island, Unit 1

B.4.1 Event Summary

Three Mile Island, Unit 1 (TMI 1), was at 100% power when the plant experienced a loss of offsite power (LOOP) after both generator output breakers in the 230-kV substation failed.¹ The LOOP resulted in an immediate trip of both the reactor and the turbine; plant computer data indicated that the trip insertion times were excessive for four control rods.² Both emergency diesel generators (EDGs) started and loaded as designed. Offsite power was restored within 90 min. The unit was cooled by natural circulation cooling until offsite power and forced cooling were restored. It was subsequently discovered that the pressurizer power-operated relief valve (PORV) was failed closed during this event (see Additional Event-Related Information).³ The estimated conditional core damage probability (CCDP) for this plant-centered LOOP is 9.6×10^{-6} .

B.4.2 Event Description

TMI 1 was at 100% power after almost 617 d of continuous operation. On June 21, 1997, the B phase of the 230-kV generator output breaker GBI-02 (Fig. B.4.1) developed a fault and caused severe overheating and the subsequent ejection of the bushing and conductor from the breaker housing. This resulted in a fault being detected on 230-kV bus 4. The parallel generator breaker, GBI-12, opened because of the detected fault on 230-kV bus 4. Breaker GBI-12 subsequently suffered a restrike, which damaged the B phase of this breaker, causing a fault on 230-kV bus 8. Automatic breaker action because of both faults isolated electric power to the station, resulting in a LOOP.¹

The LOOP caused an immediate reactor trip and turbine trip. The plant computer captured times associated with each control rod reaching the 25% zone reference as the reactor trip occurred. A review of the data showed that four control rods exceeded the trip insertion time limit of 1.66 s for three-fourths insertion. Personnel attributed the slow insertion times to reduced clearances in the old-style control rod drive thermal barriers because of the presence of deposits on the internal check valves, between the thermal barrier bushing, and on the leadscrew. All control rods inserted to the three-fourths insertion position within 3.0 s. The licensee determined that there would be no adverse effects associated with control rod insertion times as high as 3.0 s (Ref. 2).

Both EDGs started and loaded onto their respective safeguards bus as designed. Nonvital loads, including main feedwater, condensate, circulating water, and main condenser vacuum pumps, were not energized. The reactor coolant pumps (RCPs) were also without power. Natural circulation was verified in the reactor coolant system within 19 min following the trip and LOOP. Decay heat removal was established using the emergency feedwater (EFW) system and the steam generator atmospheric dump valves. Offsite power was

restored within 90 min after the breaker failures. After operators established the main condenser heat sink, the RCPs were restarted. The reactor coolant system was returned to forced circulation cooling ~9 h after the unit tripped.¹

B.4.3 Additional Event-Related Information

TMI 1 has a single PORV installed on the pressurizer that is replaced with a spare PORV during each refueling outage. The licensee discovered that during the previous refueling outage, the PORV was wired incorrectly and was subsequently inoperable for the entire operating cycle. The PORV was failed in the closed position and would not have opened in response to an automatic [16.9 MPa (2450-psig)] or a manual signal.³ The operating cycle completed with a failed PORV encompassed the LOOP event described by Refs. 1 and 2.

In addition to the PORV, two safety relief valves are connected to the pressurizer with a nominal relief set point of 17.2 MPa (2500 psig). The shutoff head of the safety injection pumps is ~20 MPa (2900 psig). Feed-and-bleed operation is possible with an inoperable PORV because the safety relief valves can be lifted with the head established by operating the safety injection pumps.⁴

TMI 1 has two dedicated EDGs (1A and 1B) to supply electric power to engineered safeguards buses 1D and 1E, respectively, in the event of a LOOP. Additionally, one EDG previously from TMI 2 is available as an alternate ac power source during a station blackout (SBO). The alternate EDG, which is manually started from the control room, can be aligned to either engineered safeguards bus 1D or 1E or the balance-of-plant bus 1C within 10 min following an SBO. Operators must close two breakers and open/lockout two breakers, and any desired loads must be manually loaded onto the bus selected to be reenergized.⁴

B.4.4 Modeling Assumptions

This event was modeled as a plant-centered LOOP. The probability of not recovering offsite power in the short term is included in the initiating event probability (IE-LOOP). That is, the probability of a LOOP is 1.0. The probability that offsite power is not recovered in ~30 min is 0.5, based on the data distributions provided in NUREG-1032, *Evaluation of Station Blackout Accidents at Nuclear Power Plants*.⁵ Consequently, IE-LOOP was set to the probability for a plant-centered LOOP assuming operators fail to recover offsite power in the short term (5.0×10^{-1}).

The probability of short-term and long-term offsite power recovery for a plant-centered LOOP and the probability of a RCP seal loss-of-coolant accident (LOCA) following a postulated station blackout were developed based on data distributions contained in NUREG-1032. The RCP seal LOCA models were developed as part of the NUREG-1150 probabilistic risk assessment (PRA) efforts. Both models are described in *Revised LOOP Recovery and PWR Seal LOCA Models*.⁶ The probabilities for the following basic events are based on these models:

1. initiating event-LOOP (IE-LOOP),
2. operator fails to recover offsite power within 2 h (OEP-XHE-NOREC-2H),
3. operator fails to recover offsite power within 6 h (OEP-XHE-NOREC-6H),

4. operator fails to recover offsite power before battery depletion (OPE-XHE-NOREC-BD),
5. operator fails to recover offsite power before RCP seals fail (OPE-XHE-NOREC-SL), and
6. RCP seals fail without cooling and injection water (RCS-MDP-LK-SEALS).

The PRA for TMI 1 indicates that an SBO with a concurrent failure of EFW would lead to core damage in approximately 2 h (Ref. 7, Table B.1-11, page B.1-25). This indicates that substantial time is available for the recovery of electric power. Potential recovery actions were modeled (using data from NUREG-1032) by the addition of a basic event (OEP-XHE-NOREC-SB) under the OP-SBO top event (OP-2H) on the LOOP event tree (Fig. B.4.2). Top event OP-SBO is substituted for the OP-2H top event whenever emergency power (EP) and EFW fail.

The alternate EDG (from TMI 2) was added to the Integrated Reliability and Risk Analysis System (IRRAS) model for TMI 1. The probability that the alternate EDG fails to start and run (basic event EPS-DGN-FC-AAC) was set to the same value as the dedicated EDGs (4.2×10^{-2}). In addition, because operators must start and load the alternate EDG manually, a basic event was added to reflect the probability that the operator fails to start and load the alternate EDG (basic event EPS-XHE-XM-AAC). Basic event EPS-XHE-XM-AAC was set at 1.0×10^{-2} in accordance with similar human error probabilities already incorporated in the IRRAS model for TMI. The common-cause failure probability of the emergency power system for the base case was based on two EDGs. This was adjusted based on the availability of three EDGs and was developed based on data distributions contained in INEL-94-0064, *Common-Cause Failure Data Collection and Analysis System* (Ref. 8, Table 5-8: alpha factor distribution summary – fail to start, CCCG = 3, $\alpha_{3S} = 0.0224$; and Table 5-11: alpha factor distribution summary – fail to run, CCCG = 3, $\alpha_{3R} = 0.0232$). Because α_3 is equivalent to the β factor of the multiple Greek letter method used in the IRRAS models, the common-cause failure probability of the EDGs (basic event EPS-DGN-CF-ALL) was adjusted from 1.6×10^{-3} based on two EDGs to 9.5×10^{-4} based on three EDGs.

The slow insertion of four reactor control rods was not considered in the model. The control rods inserted well within the time (3.0 s) that the licensee calculated to be limiting. Additionally, all but four control rods met the three-fourths insertion time prescribed by the Technical Specifications.

Because the PORV was inadvertently disabled during the operating cycle that encompassed the LOOP event, the probability that the PORV fails to open on demand (basic event PPR-SRV-CC-PORV) was set to "TRUE" (i.e., will not open). Two additional basic events were added to the IRRAS model to account for the availability of the safety relief valves to relieve any pressure buildup (basic events PPR-SRV-CC-1A and PPR-SRV-CC-1B). The probability that a safety relief valve would fail to open when its set point was reached was set to the nominal failure rate for the PORV (see Table B.4.1). Additionally, the operator would only need to verify that the high-pressure injection (HPI) pumps started in a situation that required feed-and-bleed cooling to remove decay heat; no other action regarding the PORV or the safety relief valves is required from the operators. Therefore, the probability that the operator fails to initiate feed-and-bleed cooling (basic event HPI-XHE-XM-HPICL) was reduced from 1.0×10^{-2} to 1.0×10^{-3} .

B.4.5 Analysis Results

The CCDP for this event is 9.6×10^{-6} . The dominant core damage sequence for this event (sequence 26 on Fig. B.4.2) involves

- a LOOP,
- a successful reactor trip,
- a failure of EP,
- a successful initiation of EFW,
- no challenge to the PORV (failed) or pressurizer safety relief valves,
- a failure of the RCP seals, and
- a failure to restore electric power before core damage.

This SBO sequence (sequence 26 on Fig. B.4.2) accounts for 85% of the total contribution to the CCDP. The next most dominant sequence (sequence 41 on Fig. B.4.2) contributes 11% to the total CCDP. This sequence involves an SBO, a failure of the EFW system, and a failure to recover any form of electrical power before the onset of core damage.

All of the most significant sequences involve an SBO. The nominal probability that a PORV is challenged during a LOOP or an SBO is 0.16 and 0.37, respectively, based on actual LOOP and SBO events. However, the PORV failure diminished those sequences where the PORV could potentially have lifted and then failed to reseal. Basic events PPR-SRV-CO-L and PPR-SRV-CO-SBO (defined in Table B.4.1) were set to 5.0×10^{-3} and 5.4×10^{-3} , respectively (i.e., the PORV will not open, but the safety valves are challenged) based on Integrated Plant Examination (IPE) data. Because the safety relief valves have a higher set point than the PORV, they may or may not have lifted in place of the PORV. However, the safety valves were assumed to lift during feed-and-bleed operation.

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

B.4.6 References

1. LER 289/97-007, Rev. 0, "Generator Output Breaker Failure Resulting in a Loss of Off-Site Power and Reactor Trip," July 21, 1997.
2. LER 289/97-008, Rev. 0, "Control Rod Trip Insertion Times Exceed TS Section 4.7.1.1 Limits," July 21, 1997.
3. LER 289/97-010, Rev. 0, "Pilot Operated Relief Valve (PORV) Inoperability Due to Being Mis-Wired and Failure to Perform Post-Maintenance Test (PMT) Following Replacement During 11R Refueling Outage," November 12, 1997.

4. Three Mile Island, *Final Safety Analysis Report (Updated Version)*.
5. P. W. Baranowsky, *Evaluation of Station Blackout Accidents at Nuclear Power Plants*, USNRC Report NUREG-1032, June 1988.
6. *Revised LOOP Recovery and PWR Seal LOCA Models*, ORNL/NRC/LTR-89/11, August 1989.
7. Three Mile Island Unit 1, *Probabilistic Risk Assessment (Level 1)*, December 1992.
8. Marshall and Rasmuson, *Common-Cause Failure Data Collection and Analysis System*, INEL-94/0064, December 1995.

Fig. B.4.1 Three Mile Island switchyard.

NUREG/CR-4674, Vol. 26

**Table B.4.1. Definitions and Probabilities for Selected Basic Events for
LER Nos. 289/97-007, -008, - 010**

Event name	Description	Base probability	Current probability	Type	Modified for this event
IE-LOOP	Initiating Event-LOOP (Includes the Probability of Recovering Offsite Power in the Short Term)	8.6 E-006	5.0 E-001		Yes
IE-SGTR	Initiating Event-Steam Generator Tube Rupture	1.6 E-006	0.0 E+000		Yes
IE-SLOCA	Initiating Event-Small Loss-of-Coolant Accident (SLOCA)	1.0 E-006	0.0 E+000		Yes
IE-TRANS	Initiating Event-Transient (TRANS)	1.3 E-004	0.0 E+000		Yes
EFW-TDP-FC-TDP	EFW Turbine-Driven Pump Fails	3.2 E-002	3.2 E-002		No
EFW-XHE-NOREC-EP	Operator Fails to Recover EFW during an SBO	3.4 E-001	3.4 E-001		No
EPS-DGN-CF-ALL	Common-Cause Failure of EDGs	9.5 E-004	9.5 E-004		No
EPS-DGN-FC-1A	1A EDG Fails to Start and Run	4.2 E-002	4.2 E-002		No
EPS-DGN-FC-1B	1B EDG Fails to Start and Run	4.2 E-002	4.2 E-002		No
EPS-DGN-FC-AAC	Alternate ac EDG Fails to Start and Run	4.2 E-002	4.2 E-002	NEW	No
EPS-XHE-NOREC	Operator Fails to Recover Emergency Power	8.0 E-001	8.0 E-001		No
EPS-XHE-XM-AAC	Operator Fails to Start or Load the Alternate ac EDG	1.0 E-002	1.0 E-002	NEW	No
OEP-XHE-NOREC-2H	Operator Fails to Recover Offsite Power within 2 h	2.2 E-001	1.4 E-001		Yes
OEP-XHE-NOREC-6H	Operator Fails to Recover Offsite Power within 6 h	6.7 E-002	9.9 E-004		Yes
OEP-XHE-NOREC-BD	Operator Fails to Recover Offsite Power before Battery Depletion	2.4 E-002	3.5 E-004		Yes
OEP-XHE-NOREC-SB	Operator Fails to Recover Electric Power before Core Damage (No Electric Power or EFW)	2.3 E-001	2.3 E-001	NEW	No
OEP-XHE-NOREC-SL	Operator Fails to Recover Offsite Power before RCP Seals Fail	5.7 E-001	4.8 E-001		Yes

**Table B.4.1. Definitions and Probabilities for Selected Basic Events for
LER Nos. 289/97-007, -008, -010 (Continued)**

Event name	Description	Base probability	Current probability	Type	Modified for this event
PPR-SRV-CC-1A	Safety Relief Valve 1A Fails to Open on Demand	6.3 E-003	6.3 E-003	NEW	No
PPR-SRV-CC-1B	Safety Relief Valve 1B Fails to Open on Demand	6.3 E-003	6.3 E-003	NEW	No
PPR-SRV-CC-PORV	PORV Fails to Open on Demand	6.3 E-003	1.0 E+000	TRUE	Yes
PPR-SRV-CO-L	PORV Fails to Open, but Safety Valves Challenged during a LOOP	1.6 E-001	5.0 E-003		Yes
PPR-SRV-OO-SBO	PORV Fails to Open, but Safety Valves Challenged during an SBO	3.7 E-001	5.4 E-003		Yes
RCS-MDP-LK-SEALS	RCP Seals Fail without Cooling and Injection	4.6 E-002	4.0 E-002		Yes

Table B.4.2. Sequence Conditional Probabilities for LER Nos. 289/97-007, -008, -010

Event tree name	Sequence number	Conditional core damage probability (CCDP)	Percent contribution
LOOP	26	8.2 E-006	85.0
LOOP	41	1.1 E-006	10.8
LOOP	19	1.5 E-007	1.5
Total (all sequences)		9.6 E-006	

Table B.4.3. Sequence Logic for Dominant Sequences for LER Nos. 289/97-007, -008, -010

Event tree name	Sequence number	Logic
LOOP	26	/RT-L, EP, /EFW-L, /PORV-SBO, SEALLOCA, OP-SL
LOOP	41	/RT-L, EP, EFW-EP, OP-SBO
LOOP	19	/RT-L, EP, /EFW-L, /PORV-SBO, /SEALLOCA, OP-BD

Table B.4.4. System Names for LER Nos. 289/97-007, -008, -010

System name	Logic
EFW-EP	No or Insufficient EFW Flow during an SBO
EFW-L	No or Insufficient EFW Flow during a LOOP
EP	Failure of Both Trains of Emergency Power
OP-BD	Operator Fails to Recover Off-Site Power before Battery Depletion
OP-SBO	Operator Fails to Restore ac Power before Core Damage Occurs Following an SBO and Loss of EFW
OP-SL	Operator Fails to Restore ac Power before a RCP Seal LOCA Occurs
PORV-SBO	PORV/Safety Relief Valves Challenged during an SBO
RT-L	Reactor Fails to Trip during a LOOP
SEALLOCA	RCP Seals Fail during a LOOP

**Table B.4.5. Conditional Cut Sets for Higher Probability Sequences for
LER Nos. 289/97-007, -008, -010**

Cut set number	Percent contribution	CCDP ^a	Cut sets
LOOP Sequence 26		8.2 E-006	
1	91.2	7.5 E-006	EPS-DGN-CF-ALL, EPS-XHE-NOREC, RCS-MDP-LK-SEALS, OEP-XHE-NOREC-SL
2	7.1	5.8 E-007	EPS-DGN-FC-1A, EPS-DGN-FC-1B, EPS-DGN-FC-AAC, EPS-XHE-NOREC, RCS-MDP-LK-SEALS, OEP-XHE-NOREC-SL
3	1.7	1.4 E-007	EPS-DGN-FC-1A, EPS-DGN-FC-1B, EPS-XHE-XM-AAC, EPS-XHE-NOREC, RCS-MDP-LK-SEALS, OEP-XHE-NOREC-SL
LOOP Sequence 41		1.1 E-006	
1	91.1	9.6 E-007	EPS-DGN-CF-ALL, EPS-XHE-NOREC, EFW-TDP-FC-TDP, EFW-XHE-NOREC-EP, OEP-XHE-NOREC-SB
2	7.1	7.5 E-008	EPS-DGN-FC-1A, EPS-DGN-FC-1B, EPS-DGN-FC-AAC, EPS-XHE-NOREC, EFW-TDP-FC-TDP, EFW-XHE-NOREC-EP, OEP-XHE-NOREC-SB
3	1.7	1.8 E-008	EPS-DGN-FC-1A, EPS-DGN-FC-1B, EPS-XHE-XM-AAC, EPS-XHE-NOREC, EFW-TDP-FC-TDP, EFW-XHE-NOREC-EP, OEP-XHE-NOREC-SB
LOOP Sequence 19		1.5 E-007	
1	91.2	1.3 E-007	EPS-DGN-CF-ALL, EPS-XHE-NOREC, OEP-XHE-NOREC-BD
2	7.1	1.0 E-008	EPS-DGN-FC-1A, EPS-DGN-FC-1B, EPS-DGN-FC-AAC, EPS-XHE-NOREC, OEP-XHE-NOREC-BD
3	1.7	2.5 E-009	EPS-DGN-FC-1A, EPS-DGN-FC-1B, EPS-XHE-XM-AAC, EPS-XHE-NOREC, OEP-XHE-NOREC-BD
Total (all sequences)		9.6 E-006	

^aThe conditional probability for each cut set is determined by multiplying the probability of the initiating event by the probabilities of the basic events in that minimal cut set. The probabilities for the initiating events and the basic events are given in Table B.4.1.

B.5 LER No. 309/97-004

Event Description: Reactor coolant system hot-leg recirculation valves subject to pressure locking because of post-LOCA thermal expansion of the trapped water

Date of Event: January 22, 1997

Plant: Maine Yankee

B.5.1 Event Summary

Maine Yankee was shut down for refueling when engineers noted a plant design deficiency while conducting a piping system review in response to Nuclear Regulatory Commission (NRC) Generic Letter (GL) 96-06. Personnel determined that the coolant trapped between the containment integrity check valve and the loop-fill motor-operated valves (MOV) could cause the loop-fill MOVs to become pressure locked following a loss-of-coolant accident (LOCA). The LOCA could cause the fluid that is normally trapped between these valves to expand. This, in turn, could cause the pressure between the valves to exceed the torque available to open the MOVs (i.e., the valves could become thermally pressure locked). Hence, without sufficient leakage past the loop-fill MOVs, the valves would be rendered inoperable. The loop-fill MOVs are used for hot-leg recirculation to prevent the boron from precipitating in the core. Boron precipitation could lead to core damage by obstructing coolant flow through the core, thereby reducing the removal of decay heat.¹ The estimated increase in the core damage probability (CDP) over a 1-year period for this event (i.e., the importance) is 1.3×10^{-5} . The base probability of core damage (the CDP) for the same period (i.e., 1 year) is 6.9×10^{-5} . Uncertainty in the frequency of a large-break LOCA (none have occurred) and the likelihood of a MOV failing under post-LOCA conditions contribute to the uncertainty in this estimate.

B.5.2 Event Description

On January 22, 1997, while Maine Yankee was shut down for refueling, engineers were conducting a piping system design review in response to a deficiency identified in licensee event report (LER) 309/96-022 (Ref. 2) and NRC GL 96-06 (Ref. 3). These engineers determined that the section of loop-fill piping between the containment integrity check valve (CH-72) and the loop-fill MOVs (RC-M-15, 25, 35) was susceptible to thermal pressure locking following a LOCA (Fig. B.5.1). Emergency operating procedures require this section of piping to be used for hot-leg recirculation 19 h after a large cold-leg break. This is because a large cold-leg LOCA allows a significant portion of safety injection flow from the cold-leg injection paths to bypass the core by flowing directly out the break. The result is boiling in the core, which causes the boron concentration to increase. At Maine Yankee, if the boiling persists for more than 19 h, the concentration of boron in the core can reach the saturation point, allowing precipitation to occur. Boron precipitation would further reduce or obstruct flow through the core and could lead to core damage because of insufficient decay heat removal. Boron precipitation is prevented by the timely switch to hot-leg recirculation. This ensures that injection flow will go through the core before flowing out the break in the cold leg.

Pressure locking occurs when the fluid in the valve bonnet is at a higher pressure than the adjacent piping at the time of the valve opening. The two most likely scenarios for elevating the pressure in the valve bonnet relative to the pressure in the valve system follow.

1. Thermal pressure locking (or bonnet heatup) can occur when an incompressible fluid is trapped in the valve bonnet (e.g., during valve closure) or a section of piping bounded by a check valve (as in this case), and the volume in the bonnet/piping is heated. The bonnet heatup scenarios include heating the valve bonnet by an increase in the temperature of the environment during an accident, or heatup because of an increase in the temperature of the process fluid on either side of the valve, etc. (Normal ambient temperature variation is not considered because it occurs over a long time, and pressure changes tend to be alleviated through extremely small amounts of leakage. Further, operating experience shows that normal temperature variations are not a source of pressure-locking events.)
2. Hydraulic pressure locking (or pressure trapping) can occur when an incompressible fluid is trapped in the valve bonnet and is followed by depressurization of the adjacent piping before valve opening. Examples of hydraulic pressure-locking scenarios include back-leakage past check valves and system operating pressures that are higher than the system pressure when the valve is required to open, which did not occur in this event.

Pressure locking is of concern because the pressure in the space between the two disks of a gate valve can become pressurized above the pressure assumed when sizing the valve's motor operator. This could prevent the valve operator from opening the valve when required.

B.5.3 Additional Event-Related Information

During the injection phase, Maine Yankee uses two charging pumps for high-pressure safety injection (HPSI) of water from the refueling water storage tank (RWST) into each of the three reactor coolant system (RCS) cold legs via two cold-leg injection trains. A third charging pump is available as a spare, but it must be manually aligned (Fig. B.5.1). During hot-leg recirculation, the charging pumps inject water through the loop-fill MOVs. A safety injection tank (accumulator) is available to inject water into each cold leg automatically if RCS pressure decreases below the pressure in its accumulator [about 1.4 MPa (200 psig)]. Low-pressure safety injection (LPSI) is provided by two residual heat removal (RHR) pumps, which also pump water from the RWST into each RCS cold leg. The two RHR pumps are also used for shutdown decay heat removal.⁴

The containment spray system provides for recirculation and containment cooling. On a containment spray actuation signal (CSAS), the spray system uses two spray pumps to deliver water through the RHR heat exchangers to two separate spray rings located inside containment. The water is supplied from the RWST or the containment sump following a recirculation actuation signal (RAS). A third spray pump is available as a spare, but it must be manually aligned. On an RAS, the containment spray pumps provide water from the containment sump, through the RHR heat exchangers, to the charging pump suction (and to the spray rings if a CSAS exists).

B.5.4 Modeling Assumptions

Boron precipitation was only considered to be a mechanism for core damage in a break of an RCS cold leg because this allows a significant portion of safety injection water to bypass the core and flow directly out the break. Large- and medium-break LOCAs (LBLOCAs and MLOCAs) currently are not addressed by the models used in the Accident Sequence Precursor (ASP) Program. Therefore, it was necessary to construct a model specifically for this analysis. A large-break LOCA event tree was created for the Integrated Reliability and Risk Analysis System (IRRAS) model based on the success trees in Maine Yankee's *Individual Plant Examination* (IPE).⁵ The Maine Yankee IPE estimates the frequency of a large-break LOCA to be 2.7×10^{-4} /year; the frequency of a medium-break LOCA is 8.0×10^{-4} per year.⁵ The hot-leg fill valves were considered impacted in response to a LOCA during this period (i.e., the water is trapped between valves, and the increased temperature resulting from the LOCA heats the water). A 1-year condition assessment was conducted because this is typically the longest period analyzed by the ASP Program. Hence, a 70% plant availability provides a duration time of approximately 6130 h for this event.

Successful response to a large-break LOCA includes either of the following:

1. One HPSI train, one LPSI train, one accumulator, and successful switchover to cold-leg recirculation that requires at least one containment spray pump. Hot-leg recirculation is not addressed by the IPE; however, the LER for this event indicated that the switchover to hot-leg recirculation is required 19 h after a large cold-leg break.
2. No HPSI trains, two LPSI trains, one accumulator, and successful switch-over to cold-leg recirculation. Again, switchover to hot-leg recirculation is required 19 h following a large cold-leg break.

Based on these combinations, an LBLOCA event tree was constructed (Fig. B.5.2).

The event tree for the LBLOCA event tree includes the following branches:

IE-LBLOCA. The initiating event is an LBLOCA. The frequency of an LBLOCA is estimated to be 2.7×10^{-4} /year. This value is consistent with a survey of large- and medium-break LOCA frequencies provided in the 1994 ASP report (see Appendix H.6 in Ref. 6 for additional information). A reactor trip is not a prerequisite for preventing core damage following an LBLOCA because void formations resulting from boiling terminate the fission process. Therefore, a reactor trip is not included in the event tree.

HPSI. The existing IRRAS fault tree for the HPSI system is used for this event tree branch. A system failure, by itself, does not lead to core damage. However, most HPSI system components (e.g., pumps, valves, piping) are required for successful recirculation.

LPSI-1. The fault tree for this event was constructed assuming that the break occurs in one of the three RCS cold legs. Therefore, one of three injection paths is assumed to be unavailable with all injection flow from

LPSI-2. The fault tree for this event is the same as the LPSI-1 fault tree except that both RHR pumps and both injection trains are required for success.

A1. The fault tree for this event was also constructed assuming that the break is in one of the RCS cold legs. Therefore, the contents of one accumulator are assumed to flow directly out the break. Success for this branch occurs if one of the two intact loop accumulators injects borated water properly. An accumulator is assumed to operate correctly if the associated accumulator MOV remains open and the corresponding check valve opens as designed.

Cold-Leg Recirculation. Success for this branch implies that at least one containment spray train operates to supply water to the suction of the HPSI system from the containment sump. At least one HPSI train must also operate and inject water into one of the two intact RCS cold legs.

Cold-Leg Break. Success for this branch implies that the LOCA occurred in one of the RCS hot legs, because hot-leg recirculation would not be required to prevent core damage following a hot-leg break. This analysis assumes an equal likelihood that the LBLOCA will occur in a cold leg or hot leg (i.e., LEAK-IN-COLD-LEG = 0.5).

Hot-Leg Recirculation. Success requires at least one of the three loop-fill MOVs to open and one of the two cold-leg injection paths to be isolated. Because the required components for successful hot-leg and cold-leg recirculation are essentially the same (such as HPSI pumps, RWST isolation valves), it is assumed that if cold-leg recirculation failed, then hot-leg recirculation will not be successful either, leading to core damage.

Predicting with certainty the containment environment 19 h following an LBLOCA is difficult. The location of the loop-fill valves and the temperature of the containment heat sink will greatly influence the status of the loop-fill MOVs. Additionally, because of the piping configuration, if any one of the loop-fill valves opens, the pressure will be relieved on all three valves. As a result, the nominal failure probabilities (3.0×10^{-3}) for the loop-fill MOVs (HPR-MOV-CC-HOTA, -HOTB, -HOTC) were not adjusted. However, the loop-fill MOV common-cause failure probability (HPR-MOV-CF-HOT) was adjusted from its nominal probability.

Based on the licensee discussion in the event report, there were two possible failure mechanisms for each loop-fill MOV. The event report¹ indicated that "... based on engineering judgement it has been determined that [a LOCA induced] pressure increase [in the adjacent piping] could render the loop-fill valves inoperable either by physically damaging the valves or hydrostatically locking the valve disk in place." The event report also indicated that check valve leakage on the opposite end of the affected pipe run could prevent any impact on the loop-fill MOVs (i.e., the probability of the valves becoming pressure locked = 0.0). Lacking more explicit detail, all three of these possibilities were considered equally likely to occur. If a loop-fill MOV was damaged (probability = 0.33), it was assumed that the valve would not open when required (i.e., the probability of the valves failing to operate = 1.0). If a loop-fill MOV disk was hydrostatically locked in place (probability = 0.33), there was assumed to be some chance of the motor torque overcoming the pressure lock as the hot water that expanded into the disk cavity cooled. According to the FSAR⁴, in the worst case, the containment temperature will peak within 10 s at $\sim 135^{\circ}\text{C}$ (275°F) [the initial temperature was 41°C (105°F)]. After 19 h the temperature is predicted to be $\sim 82^{\circ}\text{C}$ (180°F). This is about one-half of the peak temperature. Therefore, it was assumed that the probability of the motor torque being insufficient to overcome the loop-fill

MOV disk pressure given that the valves would initially have been hydraulically pressure locked was essentially 0.5. As a result, the common cause failure probability for the three loop-fill valves was set to $[(0.0 \times 0.33) + (1.0 \times 0.33) + (0.5 \times 0.33)]^3 = 0.1$.

It was further assumed that the operator cannot recover the hot-leg recirculation configuration if the loop-fill MOVs fail because of thermal pressure locking. Therefore, the operator nonrecovery probability (HPR-XHE-NOREC-HL) was set to TRUE (1.0).

B.5.5 Analysis Results

The increase in the CDP over a 1-year period for this event is estimated to be 1.3×10^{-5} . The nominal CDP over the same 1-year period for all sequences is 6.9×10^{-5} . There is substantial uncertainty in this estimate because of the uncertainty in the frequency of an LBLOCA (none have occurred) and the likelihood of MOVs failing under post-LOCA conditions. The dominant core damage sequence for this event (Sequence 3 on Fig. 2) involves the following events:

- a postulated LBLOCA in one cold leg,
- success of the HPSI system,
- success of the LPSI system,
- success of the accumulator system,
- success of the cold-leg recirculation configuration, and
- a failure of the hot-leg recirculation configuration.

This sequence accounts for almost 100% of the total contribution to the increase in the CDP. No other initiating events are affected by a failure of the hot-leg recirculation configuration.

If the loop-fill MOVs are considered disabled for the long-term following a LOCA, given that they become hydrostatically pressure locked, then the increase in CDP as a result of this event over a 1-year period swells to 3.9×10^{-5} . Conversely, if the drop to 22°C (180°F) in containment 18 h after a LOCA is assumed to be sufficient in all cases to allow the motor torque to overcome any pressure locking in all three loop-fill MOVs, then the increase in CDP as a result of this event drops to 5.2×10^{-6} .

Definitions and probabilities for selected basic events are shown in Table B.5.1. The conditional probabilities associated with the highest probability sequences are shown in Table B.5.2. Table B.5.3 lists the sequence logic associated with the sequences listed in Table B.5.2. Table B.5.4 describes the system names associated with the dominant sequences. Minimal cut sets associated with the dominant sequences are shown in Table B.5.5.

B.5.6 References

1. LER 309/97-004, Rev. 0, "RCS Loop-Fill Header MOV Overpressure," February 24, 1997.
2. LER 309/96-022, Rev. 0, "Containment Primary Component Cooling Piping Design Inadequacy Due to Lack of Thermal Relief Valves," August 19, 1996.

3. NRC Generic Letter 96-06, "Assurance of Equipment Operability and Containment Integrity During Design-Basis Accident Conditions," September 30, 1996.
4. Maine Yankee Atomic Power Company, *Final Safety Analysis Report*.
5. Maine Yankee Atomic Power Company, *Individual Plant Examination*.
6. R. J. Belles et al., *Precursors to Potential Severe Core Damage Accidents: 1994, A Status Report*, USNRC Report NUREG/CR-4674 (ORNL/NOAC-232), Vol. 21, December 1995.

Fig. B.5.1 Maine Yankee high-pressure safety injection/charging system.

Fig. B.5.2 Dominant core damage sequence for LER No. 309/97-004.

Table B.5.1. Definitions and Probabilities for Selected Basic Events for LER No. 309/97-004

Event name	Description	Base probability	Current probability	Type	Modified for this event
IE-LBLOCA	Initiating Event--Large-break LOCA	4.4 E-008	4.4 E-008	NEW	No
HPR-MOV-CC-HOTA	Failure of MOV RC-M-15 (Loop-Fill) to Open for Hot-Leg Recirculation	3.0 E-003	3.0 E-003	NEW	No
HPR-MOV-CC-HOTB	Failure of MOV RC-M-25 (Loop-Fill) to Open for Hot-Leg Recirculation	3.0 E-003	3.0 E-003	NEW	No
HPR-MOV-CC-HOTC	Failure of MOV RC-M-35 (Loop-Fill) to Open for Hot-Leg Recirculation	3.0 E-003	3.0 E-003	NEW	No
HPR-MOV-CF-HOT	Common-Cause Failure of Hot-Leg Recirculation MOVs	7.9 E-005	1.0 E-001	NEW	Yes
HPR-XHE-NOREC-HL	Operator Fails to Recover Hot-Leg Recirculation	8.0 E-001	1.0 E+000	NEW TRUE	Yes
LEAK-IN-COLD-LEG	Large-Break LOCA Occurs in One of the Three RCS Cold Legs	5.0 E-001	5.0 E-001	NEW	No

Table B.5.2. Sequence Conditional Probabilities for LER No. 309/97-004

Event tree name	Sequence number	Conditional core damage probability (CCDP)	Core damage probability (CDP)	Importance (CCDP-CDP)	Percent contribution ^a
LBLOCA	03	1.3 E-005	1.4 E-007	1.3 E-005	99.9
Total (all sequences)		8.2 E-005	6.9 E-005	1.3 E-005	

^aPercent contribution to the total importance.

Table B.5.3. Sequence Logic for Dominant Sequences for LER No. 309/97-004

Event tree name	Sequence number	Logic
LBLOCA	03	/HPI, /LPSI-1, /A1, /COLDLEG, RCSCOLD, HOTLEG

Table B.5.4. System Names for LER No. 309/97-004

System name	Logic
A1	Failure of One of Two Accumulators (Assumes a Cold-Leg Break)
COLDLEG	Failure of Cold-Leg Recirculation
HOTLEG	Failure of Hot-Leg Recirculation
HPI	No or Insufficient Flow From the HPSI System
LPSI-1	LPSI Fails When One of Two Pumps Are Required
RCSCOLD	LBLOCA Occurs in One of the Three RCS Cold Legs

Table B.5.5. Conditional Cut Sets for Higher Probability Sequences for LER No. 309/97-004

Cut set number	Percent contribution	Change in CCDP (importance) ^a	Cut sets ^b
LBLOCA Sequence 03		1.3 E-005	
1	97.4	1.3 E-005	LEAK-IN-COLD-LEG, HPR-MOV-CF-HOT, HPR-XHE-NOREC-HL
Total (all sequences)		1.3 E-005	

^aThe change in conditional probability (importance) is determined by calculating the conditional probability for the period in which the condition existed and subtracting the conditional probability for the same period but with plant equipment assumed to be operating nominally. The conditional probability for each cut set within a sequence is determined by multiplying the probability that the portion of the sequence that makes the precursor visible (e.g., the system with a failure is demanded) will occur during the duration of the event by the probabilities of the remaining basic events in the minimal cut set. This can be approximated by $1 - e^{-p}$, where p is determined by multiplying the expected number of initiators that occur during the duration of the event by the probabilities of the basic events in that minimal cut set. The expected number of initiators is given by λt , where λ is the frequency of the initiating event (given on a per-hour basis), and t is the duration time of the event. This approximation is conservative for precursors made visible by the initiating event. The frequency of interest for this event is $\lambda_{\text{LBLOCA}} = 4.4 \times 10^{-6}/\text{h}$. The duration time for this event is 6130 h ($8760 \text{ h} \times 0.7$).

^bBasic event HPR-XHE-NOREC-HL is a type TRUE event. This type of event is not normally included in the output of the fault tree reduction process, but it has been added to aid in understanding the sequences to potential core damage associated with the event.

B.6 LER No. 335/97-011

Event Description: Nonconservative recirculation actuation signal set point

Date of Event: November 2, 1997

Plant: St. Lucie, Unit 1

B.6.1 Event Summary

St. Lucie, Unit 1, was defueled and undergoing a steam generator replacement refueling outage. Utility personnel determined that the engineered safety feature actuation system's (ESFAS's) recirculation actuation signal (RAS) bistable set point for indicating the water level in the refueling water tank (RWT) had been set less conservatively than the Technical Specification set point. Plant personnel determined that the unit was more susceptible to core damage in the event of a large-break loss-of-coolant accident (LBLOCA) since changing the span of the RWT level indication during a 1993 refueling outage.¹ The nominal core damage probability (CDP) is 1.7×10^{-5} . The increase in CDP (i.e., the importance) is 1.7×10^{-5} over a 1-year period because of an improper RAS set point. Hence, the less conservative RAS set point results in an estimated conditional core damage probability (CCDP) of 3.4×10^{-5} for a 1-year period of operation. Uncertainty in the frequency of an LBLOCA (none have occurred) and uncertainty in the amount of emergency core cooling system (ECCS) flow required when recirculation is initiated contribute to the uncertainty in this estimate.

B.6.2 Event Description

On October 27, 1997, St. Lucie, Unit 1 was defueled and undergoing a steam generator replacement refueling outage. As part of the outage, obsolete ESFAS bistables were being replaced to improve system reliability and calibration methods. The equipment to be replaced included all four channels of the RWT low-level bistables. A signal from these RWT low-level bistables causes the operating mode of the safety injection system to change from the injection mode to the recirculation mode following a loss-of-coolant accident (LOCA).

Because of the RWT bistable changes, a system engineer performed additional verification to ensure that the RWT level set point agreed with the instrument loop scaling requirement. This review showed that the Technical Specification set point of 1.2 m (48 in.) from the bottom of the RWT correlated to a bistable set point of 5.28 mA.¹ The functional test procedure required an assigned set point of 4.96 mA, which corresponds to a water level in the RWT of 0.9 m (36 in.) above the tank bottom.¹ The less conservative set point dictated by the functional test procedure was applied to all four channels of the Unit 1 RWT level instrument bistables.

In January 1993, an engineering calculation was issued by the St. Lucie engineering staff to change the span of the RWT level measurement loop such that 0 m (0 ft) would reference the bottom of the tank. The level instruments are actually 0.3 m (1 ft) above the bottom of the RWT, and the 0-m (0-ft) mark previously referenced the height of the level instruments. Before the change in the span of the RWT level, the set point

procedure correctly initiated the RAS 1.2 m (48 in.) above the true bottom of the RWT [0.9-m (36-in.) set point plus 0.3 m (12-in.) instrument height].¹ After the change in the span of the RWT level, the set point procedure was not changed. Subsequently, the set point procedure incorrectly initiated RAS at 0.9 m (36 in.) above the bottom of the RWT.

B.6.3 Additional Event-Related Information

The RAS causes the suction source for the ECCS to transfer from the RWT at the end of the injection phase to the containment sump. This begins the recirculation phase. The injection phase is not influenced by the set point error; under worst-case conditions, the injection phase will last at least for the initial 20 min following a LOCA.¹ When the RAS set point is reached, the containment sump isolation valve is opened in ~30 s, and the RWT isolation valve is closed in ~90 s. The operator is directed by the emergency operating procedure (EOP) to initiate recirculation manually if the automatic signal fails to initiate recirculation when the RWT level reaches 48 in. from the bottom of the tank.¹

The ECCS suction pipe outer diameter is ~0.6 m (24 in.). The top of the inner diameter of the ECCS suction pipe is 1.1 m (42.25 in.) above the bottom of the RWT. The bistable set point error would delay the automatic initiation of recirculation until the RWT water level was ~15 cm (6 in.) below the top of the ECCS suction piping. Without operator action, a condition known as open channel flow would occur. From calculations made by the licensee, open channel flow conditions could not support full ECCS flow [~49,000 L/min (13,000 gal/min)]. The mismatch between available open channel flow and full ECCS flow would drain down the level in the ECCS suction piping and lead to air ingestion and reduction of the available net positive suction head for the ECCS pumps. Under these conditions, chugging flow would result until the ECCS pumps became air bound. This interruption of ECCS flow would prevent a further drain down of the RWT, and the lower RAS set point might never be reached.¹

The licensee further calculated that ECCS flows below 26,500 L/min (7000 gal/min) could be supported by open channel conditions until the lower RAS set point was reached.¹ This limits concern for ECCS failure, as a result of the less conservative RWT bistable set point, to an LBLOCA. Additionally, the peak containment temperature and pressure will be mitigated within the first 20 min following a LOCA; when containment pressure falls below 0.03 MPa (5 psig), operators are directed by the EOPs to secure the containment spray pumps. Because the spray pumps provide more than 22,700 L/min (6000 gal/min) flow [25,500 L/min (6750 gal/min), Ref. 2, Table 6.3-6], this would reduce the total ECCS flow required below 26,500 L/min (7000 gal/min) before reaching open channel flow conditions.

B.6.4 Modeling Assumptions

This event was modeled as a failure of the automatic RAS for an LBLOCA during a 1-year period. A failure to initiate recirculation could air bind all ECCS pumps following an LBLOCA, leading to core damage. Therefore, the significance of this event can be estimated directly from the change in ECCS pump failure probabilities because of the improper RAS set point and the probability of an LBLOCA during a 1-year period. The *St. Lucie Individual Plant Examination* (IPE) estimates the frequency of an LBLOCA to be 2.7×10^{-4} /year.

The increased probability of core damage because of ECCS pump failures is estimated by considering the probability that the operators will fail to initiate recirculation manually when the RWT water level drops to 1.2 m (48 in.) and the probability that the operators will fail to secure the spray pumps when conditions allow. Hence, the increased probability of core damage is

$$P(\text{LBLOCA}) \times P(\text{operator fails to initiate recirculation manually}) \times P(\text{operator fails to secure spray pumps}).$$

Operator fails to initiate recirculation manually

Manual initiation of recirculation following a LOCA is directed by EOPs if the automatic RAS should fail. The operators had correct indication of the RWT level in the control room, and the EOP directs operator attention to the RWT level when the water level drops to 1.8 to 2.4 m (6 to 8 ft). Manual initiation of recirculation when directed by the EOP would prevent any damage to the ECCS pumps because of the RAS set point error. It was assumed that the high-pressure injection (HPI) pumps would not be required to prevent core damage for the LBLOCA of concern in this event. Therefore, the low-pressure injection (LPI) pumps were expected to be the key to preventing core damage. Reference 1 indicated that 240 s was available after reaching the nominal RAS set point before the LPI pumps would fail. (The HPI pumps would fail within 90 s.) A simulator test suggested that operating crews maintained positive control of the RWT level and recognized the need to manually initiate recirculation ~40 s after the nominal automatic set point was reached. The *Human Reliability and Safety Analysis Data Handbook*³ suggests that for postaccident task actions, a 1-min delay for travel/manipulation should be allowed (Ref. 3, p. 66). So, 100 s was considered the median time response for an operating crew. Allowing ~10 s for the containment sump valves to reposition enough to allow significant flow, the critical time was assumed to be 230 s before the LPI pumps would fail because of gas binding (i.e., 240 s - 10 s). The probability of the operating crew failing to initiate recirculation manually can be estimated by assuming that the failure probability can be represented as a time-reliability correlation (TRC) as described in *Human Reliability Analysis*.⁴ Operator response was assumed to be rule-based and without hesitancy. For the 230-s period of interest, a failure probability of 1.2×10^{-1} was estimated.

Operator fails to secure spray pumps

If total ECCS flow could be reduced below 26,500 L/min (7000 gal/min) before reaching the automatic RAS set point, then the potential for ECCS pump failure, because of the nonconservative bistable set point, is eliminated (Ref. 1, p. 9). Analysis of containment pressure curves in the final safety analysis report (FSAR)² indicates that containment pressure should be reduced to 0.03 MPa (5 psig) in ~20 min following an LBLOCA. If the RWT level were at the Technical Specification minimum level [1,521,000 L (401,800 gal) (Ref. 2)] and ECCS flows were at the maximum indicated by Ref. 1 [49,000 L/min (13,000 gal/min)], then a minimum of 25.8 min would be available until the intended automatic RAS set point is reached [251,000 L (66,200 gal) (Ref. 2)]. The EOPs direct the operating crew to secure the containment spray pumps when containment pressure returns below 0.03 MPa (5 psig). The *Human Reliability and Safety Analysis Data Handbook*⁴ suggests that for postaccident task actions, a 5-min delay for diagnosis/ analysis be allowed and a 1-min delay for travel/manipulation be allowed (Ref. 4, p. 66). With this median response prediction, the probability of the operating crew failing to secure the spray pumps can be estimated by assuming that the failure probability can be represented as a TRC as described in *Human Reliability Analysis*.³ Operator

response was assumed to be rule-based, but with hesitancy, because conditions to secure the spray pumps are not met immediately. This operator action was assumed to be independent of the operator action to manually establish the recirculation line-up, because of the way the EOP directs these activities be performed and the independence of the instrumentation required. Allowing 0.2 min for equipment response, a failure probability of 5.2×10^{-1} was estimated for the 5.6-min period of interest [(25.8 - 20.0 - 0.2) min]. A sensitivity study on the operator response time is presented at the end of the next section.

B.6.5 Analysis Results

The nominal CDP over a 1-year period because of an improper RAS set point is approximately 1.7×10^{-5} . The increase in the CDP over a 1-year period (i.e., the importance) is 1.7×10^{-5} . Hence, the less conservative RAS set point increased this probability to 3.4×10^{-5} . This value is the CCDP for the 1-year period with an improper RAS set point. A large uncertainty is associated with this estimate because it relies on an estimated LBLOCA frequency (none have occurred) and estimations of operator response during accident conditions.

The dominant core damage sequence (sequence 4 in Fig. B.6.1) for this event involves

- an LBLOCA,
- successful injection from the safety injection tanks,
- a failure of automatic RAS,
- operator fails to manually back up the RAS, and
- operators fail to secure the containment spray pumps before the RAS set point is reached.

The CCDPs are shown in Table B.6.1, while Table B.6.2 lists the sequence logic associated with the sequences listed in Table B.6.1. Table B.6.3 provides the definitions and failure probabilities for event tree branch points in Fig. B.6.1.

The HPI pumps were expected to fail 90 s following an RAS failure.¹ If it is assumed that HPI pump failure impacts adequate decay heat removal following some LOCA events of concern, the probability of the operating crew failing to initiate recirculation manually before HPI pump failure can be estimated by assuming that the failure probability can be represented as a TRC as described in *Human Reliability Analysis*.³ Operator response was assumed to be rule-based and without hesitancy. Again allowing 10 s for valves to reposition and allow significant flow, a failure probability of 6.2×10^{-1} was estimated for the 80-s period of interest. In this case, the estimated increase in the CDP is 8.7×10^{-5} for a 1-year period with the RAS set point too low. The CCDP then is increased to 1.0×10^{-4} .

It could be assumed that the operator focus on current EOP steps and accident conditions overall would preclude any consideration of securing the containment spray pumps so early in the event. In this case, the probability of failing to secure the spray pumps before reaching the RAS set point would be 1.0. The estimated CCDP for this event increases to 4.9×10^{-5} for a 1-year period with the RAS set point lower than the design basis. In contrast, with increased attention on RWT water management per the EOP, it is possible that the operating crew would be quick to secure containment spray pumps when it became permissible. If the median response were considered to be 3 min instead of the 6 min assumed previously, the probability that the operator fails to secure the spray pump is 1.9×10^{-1} . The estimated CCDP for this event decreases

to 2.3×10^{-5} for a 1-year period with the RAS set point too low. Similar results are obtained if the water level in the RWT is assumed to start well above the minimum water level allowed by Technical Specifications when demanded.

B.6.6 References

1. LER 335/97-011, Rev. 0, "Non-Conservative Recirculation Actuation Signal Set Point Resulted in Operation Prohibited by the Technical Specifications," December 2, 1997.
2. St. Lucie, *Final Safety Analysis Report (Updated Version)*.
3. D. I. Gertman and H. S. Blackman, *Human Reliability and Safety Analysis Data Handbook*, John Wiley and Sons, 1994.
4. E. M. Dougherty and J. R. Fragola, *Human Reliability Analysis*, John Wiley and Sons, 1988.

Fig. B.6.1. St. Lucie LBLOCA event tree.

Table B.6.1. Sequence Conditional Probabilities for LER No. 335/97-011

Event tree name	Sequence number	Conditional core damage probability (CCDP)	Core damage probability (CDP)	Importance (CCDP-CDP)	Percent contribution
LBLOCA	4	3.4 E-005	1.7 E-005	1.7 E-005	99.9
LBLOCA	5	2.7 E-008	2.7 E-008	0.0 E+000	0.1
Total (all sequences)		3.4 E-005	1.7 E-005	1.7 E-005	

Table B.6.2. Sequence Logic for Dominant Sequences for LER No. 335/97-011

Event tree name	Sequence number	Logic
LBLOCA	4	/SIT, RAS, RAM, SPRAY
LBLOCA	5	SIT

Table B.6.3. System Names for LER No. 335/97-011

System name	Description	Failure probability
IE-LBLOCA	Initiating Event-LBLOCA	2.7 E-004
RAS	The RAS Bistable Fails to Change the Safety Injection Mode from Injection to Recirculation	1.0 E+000
RAM	Operator Fails to Manually Initiate Recirculation when the Water Level in the RWT Drops to 1.2 m (48 in.)	1.2 E-001
SIT	The Safety Injection Tanks Fail to Inject Water Properly	1.0 E-004
SPRAY	Operator Fails to Secure the Spray Pumps when Conditions Allow	5.2 E-001

Appendix C:
Shutdown Precursors for 1997

C.1 Shutdown Precursors

C.1.1 Accident Sequence Precursor Program Event Analyses for 1997

This appendix documents 1997 operational events selected as 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 the Nuclear Operations Analysis Center (NOAC), or
2. the LER or other event documentation was identified as requiring review by the Nuclear Regulatory Commission (NRC) Office for Analysis and Evaluation of Operational Data.

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

C.1.2 Shutdown Precursors Identified

No shutdown precursor events were identified among the 1997 events reviewed at the NOAC. Events were identified as shutdown precursors if they met the following 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} .

Appendix D:

Potentially Significant Events Considered Impractical to Analyze

D.1 Potentially Significant Events Considered Impractical to Analyze

Two of the licensee event reports (LERs) for 1997 were identified as potentially significant but impractical to analyze. It is believed that events considered impractical 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 impractical events are listed in Table D.1.

Table D.1 Potentially Significant Events Considered Impractical to Analyze

Event Number	Plant	Event description	Page
LER 336/97-015	Millstone 2	Nine of 89 containment penetrations are susceptible to thermally induced over-pressurization	D.2-1
LER 336/97-023	Millstone 2	The maximum allowable peak fuel element cladding temperature may be exceeded during a LOCA	D.3-1

D.1.3 Event Documentation

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

For each impractical event, a description of the operational event, event-related plant design information, the assumptions and approach used to model the event, analysis results, and references are given.

D.2 LER No. 336/97-015

Event Description: Nine of 89 containment penetrations are susceptible to thermally induced overpressurization

Date of Event: April 15, 1997

Plant: Millstone 2

D.2.1 Event Summary

Personnel at Millstone 2 determined that 89 containment penetrations were potentially susceptible to overpressurization conditions due to the thermal expansion of the fluid (water) during either normal or post-accident conditions. Of the 89 penetrations, it was further determined that 9 were susceptible to thermally induced overpressurization.

D.2.2 Event Description

On September 30, 1996, the Nuclear Regulatory Commission (NRC) informed licensees in Generic Letter (GL) 96-06 that the potential existed for the containment air recirculation (CAR) cooler water systems to be susceptible to either water hammer or two-phase flow conditions during postulated accident conditions. On April 15, 1997, personnel at Millstone 2 determined that the potential did exist for water hammer and two-phase flow to occur in the CAR cooler piping and, therefore, could cause the piping to fail such that the CAR coolers may not be able to perform their safety function during certain accident conditions.

GL 96-06 also requested that licensees determine if piping systems that penetrate containment are susceptible to thermally induced overpressurization when isolated. Personnel at Millstone 2 determined that 89 containment penetrations were potentially susceptible to overpressurization conditions due to the thermal expansion of the fluid (water) during either normal or postaccident conditions. Of the 89 penetrations, it was further determined that 9 were susceptible to thermally induced overpressurization.

Due to the potential of thermally induced overpressurization and the effects of either water hammer or two-phase flow conditions that could compromise the containment penetration integrity, the licensee considers this condition to be potentially safety significant.

D.2.3 Basis for Selection as an "Impractical" Event

The LER indicates that 9 (of 89) containment penetrations are susceptible to thermally induced overpressurization. These penetrations are not identified, and the conditions of concern are not specified. A request for more information from the licensee was forwarded to the NRC; however, more information from the licensee is not expected until next year. Because the information requested is currently unavailable, this event is currently impractical to analyze.

D.2.4 References

1. LER No. 336/97-015, "Performance Deficiency of Containment Air Recirculation Coolers During Design Basis Accidents (Response to Generic Letter 96-06)," May 15, 1997.

D.3 LER No. 336/97-023

Event Description: The maximum allowable peak fuel element cladding temperature may be exceeded during a LOCA

Date of Event: August 30, 1997

Plant: Millstone 2

D.3.1 Event Summary

On June 12, 1997, during a review of the high-pressure safety injection (HPSI) pump Technical Specifications (TS), personnel determined that the actual HPSI system flow rates to the reactor coolant system (RCS) may be less than the flow assumed in the Final Safety Analysis Report (FSAR). Because the potential exists that the resulting HPSI flow rates could result in the peak fuel element cladding temperature limit being exceeded, the licensee considered this condition to be potentially safety significant.

D.3.2 Event Description

During a review of the HPSI pump TS, personnel determined that the actual HPSI system flow rates to the RCS may be less than the flow rates assumed in the FSAR loss-of-coolant accident (LOCA) and the main steam line break (MSLB) analyses. The following nonconservative assumptions could significantly reduce the volume of HPSI system flow assumed to be delivered to the RCS, which are in turn used to determine if the peak fuel element cladding temperature limit would be exceeded:

- The existing analysis assumes the same HPSI system flow rates to each of the four cold legs during a LOCA. However, HPSI flow rates calculated on a hydraulic resistance basis show significantly more flow could be spilled out the break than the 25% assumed. At high HPSI pressures, this could result in a flow reduction of up to 265 L/min (70 gpm).
- The flow transmitters that are used to verify the required HPSI flow rates have an instrument inaccuracy of $\pm 4\%$. Flow instrument accuracy was not addressed in the existing analysis.
- The HPSI pump head/flow performance assumed by the existing analysis is based on the nominal manufacturer's curve without tolerance or allowance for pump degradation. Flow testing has shown that the high flow portion for the A HPSI pump is less than the manufacturer's curve.

Based on the effect of these nonconservative assumptions, when RCS pressures are between the shutoff head of the HPSI pump and ~ 7.6 MPa (1100 psig), HPSI flow could be less than assumed in the existing accident analyses, even with two operating HPSI trains. Consequently, the maximum peak fuel element cladding temperature of 1200°C (2200°F) allowed by 10 CFR 50.46 may be exceeded.

D.3.3 Basis for Selection as an "Impractical" Event

The current SLOCA analysis is based on the existing nonconservative HPSI flow rate assumptions and has a peak fuel element cladding temperature limit of 1100°C (2010°F). Because a revised HPSI system delivery flow to the RCS has not been calculated, the LOCA analyses have not been reevaluated. Hence, it is unknown if the peak fuel element cladding temperature limit of 1200°C (2200°F) allowed by 10 CFR 50.46 can be met. (An initial evaluation suggests that sufficient flow would be available with both trains operating to ensure that the peak fuel element cladding temperature will not be exceeded.)

D.3.4 References

1. LER No. 336/97-023, "Minimum HPSI Flow Used in FSAR Accident Analysis may be Non-conservative," July 14, 1997.

Appendix E:
Containment-Related Events

E.1 Containment-Related Events

No reactor plant operational event for 1997 was selected as a containment-related event. Such events involve unavailability of containment function, 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 Program; however, the potential for increased exposure to the public justifies their inclusion in the report. Containment models have not been developed as part of the Accident Sequence Precursor Program. Again, no containment-related events were identified for 1997.

Appendix F:
“Interesting” Events

F.1 "Interesting" Events

Five reactor plant operational events for 1997 were selected as "interesting" events. These events are documented in this section. "Interesting" events are not normally precursors 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 1997 are shown in Table F.1.

A summary, event description, and any additional event-related information are provided for these events.

Table F.1 Index of "Interesting" Events

Event number	Plant	Event description	Page
LER 219/97-010	Oyster Creek	Generator exciter fire results in partial LOOP	F.2-1
LER 247/97-018	Indian Point 2	A fault in a unit auxiliary transformer protective relay causes a loss of generator load	F.3-1
LERs 293/97-004, -006, -007	Pilgrim 1	LOOP occurs during shutdown	F.4-1
LERs 333/97-001, -002	FitzPatrick	Fouling of the circulating water system traveling screens	F.5-1
LER 461/97-018	Clinton	Normal power supply breaker for safety bus fails to open	F.6-1

F.2 LER No. 219/97-010

Event Description: Generator exciter fire results in partial LOOP

Date of Event: August 1, 1997

Plant: Oyster Creek

F.2.1 Event Summary

A brush shattered during performance of an at-power maintenance procedure on the main generator exciter, resulting in a generator field ground and an insulation fire. The reactor was scrammed, the turbogenerator tripped, and the plant 4-kV buses transferred from their unit auxiliary supply to the plant startup transformers. The 4-kV safety bus voltages then degraded sufficiently to cause the buses to be stripped of their offsite power feeds. The emergency diesel generators (EDGs) started and energized the safety buses. The control rod drive pumps failed to automatically start as designed.¹

F.2.2 Event Description

A preventive maintenance procedure was being performed on the main generator exciter when a brush shattered, causing extensive sparking. A generator field ground occurred, and a fire started in the ventilation exhaust duct. Plant operators then manually scrammed the unit in accordance with plant procedures.

The scram resulted in a turbogenerator trip, which caused the plant 4-kV buses to transfer to the startup transformers. After the transfer, emergency bus voltages fell below the degraded grid voltage relay setpoint, and the offsite bus feeders for the emergency buses tripped. The EDGs started and energized their respective buses. All loads sequenced on correctly except for the control rod drive (CRD) pumps, which started and immediately tripped on undervoltage. The reactor protection system was briefly deenergized during the transfer to the EDGs and, as a result, primary and secondary containment isolations occurred. The "electromatic relief valves" (main steam relief valves) operated to limit reactor pressure, and the isolation condenser was aligned. The plant was then taken to cold shutdown.

F.2.3 Basis for Selection as an "Interesting" Event

The low-voltage condition sensed on the plant emergency buses was determined to be genuine. Because of heavy seasonal demand and unavailability of a utility substation, regional grid voltage dipped about 4.5% after the plant trip. An additional drop of up to 6% occurred across the plant startup transformers, whose voltage regulators were found to be set too low. Accordingly, the emergency bus voltages dropped below the degraded grid trip point and did not recover above the reset point until after the undervoltage trip time delay relays had timed out. Switchyard voltages returned to normal approximately 20 s into the event, and the switchyard could have been used to supply the engineered-safety features (ESF) buses thereafter.²

During the event, power was maintained at acceptable voltage levels to the nonsafety 4-kV buses A and B, and systems powered from buses A and B (such as condensate and feedwater) remained available.²

The CRD pumps at Oyster Creek are designed to automatically load onto the safety buses after the EDGs start, during a LOOP event. During the event, the CRD pumps started but tripped immediately on undervoltage. An investigation determined that the CRD pump breaker undervoltage protection circuits had not been allowed sufficient time to reset prior to starting the pumps. As a result, an "antipump" circuit sensed simultaneous open and close signals for the breakers and locked out the pumps. Plant operators diagnosed the problem, reset the pump undervoltage trips, and started the pumps locally at the breakers.

F.2.4 Factors of Interest

Because offsite power remained available to the plant nonsafety buses throughout the event and was available to the safety buses within 20 s after the plant trip, this event did not meet all criteria for inclusion as an ASP event. However, the event appears to be an unexpected partial LOOP, and a description of this interesting event is therefore included.

F.2.5 References

1. LER 219/97-010, Rev. 0, "Manual Reactor Scram, ESF Actuation and Design Deficiencies Noted As a Result of Generator Exciter PM," August 1, 1997.
2. Personal communication from P. O'Reilly, U.S. Nuclear Regulatory Commission, to B. W. Dolan, Science Applications International, Inc., April 1998.

F.3 LER No. 247/97-018

Event Description: A fault in a unit auxiliary transformer protective relay causes a loss of generator load

Date of Event: July 26, 1997

Plant: Indian Point 2

F.3.1 Event Summary

With the unit at 99.4% power, a malfunction of a protective directional relay in switchyard transformer TA-5 caused a generator load shed to occur. The main turbine subsequently tripped on mechanical overspeed, which in turn generated a reactor trip. The frequency mismatch generated by the overspeed condition prevented the automatic transfer of loads from the unit auxiliary transformer to the station auxiliary transformer. This caused a loss of power to four 6.9-kV buses and two 480-V buses. Two 6.9-kV buses and two 480-V buses remained energized. All reactor coolant pumps lost power, and decay heat was removed by natural circulation for approximately 40 min. This transient with electrical complications had the potential to develop into a complete loss of offsite power event.

F.3.2 Event Description

On July 26, 1997, the plant was operating at 99.4% power when a fault occurred in a protective directional relay in switchyard transformer TA-5. For protection, the directional relay trips several switchyard breakers that feed the 138-kV supply transformer, TA-5, if a minimum current is sensed to be reversed and feeding the switchyard ring bus. When the minimum current is reached, if the current is in the proper direction, the protective function of the relay is prohibited. In this case, the actuation inhibit circuit failed to work when the minimum current was established and the transformer was isolated by tripping three switchyard breakers. This action also isolated one of two available load feeders powered from the Indian Point 2 generator. The remaining load feeder was out of service for maintenance. Therefore, when transformer TA-5 was isolated, a loss of load on the Indian Point 2 generator also occurred.

The loss of electrical load caused the main turbine to overspeed and trip on mechanical overspeed. The turbine trip caused a reactor trip. The generator remained operational for an additional 7 s until an overcurrent condition on the unit auxiliary transformer caused the generator to trip. While the generator remained online, the frequency increased from 60 Hz to approximately 70 Hz, causing all rotating equipment powered by 6.9-kV buses 1-4 to overspeed. The frequency mismatch prevented the automatic transfer of loads from the unit auxiliary transformer to the station auxiliary transformer, which powers 6.9-kV buses 5 and 6. This caused 6.9-kV buses 1-4 and 480 buses 2A and 3A to lose power. Emergency diesel generator (EDG) 22 started, but did not automatically power 480-V buses 2A and 3A. Motor-driven auxiliary feedwater (AFW) pump 21 did not start when demanded, because it did not have a power supply. Motor-driven AFW pump 23 and turbine-driven AFW pump 22 started as expected.

The 6.9-kV buses 1-4 were manually transferred to the station auxiliary transformer approximately 4 min after the generator trip. All reactor coolant pumps were deenergized during the event, and decay heat was removed by natural circulation cooling, for approximately 40 min, until a reactor coolant pump was restarted.

Each EDG will start following a safety injection signal or when an undervoltage condition exists on any 480-V bus. Following either of these EDG start signals, the EDGs will run at idle speed and can be connected to a deenergized bus manually by an operator in the control room. The EDGs will not automatically load onto a deenergized bus unless a station blackout condition is detected. A station blackout is considered to have occurred if 480-V bus 5A or 6A is deenergized. A safety injection signal concurrent with a station blackout will cause the 480-V buses to be stripped, and the EDGs will then sequence the required safeguards equipment onto the 480-V buses. In the event described in LER 247/97-018, power was never interrupted to 480-V bus 5A or 6A. Therefore, EDG 22 did not automatically power 480-V buses 2A and 3A even though the buses were deenergized.

F.3.3 Basis for Selection as an "Interesting" Event

The sequence of events affecting the Indian Point 2 electrical system prevented the fast transfer of 6.9-kV buses 1-4 from the unit auxiliary transformer to the station auxiliary transformer. The EDG logic did not cause 480-V buses 2A and 3A to be automatically energized from EDG 22 when those buses became deenergized. After the unit trip, decay heat was removed from the reactor coolant system by natural circulation for approximately 40 min.

F.3.4 Factors of Interest

The breaker maintenance in the switchyard at the time of this event established the initial conditions that allowed this event to progress the way that it did. The operators were forced to initiate actions to repower 480-V buses 2A and 3A manually. If the operators had been slow to take this action, or if AFW pump 22 or 23 were unavailable, the potential existed for a more severe transient to occur. Additionally, the potential for a transient-induced LOOP was increased in this incident because of the sequence of events in the electrical system that initiated the partial loss of power.

F.3.5 References

1. Licensee Event Report 247/97-018, "Buchanan's Substation Ringbus Breaker Trip Causes IP2 Turbine Overspeed Trip and Reactor Trip," July 26, 1997.
2. Indian Point Nuclear Generating Unit No. 2, *Updated Final Safety Analysis Report*.

F.4 LER Nos. 293/97-004, -006, and -007

Event Description: LOOP occurs during shutdown

Date of Event: March 7, 1997

Plant: Pilgrim 1

F.4.1 Event Summary

The Pilgrim Nuclear Power Station (PNPS) was in a refueling outage (RFO) on March 7, 1997, when the main transformer (MT) failed as the result of an internal short; subsequently, it ruptured and leaked insulating oil around the transformer pad and into the turbine building. Then, on March 31, 1997, while still in an RFO, the plant experienced a complete loss of all offsite ac power (LOOP) due to a severe storm that passed through the area and placed the station in an unusual event for over 20 h.

F.4.2 Event Description

PNPS was in an RFO with their coastal storm preparations and actions procedure in effect in anticipation of an impending Northeaster storm.¹ The LER also states that, "Scheduled maintenance and surveillance activities were suspended and actions initiated to prepare for the storm." In addition, it was noted in the LER that "The preferred source of off-site power, 345-kV transmission lines 342 and 355, was energized. The 345-kV switchyard air circuit breakers (ACBs) 102, 103, 104, and 105 were closed. The startup transformer (SUT) was energized from lines 342 (via ACB-103) and 355 (via ACB-102)." Thus, the SUT was supplying power to safety buses A5 and A6. A new MT [see LER 293/97-004 (Ref. 2) and the additional event-related information below] had been moved onto its pad, but as noted in the LER, "... was neither electrically nor mechanically connected." Because of this, the unit auxiliary transformer (UAT) was also not available. The reactor vessel had been refueled, and the vessel head was installed and tensioned. The reactor mode switch was in the "REFUEL" position.

To better understand the following sequence of events, refer to Fig. F.4.1, ac power distribution at PNPS. [This figure is a compilation of Final Safety Analysis Report (FSAR) Fig. 8.2-1, Rev. 13 (Ref. 3)] and an unnumbered figure from Appendix B of the PNPS *Individual Plant Examination* (IPE).⁴ At 2221, March 31, 1997, ACBs 102 and 105 tripped open, line 355 de-energized and re-energized, ACB 102 automatically closed, but ACB 105 remained open (this is consistent with their design functions). The possibility of a lightning strike in the switchyard prompted a switchyard walkdown. After the walkdown had revealed no damage, the regional power authority, REMVEC, issued switching orders that directed the operators to manually close ACB 105. Instrumentation information from the 67 m (220 ft) meteorological tower was lost at 2320, probably due to a lightning strike; however, information from the 49 m (160 ft) tower was not affected. Then, at 0135 on April 1, 1997, ACBs 102 and 105 tripped open again, and again ACB 102 automatically closed but ACB 105 remained open (in accordance with their design). Power was lost to two 120-V ac buses, causing various engineered safety features (ESF) initiations. The operators reset the regulating transformers, re-energized the buses, restarted salt service water pump (SSWP) 208D, and reactor

building closed cooling water pumps (RBCCWPs) A and B that had tripped as a result of the power loss to the 120-V ac buses. The ESF actuations were reset, along with the buses, within 25 min. At 0209, ACB 102 tripped open again; however, at this time ACB 105 still had not been reclosed following its opening at 0135. The 120-V ac buses lost power again along with the associated ESF actuations. At 0225, in accordance with REMVEC switching orders, ACB 102 was tagged open. Operators started emergency diesel generator (EDG) A and connected it (i.e., loaded) to its associated safety bus, A5, at 0234. They also started EDG B and loaded it to its respective safety bus, A6, at 0238. ACB 103 tripped open at 0257, causing a SUT lockout. As a result, buses A1, A2, A3, and A4 were all de-energized. In addition, normal control room lighting was lost, condensate and feedwater were lost, the main condenser circulating water pumps tripped, the reactor recirculating pumps tripped, the reactor protection system motor-generator sets tripped, a reactor scram signal was generated, primary containment isolation system (PCIS) Groups 1, 2, 3, and 6 were actuated causing a loss of shutdown cooling (SDC), and fuel pool cooling (FPC) was lost.

At this time, additional people were called to the site. In accordance with plant procedures and guidelines, the lockout relay on the SUT could not be reset until the cause for the lockout had been determined. Following REMVEC switching orders, the operators tagged open ACB 104, thus isolating the plant from its normal and preferred sources of offsite power. SDC was restored at 0310. The station blackout diesel generator (SBODG) was started at 0325; meanwhile, the weather conditions at the plant were, in the words of the LER, "50-60 mph [80-97 km/h] winds from the northeast with stronger wind gusts and heavy snow -- 'white-out' conditions." The 23-kV line from Manomet was lost at 0339, resulting in a complete LOOP to the station. The licensee declared a unusual event (UE) at 0349, which remained in effect for more than 20 h. FPC was restored at 0530, using a temporary power source with a "jumper" cable. Water was discovered entering the radwaste building (RWB) with an accompanying alarm shortly after 0600. At 0643, 23-kV power was restored to the site; however, line voltage was not stable enough to terminate the UE. Three inches (in.) (7.6 cm) of water were discovered in the residual heat removal (RHR) train B room. REMVEC re-energized line 342 by 0926; however, line 342 is de-energized again at 0942 because of unstable line voltage. At 1100, the operators, following an inspection of the reactor building, determined that the 3.8 cm (1.5 in.) of water in the reactor core isolation cooling (RCIC) room and the 7.6-10 cm (3-4 in.) of water in the RHR B room were less than the assumed minimum for the plant flooding analysis. The RHR B and RCIC room level alarms were cleared by 1246, but another flood alarm was received at 1250. The latest alarm, however, indicated that there was 5 cm (2 in.) of water in the torus room. All area flooding alarms were cleared by 1411. Line 342 was re-energized with no further interruptions at 1731 by REMVEC. The LER indicated that, "ACB-103 was not closed because the results of SUT oil sample testing had not been completed." Line 355 was re-energized and ACBs 104 and 105 were closed at 2144. The SUT lockout relay was finally reset at 2338, and the SUT was re-energized at 2339. ACBs 102 and 103 were closed at this time. The event was terminated with the UE termination at 2347.

As indicated above, a new MT was in place but unavailable since the old MT had catastrophically failed on March 7, 1997 (Ref. 2). Before the transformer failure, PNPS was in an RFO, the reactor was defueled, the reactor cavity was "flooded up" and separated from the spent fuel pool, RHR was in augmented FPC mode II (AFPC), the SUT was out of service (OOS) for maintenance, EDG A was OOS for maintenance, EDG B was in standby, and "Portions of the station's 4.16-kV auxiliary power distribution system were being powered from the UAT that was energized by the 345-kV switchyard via ACBs 104 and 105 and the main transformer." This last condition is known as "backscuttlng," whereby the main transformer is used in a step-

down mode as opposed to its normal step-up mode. At 1449 on March 7, 1997, ACBs 104 and 105 tripped open due to the transformer failure, which resulted in the safety buses A5 and A6 losing power momentarily and subsequently losing their loads. Bus A5 was repowered by its backup source, bus A8, since its associated EDG was OOS. Bus A6 was re-energized by EDG B. As a result of the transformer failure, approximately 20,400 L (5,400 gal) of transformer insulating oil was lost; some spilled around the transformer locally, and the rest leaked into the turbine building. The fire brigade was activated, and the licensee monitored the oil spill at the transformer pad and various rooms in the turbine building (e.g., the 4-kV switchgear room B, the main condenser room, and the radwaste corridor). The transformer was isolated electrically and grounded by 1537, and AFPC was restarted at 1540. The spent fuel pool temperature had increased 1°C (2°F) during the time AFPC was lost. A manual start of the SBODG was attempted at 2125 to account "...for shutdown safety considerations...". However, the SBODG tripped on a low engine oil pressure lockout signal. The licensee performed a special test of the SBODG on March 19, 1997, and determined as a result of that test that "The satisfactory results of the test provide reasonable assurance the SBODG would have started satisfactorily within 10 min if a total loss of off-site power condition (station blackout) had occurred on March 7, 1997." Several other sources of information are available (see Refs. 5-8), as well as two NRC Information Notices (IN 97-21 and IN 97-37) pertaining to this event. The MT was subsequently replaced; however, the new transformer was not available when the severe storm occurred on March 31, 1997.

F.4.3 Basis for Selection as an "Interesting" Event

The event that occurred on March 7, 1997, involved the failure of the MT while the plant was shut down and in an RFO. The damage was contained, and the spread (spill) of oil did not exceed design limits or expectations for flooding or fires. The event took place more than 15 d before the complete LOOP on April 1, 1997. An important effect resulting from this event was the destruction of the MT. This caused the plant's ac power distribution to be in a unique state until the MT could be replaced. Thus, when the LOOP occurred on April 1, 1997, the new MT was still OOS. Further, on March 7, all the spent fuel was in the refuel pool, since the reactor was defueled, but as noted in the LER, the temperature of the pool only rose 2°F during this event, and the main concern was the prevention of possible fires from the spilled oil. Additionally, the 23-kV offsite power source was never lost, and the plant was in an unusual electrical lineup (backskuttle) that has since been prohibited by revised plant procedures. Therefore, based on all this, there was no risk for core damage during this event.

The event described in LER 293/97-007 was a LOOP for about 3 h during a major storm (Northeast blizzard) that hit the Cape Cod area on March 31, 1997, through April 1, 1997. Several items mitigated the potential for core damage resulting from the LOOP. First, as noted above, the MT was OOS; as a result, the UAT was also electrically unavailable. Obviously, the main generator was also unavailable since the plant was shut down. The plant was in cold shutdown, head on, refueled following an outage that began February 15, 1997; hence, there was very little decay heat contained in the fuel. Most importantly, however, was that since the MT was OOS, the plant was prevented from starting up in accordance with the plant Technical Specifications. Therefore, this event could not have occurred while the plant was at power. Also the LER indicated that the plant lost one 345-kV (Bridgewater SubStation) offsite power source first, and then the switching authority, REMVEC, ordered the plant to disconnect (tag open) the ACBs. The second offsite 345-kV line from Canal SubStation was lost almost 45 min later (again REMVEC ordered one of the ACBs tagged open). This last line loss caused a lockout on the SUT. When the first 345-kV line was tagged open,

the plant, in accordance with their coastal storm procedures and preparations, separated from the grid (i.e., the SUT supply) and started and loaded both EDGs, so that the plant was independent of the grid. If the plant is at power when the coastal storm procedures are in effect, the operators have the option to shut the plant down. When the second 345-kV line tripped, the plant started and placed the SBODG in standby. The last offsite power source (23-kV from Manomet SubStation) was lost about 45 min after the last 345-kV line was lost. Power was restored to the 23-kV line about 3 h later, and the 345-kV lines were restored about 5 h after that.

Based on the above, the two events taken together did not constitute a significant risk for core damage. The conditional core damage probability for this event is less than the minimum required for it to be considered as an accident sequence precursor; however, because it involved an unusual plant electrical lineup and was extremely complicated, the event is documented here. Moreover, the effects from the long duration storm (more than 24 h) and the loss of three separate offsite power sources further reinforced this notion of documentation.

F.4.4 Factors of Interest

The lessons learned from the March 7 incident were applied during the event that occurred on April 1, 1997. The licensee learned that the SBODG was vulnerable to a loss of ac power to its auxiliary systems, which could have disabled the diesel; however, when the storm hit Cape Cod and before the SBODG was demanded, the licensee had the diesel running in standby. Also, the licensee prohibited future use of the backscuttling lineup for transformers connected to offsite power sources.

F.4.5 References

1. LER 293/97-007, Rev. 0, "Safeguards Buses De-Energized and Losses of Off-Site Power During Severe Storm While Shut Down," May 1, 1997.
2. LER 293/97-004, Rev. 0, "Loss of Preferred Off-Site Power and Oil Spill Due to Main Transformer Fault While Shut Down," April 7, 1997.
3. *PNPS Updated Final Safety Analysis Report, Revision 19*, July 1, 1996.
4. *PNPS Individual Plant Examination*, September 1992.
5. NRC Weekly Information Report for the Week Ending March 14, 1997.
6. NRC Weekly Information Report for the Week Ending March 21, 1997.
7. NRC 10 CFR 50.72 Report No. 31912, March 7, 1997.
8. NRC Headquarters Daily Report, MR No. 1-97-0018, March 12, 1997.

Fig. F.4.1. The ac power distribution system at the Pilgrim Nuclear Power Station. (Based on Fig. 8.2-1 of the *PNPS Updated Final Safety Analysis Report, Revision 19*, July 1, 1996 and Appendix B of the *Individual Plant Examination*.) NO is normally open, xmfr is transformer.

F.5 LER Nos. 333/97-001, -002

Event Description: Fouling of the circulating water system traveling screens

Date of Event: January 23, 1997

Plant: FitzPatrick

F.5.1 Event Summary

FitzPatrick was operating at 100% power on January 23, 1997, when the water level in the intake bay for the plant's circulating water system (CWS) began to drop. When securing a CWS pump failed to restore the water level in the CWS intake bay, operators manually scrammed the reactor. Approximately 11 h after the scram, operators attempted to align the residual heat removal (RHR) system in the shutdown cooling (SDC) mode of operation. Compressing the air in the system suction piping led to pressure pulsations which caused the SDC system to isolate.

F.5.2 Event Description

At 2210 on January 23, 1997, FitzPatrick was operating at 100% power when the water level in the intake bay for the plant's CWS began to drop. Suspecting that the CWS traveling screens had become obstructed by frazil ice, control-room operators aligned a tempering (warming) flow to limit potential icing on the screens. Other operators were sent to the intake screenhouse to determine the status of the traveling screens. Operators found the shear pin for screen A was found to be sheared, which had prevented automatic backwash and cleaning of the screen. The backwash system for screens B and C had been left in manual mode to support maintenance work. When operators attempted to backwash screens B and C, the shear pins on these screens also sheared because of heavy debris accumulation. Continued attempts to restore the screens to an operable status were unsuccessful.

The accumulated debris obstructing the screens, later determined to be comprised mainly of small fish, continued to obstruct circulating water flow. Control room operators reduced reactor power and removed one of three CWS pumps from service, but the water level in the intake bay continued to drop. At 2224, operators then manually scrammed the reactor from 57% power and shut off a second CWS pump. The reduced CWS flow allowed the water level in the bay to recover. Approximately one and one-half hours after the scram, the remaining circulating water pump was shut down to facilitate repairs to the CWS traveling screen system. CWS was unavailable for 13 min.

At 0937 on January 24, 1997, (about 11 h after the scram), RHR pump D was started to provide SDC, but the inboard and outboard SDC system isolation valves immediately received an isolation signal and closed. The isolation signal was determined to have been caused by the presence of air in the SDC suction line. Upon alignment and startup of the RHR system, water entering the piping compressed the air in the suction piping, resulting in a pressure transient at the suction piping pressure switches. These switches, sensing an apparent high suction pressure of 0.5 MPa (75 psig), initiated an SDC isolation.

The RHR system was filled and vented and a second, successful, attempt was made at 1256 to place the system in service.

F.5.3 Basis for Selection as an "Interesting" Event

FitzPatrick has experienced SDC isolations in the past (LER Nos. 93-005, 92-046, 91-011, 90-013, 90-020, and 90-016). Several procedural improvements were implemented to improve system venting. A modification to the pressure instrument sensing line to prevent air traps was completed and the operating procedure was revised to vent the SDC suction piping in an effort to eliminate SDC isolations in 1993 (LER No. 93-005). This included a requirement to cycle the inboard and outboard SDC suction isolation valves. Because of the configuration of the piping (i.e., lack of a high point vent), difficulty in venting the piping has been experienced. Due to an inadequate vent path, air can remain in the SDC suction piping. Difficulty in venting the piping was documented and a deficiency/event report, issued in June 1995, recommended the installation of a high-point vent at the top of the suction piping. This recommendation was given a low priority due to the absence of SDC isolation problems since 1993.

F.5.4 Factors of Interest

FitzPatrick had experienced SDC isolations in the past and its own deficiency/event report recommended installing a high-point vent at the top of the suction piping. During the January 23, 1997, transient, SDC was lost for 3 h and 20 min. No increase in the temperature in the reactor coolant system is indicated. Further, except for about 13 min, CWS was always available because the minimum elevation in the Screenwell during the transient was 73 m (239 ft). At this level, the RHR service water, essential service water, and the fire pumps would have been able to perform their safety function because the intake water level returned to normal when the nonsafety related CWS pumps were removed from service. Corrective actions to be taken at FitzPatrick this time include installing a high-point vent to improve the ability to vent the RHR SDC suction piping.

F.5.5 References

1. LER No. 333/97-001, Rev. 1, "Manual Reactor Scram Due to Fouling of the Circulating Water System Traveling Screens," February 13, 1998.
2. LER No. 333/97-002, Rev. 0, "Shutdown Cooling Isolation," February 24, 1997.

F.6 LER No. 461/97-018

Event Description: Normal power supply breaker for safety bus fails to open

Date of Event: August 23, 1997

Plant: Clinton Power Station, Unit 1

F.6.1 Event Summary

On July 22, 1997, the plant was in cold shutdown when operations personnel at the Clinton Power Station (CPS) were changing offsite power sources for the Division 1 4.16-kV bus 1A1 electrical distribution system from the reserve auxiliary transformer (RAT) to the emergency reserve auxiliary transformer (ERAT).¹ During this evolution the reserve feed circuit breaker is closed and the main feed circuit breaker for Division 1 is opened; however, the main feed circuit breaker did not open as expected because the circuit breaker contacts were in an intermediate condition. This resulted in two separate offsite power supplies supplying the Division 1 electrical distribution system. On August 5, 1997, during a swap of the residual heat removal (RHR) pump A to pump B, the A RHR pump circuit breaker failed to open on demand. On August 23, 1997, during a review of the results of the maintenance performed on all Westinghouse model safety-related circuit breakers, personnel determined that the condition of three circuit breakers (of the 75 tested) was similar to the condition of two Westinghouse model DHP safety-related circuit breakers that failed to open on demand on July 22 and August 5, 1997. Station personnel determined that this condition represented a situation that could have prevented the circuit breakers from fulfilling their safety function to shut down the reactor and maintain it in a safe shutdown condition.

F.6.2 Event Description

On July 22, 1997, at about 1307, the plant was in cold shutdown when control room operators were transferring the power supply for Division 1 4.16-kV bus 1A1 from the RAT to the ERAT (Fig. F.6.1). The operator closed the ERAT feed breaker switch, thereby closing the ERAT feed breaker to bus 1A1. The operator allowed the ERAT breaker control switch to return to "AUTO," which should have automatically tripped open the RAT breaker. As expected, the red "breaker-closed" position indicating light for the RAT breaker went out, but the green "breaker-open" light for the RAT breaker did not come on. Also, an expected "auto breaker trip" annunciator signal was not received. These indications signified that the RAT breaker had failed to trip open, which was further confirmed by the operators noting that the ammeters indicated there was load on both the RAT and ERAT powering bus 1A1. At 1311, the RAT breaker failed to open on a second attempt. At this time, the RAT and ERAT were both supplying power to bus 1A1 (Ref. 2).

At 1312, the control room operators sent an operator to the Division 1 switchgear. Smoke was observed coming from the upper portion of the RAT main feed breaker cubicle. The fire brigade was called out, but they reported that there was no fire in the cubicle. The licensee later determined that when the breaker failed to open, the designated auxiliary "a" contact did not deenergize the trip coil as it normally would. The trip coil, being designed only for momentary energization, had overheated and opened, terminating the over-

temperature condition that had produced the smoke. The RAT breaker again failed to open on a third attempt at about 1315.

Operators assessed the impact on electrical loads and plant conditions with a loss of bus 1A1 and decided to deenergize the bus to safely deal with the RAT breaker. The operators removed the major loads from bus 1A1, including RHR pump A (at 1311) and the reactor water cleanup pump (at 1335). RHR pump B was placed into operation (at 1407) to maintain core cooling. The ERAT breaker was then opened.

A visual inspection of the breaker indicated that the trip coil had severely overheated and that the trip trigger below the trip coil was not fully down and reset, indicating that the trip mechanism was unlatched, and the breaker mechanical position indication was intermediate, that is, only partially open.

A plan was developed by engineering and maintenance, with assistance from Westinghouse personnel, to determine the cause of the circuit breaker's failure to open. Various tests and inspections of the circuit breaker were performed onsite with the assistance of Westinghouse personnel to determine the cause of the circuit breaker's failure to open. This inspection and testing did not reveal any abnormalities that were believed to be the cause of the failure. The circuit breaker was then sent off site to a Cutler-Hammer facility for further inspection. Cutler-Hammer is the current manufacturer of this circuit breaker model. The inspections, tests and disassembly activities performed at the Cutler-Hammer facility did not reveal any single deficiency that could explain the failure of the circuit breaker to open on July 22, 1997. Inspections included checks of the following items: operating linkages for misalignment or physical damage, puffer tube assembly condition and alignment, degraded lubrication, loose debris, spring strength, bearings, and trip latch.

On August 2, 1997, the Division 1 RHR pump A was placed in the shutdown cooling (SDC) mode to maintain core cooling. On August 5, 1997, at 0359, the Division 2 RHR pump B was started and placed in the SDC mode to secure Division 1 equipment for the purposes of conducting surveillance tests. After the operators placed RHR pump B in the SDC mode, the discharge valve for RHR pump A was closed. Attempts to stop RHR pump A by opening the circuit breaker to the pump failed. When the control room hand switch was turned to open the breaker, as expected, the red "breaker closed" light position indicating light for the RHR pump A breaker went out, but the green "breaker-open" light did not come on. In addition, control room indicators for pump flow and motor current did not fall to zero as expected. These indications meant that the pump had not stopped. When the hand switch was released, the red "breaker-closed" light did not come on. RHR pump A discharge valve was immediately reopened to prevent overheating the pump (which placed both Divisions 1 and 2 in SDC mode). The licensee estimated that RHR pump A operated for ~10 s with its discharge valve closed.

At 0413, the control room operators dispatched operators, electricians, and engineers to the Division 1 switchgear (bus 1A1) to determine the actual breaker position and condition. Unlike the bus 1A1 RAT main feed breaker event, no smoke was observed coming from the RHR pump A breaker cubicle. The licensee later determined that with a different control circuit, the RHR pump A breaker's trip coil was deenergized upon releasing the hand switch; hence, it did not severely overheat and smoke.

Personnel at the switchgear noted that the red "breaker-closed" local position indicating light on the cubicle door was illuminated. After the door to the breaker cubicle was opened, the licensee observed that the breaker

was not fully open, but in the intermediate position. Because bus 1A1 was still energized, the licensee discontinued the breaker investigation until the bus could be de-energized.

The licensee then developed procedures to remove electrical loads from the bus and de-energize bus 1A1. At 0749, with bus 1A1 stripped of its loads and the Division 1 diesel and RAT main feed breaker to the bus locked out, the control room operators opened bus 1A1 ERAT feed breaker and de-energized bus 1A1. However, the RHR pump A breaker under voltage relay dropped out upon de-energizing the bus and because the fuses for control power to the breaker had not been removed, the breaker's trip coil energized again. This action still did not fully open the breaker.

On August 6, 1997, a team made up of circuit breaker manufacturer experts, independent circuit breaker experts, failure analysis experts, and site maintenance and engineering personnel was formed to determine the cause of the circuit breaker to fail to open. This team, after extensive inspection and testing of the circuit breaker, determined that the cause of the failure of the circuit breaker to open was that the sum of the opening forces in the circuit breaker were not sufficient to overcome the friction from rough and unlubricated main and auxiliary contacts and degraded lubrication. The friction in the contacts was the largest contributor to the additional friction force in the circuit breaker. At that time, the condition of the other Westinghouse safety-related model DHP circuit breakers at the plant was indeterminate.

As a result of the two recent failures of the Westinghouse 4.16-kV breakers, corrective maintenance was instituted for all of the remaining Westinghouse 4.16-kV breakers (75 breakers).³ While performing this maintenance on other Westinghouse breakers, conditions similar to the two failed breakers were detected, although none of those breakers had actually failed. The similarities noted were (1) rough and unlubricated main and auxiliary contacts and (2) degraded lubrication. Because of these similarities, it was believed that the physical condition of the installed circuit breakers presented a condition that could have prevented the circuit breakers from fulfilling their safety function to shut down the reactor and maintain it in a safe shutdown condition.

F.6.3 Basis for Selection as an "Interesting" Event

The circuit breakers that failed at CPS were Westinghouse Type DHP, 4.7-kV-rated, air-magnetic circuit breakers. DHP breakers of various current ratings are used in both safety-related (Divisions 1 and 2) and non-safety-related portions of the 4.16-kV electrical distribution system at CPS.²

The main and arcing contacts of the breaker are opened normally by the energy stored in the opening springs (which act on the moving contact arm drive linkages) and the kickout springs (that act directly on the moving contact arms themselves). The opening energy is stored in the springs by the action of the closing operation, that is, some of the energy that is expended by the closing spring in closing the breaker stores energy in the springs used to open the breaker.

The opening operation may be initiated (i.e., the breaker may be tripped) manually or electrically. Manual tripping is accomplished by lifting the trip trigger on the front of the breaker by hand. This same trip trigger is lifted by the trip coil in electrical operation in response to local or remote hand control switches or automatic signals such as from protective relays, interlocks, or load shedding functions. Lifting of the trip

trigger unlatches the tripping mechanism, which releases the mechanical lock on the contact operating mechanism. This allows the contacts to move with the force of the opening springs (during the entire opening operation) and the kickout springs (used to disengage the main and arcing contacts at the beginning of the opening stroke).

The history of the failed DHP breakers includes the bus 1A1 RAT main feed breaker (on July 22, 1997) and the RHR pump A breaker (on August 5, 1997). The last full preventive maintenance (PM) was performed on the bus 1A1 RAT breaker on July 20, 1993. On May 23, 1997, the breaker was racked in (closed) and on May 24, 1997, the bus 1A1 RAT breaker was closed and opened ~9 times. The RHR pump A breaker was cycled open and closed ~9 times between June 12 and August 2, 1997, when the RHR pump A was started in SDC mode for the last time prior to its failure to open.

Twenty-four of the 75 breakers that were inspected following the two breaker failures perform safety functions. Four of these 24 safety-related breakers are associated with the ATWS trip of the recirculation pumps (2 per division). The remaining 20 breakers are divided into two divisions (10 per division). Of the 20 breakers, only the normal offsite power feed breakers to the safety buses are normally closed and must open to perform their safety-related function.⁴

After the RHR pump A breaker failed to trip open on demand on August 5, 1997, operations personnel declared all Westinghouse 4160-V safety-related breakers inoperable. Consequently, the plant entered the Technical Specifications (TS) Limiting Conditions for Operation (LCO) Action Statements that require the equipment (breakers) to be returned to an operable status "without delay and in a controlled manner." On August 30, 1997, the plant was in Mode 4 (cold shutdown) undergoing a refueling outage when all non-essential personnel were given the Labor Day holiday weekend off (3 days). This suspension of work activities constituted a violation of the TS LCOs.⁵

It was evident from the AIT report that only the "failure to open" mode for the breakers was a concern. That is, the breakers would close when demanded. Since only 2 of the 75 breakers affected by the failure mechanism are required to open as a safety function, this event analysis focused on those 2 breakers. As a result, loss of offsite power (LOOP) events are important to this analysis because the breakers must open before the emergency diesel generators (EDGs) can load. In this event, failure of the RAT breaker 1A1 to open prevents EDG A from loading onto its safety bus because interlocks that monitor the position of the auxiliary contacts in the breakers prevent the EDG output breaker from closing. Also, the alternate feed from the ERAT is similarly prevented from closing due to additional interlocks between the RAT normal feeder breaker and the ERAT alternate feeder breaker for the bus. For LOOPS recovered in less than 10 min, the operators will not have had enough time to reposition (i.e., open) the failed breaker before incoming power is restored. As was the case during the observed RAT breaker failure, this is expected to damage the breaker and result in a substantial delay in recovering power to the bus. Note that this condition is also true for the other safety bus and its normal offsite power supply from the RAT, its alternate offsite power supply from the ERAT, and its emergency power supply from its EDG. For LOOPS lasting longer than 10 min, the operators will have time to reposition the failed breaker locally at the breaker cubicle; thus, the EDG will be able to supply emergency loads and power the bus after a minor recovery action.

F.6.4 Factors of Interest

The NRC sent an Augmented Inspection Team (AIT) to CPS on August 5, 1997. The findings and conclusions from the AIT investigation are significant because it concluded that both circuit breaker failures were caused by inadequate and inappropriate maintenance activities and by deficiencies in CPS' corrective action system. The combined deficiencies resulted in a potential common mode failure being introduced for all 4.16-kV circuit breakers at CPS manufactured by Westinghouse Corporation. The findings and conclusions of the AIT investigation read, in part:²

... the AIT concluded that the failure to properly maintain the safety related electrical circuit breakers introduced a common mode failure into at least all 4.16-kV Westinghouse electrical circuit breakers at CPS.

Maintenance on breakers over their life has not been consistent with vendor recommendations (see NRC Inspection Report No. 50-461/97003) for frequency or scope of preventive maintenance. In this case, the most significant item was failure to adequately maintain and lubricate the main and arcing contact (both moving and stationary). Further, there has been a history at CPS of using unapproved cleaning agents which could have led to the removal or contamination of existing lubrication.

Inspection Report No. 50-461/97003 identified a number of items associated with breaker maintenance and corrective actions for past breaker failures. CPS' assessment of that inspection report did not effectively address the scope of the potential problems and therefore did not identify and implement effective corrective actions. Specifically, CPS failed to identify that the main and arcing contacts were not being lubricated and, therefore, did not include a specific check for contact condition in their short term corrective actions.

CPS' response to the July 22, 1997, breaker failure did not appropriately integrate the failure and historical problems with breakers into a comprehensive investigation plan. The breaker's as-found condition was not preserved and the breaker was cycled several times prior to sending it to the vendor for additional inspection. Even though the breaker was sent to the vendor, the scope of work authorized by CPS did not provide a comprehensive assessment of the breaker. CPS' and the vendor's lack of understanding of the breakers operation also contributed to the poor evaluation of the failure. For example, the condition of the main and arcing contacts was observed; however, no significance was placed on their condition.

The AIT also evaluated CPS' investigation into the August 5, 1997, breaker failure and concluded that overall the methodology was a significant improvement over that used for the July 22, 1997, breaker failure. The licensee took prudent action in quarantining RHR pump A breaker to preserve the as found condition of the breaker following its failure. Contracted engineering consultants and industry experts comprising the SIT [the licensee's Special Investigation Team] provided guidance to the licensee to inspect the breaker methodically and determine a possible root cause.

The SIT determined that the primary cause for the breaker failure was that available opening forces were insufficient to overcome the system's resistances. At this point however, the SIT appeared to focus on the system resistances associated with the main contact blades and did not initially consider all potential sources of system resistance, e.g., the potential contribution from pole shaft bearing. Further, the SIT did not consider the opening forces during their initial investigation. Specifically, the SIT did not initially consider the kick-out and opening springs as being potential contributors to the failure. AIT discussions with the SIT regarding these issues resulted in a more complete evaluation being conducted.

The SIT's final determination, that lack of appropriate maintenance of the main and arcing contacts combined with a short and bent kick-out spring were the causes of the August 5, 1997, RHR pump A breaker failure was consistent with the AIT's independent evaluation.

F.6.5 References

1. LER No. 461/97-018, "Inadequate Preventive Maintenance Leads to Possible Failure of Westinghouse DHP Circuit Breakers to Open on Demand," September 19, 1997.
2. "NRC Region III Augmented Inspection Team Review of the Failure of the Residual Heat Removal pump 'A' Circuit Breaker to Open on Demand," Inspection Report 50-461/9701, November 24, 1997.
3. 10 CFR 50.72 Report No. 32808, "Westinghouse 4160 Volt Breaker Lubrication Problem Discovered," August 23, 1997.
4. Personal communication, P. M. Thompson, Illinois Power Company, Clinton Station, and D. A. Copinger, ORNL, March 9, 1998.
5. LER No. 461/97-024, "Failure to Comply with the Technical Specifications Action Statement to Immediately Restore ac Power Sources Due to Inadequate Interpretation of the TS Action," October 29, 1997.
6. Clinton Power Station, *Individual Plant Examination—Final Report*, September 1992.

Fig. F.6.1 Electrical distribution system for Clinton. (RAT is the reserve auxiliary transformer, ERAT is emergency reserve auxiliary transformer, and EDG is emergency diesel generator.) (Source: Clinton Power Station, *Individual Plant Examination—Final Report*, September 1992.)

Appendix G:
Resolution of Comments on the
Preliminary 1997 Precursor Analyses

Appendix G

G.1 Comments

This appendix contains the comments received from the applicable licensees and the Nuclear Regulatory Commission (NRC) staff for the 1997 precursors. The comments for each 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. Because of the length of the comments received, they are paraphrased, if necessary, 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 precursors resulted in revisions to the preliminary precursor analyses contained in Appendix B of this report; these events are noted in Table G.1.

Table G.1 List of Comments on Preliminary Precursor Analyses

Event number	Plant	Event descriptions	Page
LER 270/97-001	Oconee 2	Unisolable reactor coolant system leak	G.2-1
LER 287/97-003	Oconee 3	Two high-pressure injection pumps were damaged because of a low water level in the letdown storage tank	G.3-1
LER 289/97-007, -008, and -010	TMI 1	Failure of both generator output breakers causes a LOOP	G.4-1
LER 309/97-004	Maine Yankee	Reactor coolant system hot-leg recirculation valves subject to pressure locking because of post-LOCA thermal expansion of the trapped water	G.5-1
LER 335/97-011	St. Lucie 1	Nonconservative recirculation actuation signal set point	G.6-1

G.2 LER No. 270/97-001

Event Description: Unisolable reactor coolant system leak

Date of Event: April 21, 1997

Plant: Oconee 2

G.2.1 Licensee Comments

Reference: Letter from W. R. McCollum, Jr., Site Vice President, Oconee Nuclear Sites, to U. S. Nuclear Regulatory Commission, "Comments on Preliminary Accident Sequence Precursor Analysis of Operational Event at Oconee Nuclear Station, Unit 2 (LER No. 270/97-001)," February 24, 1998.

As discussed below, Duke believes that the value assigned to the conditional probability of a small-break loss-of-coolant accident (SLOCA) is not appropriate and that the failure probability of the high-pressure injection (HPI) system to respond to the HPI line break, which is used in this preliminary analysis is conservative compared to the plant-specific reliability estimate.

Comment 1: Conditional SLOCA Probability – While the Swedish Nuclear Power Inspectorate's (SKI) piping failure database provides a source of information on the frequency of piping failures, it is not reasonable to extrapolate this generic data beyond an estimate of the frequency of events. This small group of events (13 leakage events and no ruptures) is inadequate to make a statistical inference of the conditional probability of pipe rupture. Assigning the value of 0.053 for the rupture probability for the Oconee leakage event based on no ruptures in 13 events is not reasonable in a best estimate analysis process. This approach also ignores the phenomenological aspects of crack growth from thermal cycling and the physical attributes of the piping. For example, the analysis does not consider that the piping material is a highly ductile austenitic stainless steel. Piping stress analysis of the failed Oconee piping material concluded that even with the existing crack, the HPI line had enough remaining strength to provide a factor of safety greater than 2 under design-basis event loads.

As discussed in several communications with the Nuclear Regulatory Commission (NRC),¹⁻⁵ Duke performed extensive metallurgical examination of the failed piping section and determined that the leaking weld crack had propagated over a long period of time, believed to be greater than 2 years. The primary initiator of the crack was high-cycle/low-amplitude

stresses consistent with thermal cycling in the weld region. This type of crack grows very slowly at specific times when temperature and flow variations occur in the reactor coolant system (RCS) or the HPI makeup flow. After the onset of the initial leak [8.9 L/min (2.36 gal/min)] in the April 21, 1997, Oconee Unit 2 event, the leakage rate increased gradually over the next 19 h, peaking at 45 L/min (12 gal/min). The increase in RCS leakage rate between initial discovery and unit shutdown was not believed to be due to additional growth of the crack itself. It is more plausible that the gradual increase in leakage rate was caused by the erosion of material within the opened crack or other undetermined mechanisms. Without substantial additional growth of the crack or a substantial external load [much greater than design-basis accident (DBA) conditions], it is highly improbable that a catastrophic rupture (SLOCA) could occur.

Duke's conclusion from these examinations and analysis was that the probability of complete rupture of this line was still very small. This type of event is not well suited for accident sequence precursor (ASP) analysis given the current state of materials engineering and operational experience and the extrapolation necessary to obtain a conditional probability of the initiating event.

Response 1: Following the receipt of Duke's comments, the probability of pipe rupture was reassessed. Although the pipe rupture probability was reduced by a factor of 2, the revised conditional core damage probability (CCDP) estimate was still above the ASP cutoff value of 1.0×10^{-6} . In the actual event the crack developed slowly and began to leak. This leakage was detected, and the plant was shut down while the injection line remained substantially intact. Probabilistically, however, it is possible that the crack could have developed differently, resulting in a catastrophic failure of the injection line before detection.

To develop an estimate of the conditional probability for a piping failure (crack, leak, or rupture), the SKI piping-failure database⁶ was queried for thermal-fatigue failures. Twenty events involving cracks or leaks in 2.5 to 10 cm (1 to 4 in.) stainless steel piping were identified. Using Bayesian statistics with a binomial noninformative prior,⁷ a conditional probability of rupture given failure of 2.4×10^{-2} was calculated. Although associated with an observed leak, the probability of pipe rupture estimated in the analysis represents the likelihood that the defect *could* have progressed to a rupture at some time during its development, and not necessarily the probability that the leak, as it ultimately developed, *would* have proceeded further to a rupture. This approach is similar to that used in other degradation analyses (as well as in ASP analyses of degraded components).

It is noted in the Modeling Assumptions section that because no ruptures have been observed, this estimate may be conservative. As such, a confirmatory estimate was made using cyclic (vibration-induced) fatigue data. Several of the thermal-fatigue-induced failures in the SKI database also included cyclic fatigue as a contributing factor, which may have been the case in the Oconee event as well. Of the 78 failures, two cyclic fatigue-related ruptures have been observed, resulting in an estimated conditional probability of 3.2×10^{-2} . This is about the same as the estimate for thermally induced fatigue. These values are

consistent with, and in some cases smaller than, the estimates developed in other studies [e.g., Thomas⁸ (2–45%) and Electric Power Research Institute (EPRI)⁹ (9–11%)].

The Modeling Assumptions section was also expanded to acknowledge the potential use of probabilistic fracture mechanics as an alternate to the “data-driven” models used in the ASP event analysis and to note, based on Ref. 6, that under similar boundary conditions, the two methods produce similar (i.e., the same order of magnitude) results.

In addition to the use of the revised conditional probability of pipe rupture, the analysis was revised to describe the significant uncertainty in the probability estimate and the causes of the uncertainty (including the results of one fracture mechanics study that indicated high conditional rupture probabilities for weld cracks in stainless steel piping), and to describe the reasons behind the choice of an SLOCA instead of a medium-break LOCA for the analysis (a medium-break LOCA is indicated based on injection line diameter alone).

Comment 2: HPI System Failure Probability – Duke’s review of the preliminary ASP basic event probabilities showed that most of the values were consistent with Duke probabilistic risk assessment (PRA) analyses, with the important exceptions of HPI-MDP-CF-START (Common-Cause Failure of Motor-Driven HPI Pumps B and C to Start) and HPI-XHE-XM-PMPB (Operators Fail to Align HPI Pump B to Loop B). Duke believes that the values for these events are overly conservative and should be lowered.

In the case of a common-cause failure of HPI pumps B and C to start, the ASP assessment value of 6.3×10^{-4} is a factor of 5 higher than the most recent Duke analysis.¹⁰ This value is also high relative to the ASP failure probability assigned for individual HPI pump train failure (3.9×10^{-3}). Generally, common-cause start failure probabilities should not exceed 10% of the single train start failure probability unless a detailed plant-specific common-cause assessment is performed to support using a higher common-cause value.

Event HPI-XHE-XM-PMPB models the failure of operators to align HPI pump B to RCS loop B by opening motor-operated valve (MOV) HP-409. This action is proceduralized in the Oconee Emergency Operating Procedure (EOP) (EP/2/A/1800/01) under Enclosure 505 “ES Actuation” Steps 2.3 and 2.4. In these steps, operators verify that the minimum injection flow required for each header is met and that HPI pump runout limits are not exceeded. If the required HPI flow to header B is not met, operators are directed to open HP-409. Operators receive extensive training on this enclosure and specifically on HPI line break events. Failure to perform this clear and straightforward action was quantified at 1.0×10^{-3} in the Oconee Individual Plant Examination (IPE) and was verified in more recent analyses.^{11,12} The value used in the ASP analysis is an order of magnitude higher and is considered to be overly conservative.

Response 2: All common-cause failure probabilities used in the analysis have been revised to be consistent with data developed by the Idaho National Engineering and Environmental Laboratory for NRC.¹³ For HPI-MDP-CF-START, this resulted in a reduction in probability to 1.9×10^{-4} . In addition, the probability for HPI-XHE-XM-PMPB was revised to 1.0×10^{-3} to be consistent with the value used in the Oconee IPE.

Comment 3: The question of whether or not the CCDP of this event is less than the precursor threshold (10^{-6}) depends primarily on the value assigned to the conditional probability that the leakage event would have progressed to a small-break event. Duke believes it is very difficult to select a specific value for this probability. Since it is very difficult to assign a number to such a "precursor to a small-break LOCA initiating event", Duke suggests that this event be treated as a "potentially significant event considered impractical to analyze."

Response 3: The significant uncertainty in the conditional probability of an SLOCA given the observed leakage is acknowledged. While the conditional probability used in the final analysis is a factor of two lower than that used in the preliminary analysis, the event still satisfies the criteria for a precursor. As noted in the response to Comment 1, the analysis has been revised to describe the significant uncertainty in the pipe rupture probability estimate and the causes of that uncertainty. As discussed in the above response to Comment 2, the common-cause failure (CCF) probabilities were revised to be consistent with recently published data obtained from industry operational experience.¹³ This resulted in a reduction in many of the key CCF probabilities from the values used in the preliminary analysis of this event. However, the CCF probabilities for the decay heat removal (DHR) heat exchangers and the motor-driven DHR pumps increased significantly. (For the heat exchangers, this was partially due to a change in the effective surveillance interval based on time between shutdowns, similar to the approach used in the Oconee IPE¹¹.) The net result of these changes was an increase of a factor of two in the estimated CCDP for this event.

References

1. J. W. Hampton to USNRC, "Justification for Continued Operation of Oconee Unit 1 Based on Oconee Unit 2 HPI Line Leak," May 2, 1997.
2. J. W. Hampton to USNRC, "Response to Request for Additional Information on the High Pressure Injection (HPI) System," May 9, 1997.
3. J. W. Hampton to USNRC, "Response to Request for Additional Information on the High Pressure Injection (HPI) System," May 13, 1997.

4. J. W. Hampton to USNRC, "Justification for Continued Operation of Oconee Unit 1 Based on Oconee Unit 2 HPI Line Leak – Supplemental Information," May 19, 1997.
5. J. W. Hampton to USNRC, "Justification for Continued Operation of Oconee Unit 1 Based on Oconee Unit 2 HPI Line Leak – Supplemental Information," May 22, 1997.
6. R. Nyman, D. Hegedus, B. Tomic, and B. Lydell, *Reliability of Piping System Components, Framework for Estimating Failure Parameters from Service Data*, SKI Report 97:26, December 1997.
7. *PRA Procedures Guide*, USNRC Report NUREG/CR-2300, January 1983. p. 5-36.
8. H. M. Thomas, "Pipe and Vessel Failure Probability," *Reliability Engineering*, 2:83 (1981).
9. *Pipe Failures in U.S. Commercial Nuclear Power Plants*, EPRI TR-100380, July 1992.
10. Duke Power Company, *Oconee Nuclear Station HPI Reliability Study*, December 1977.
11. Duke Power Company, *Oconee Nuclear Station IPE Submittal Report*, 1989.
12. Duke Power Company, *Oconee Nuclear Station PRA Revision 2 Summary Report*, December 1996.
13. Marshall and Rasmuson, *Common-Cause Failure Data Collection and Analysis System*, INEL-94/0064, December 1995.

G.2.2 NRC Comments

No comments were provided by NRC.

G.3 LER No. 287/97-003

Event Description: Two high-pressure injection pumps were damaged because of a low water level in the letdown storage tank

Date of Event: May 3, 1997

Plant: Oconee 3

G.3.1 Licensee Comments

Reference: Letter from W. R. McCollum, Jr., Site Vice President, Oconee Nuclear Site, to U. S. Nuclear Regulatory Commission, "Review of Preliminary Accident Sequence Precursor Analysis of Operational Event at Oconee Nuclear Station - LER No. 287/97-003," May 27, 1998.

Comment 1: The estimated conditional core damage probability (CCDP) calculated by the Nuclear Regulatory Commission (NRC) for this event (3.3×10^{-5}) is lower than but in the same range as the value calculated by Duke using the current model of the Oconee probabilistic risk assessment (PRA) (8.8×10^{-5}). There are some differences in the way these values were calculated, as addressed below.

Comment 1a: The fraction of time that was assumed for the high-pressure injection (HPI) pumps to be vulnerable to failure as a result of low letdown storage tank (LDST) level differs between the two analyses. The NRC assumed that for 20% of the time between February 22 and May 3, the LDST level was low enough to cause failure of the HPI pumps had they been needed to mitigate a loss-of-coolant accident (LOCA). This was determined from a simplified model of LDST level and pressure as a function of LDST reference leg level during a draw down of the borated water storage tank (BWST). The Duke analysis simply assumed the HPI system to be vulnerable to failure for 50% of the time between February 22 and May 3.

Response 1a: The difference in analysis assumptions is acknowledged. In fact, if the preliminary analysis assumed that the HPI system was vulnerable to failure 50% of the time between February 22 and May 3, the calculated CCDP would be very close to the CCDP calculated by Duke.

Comment 1b: The NRC analysis assumes two separate independent recoveries for small-break (SLOCAs),

- PCS-XHE-XM-CDOWN, which addresses the failure of the operators to depressurize the unit and initiate the residual heat removal (RHR) system prior to HPI failure,
- PCS-XHE-XM-FDEPR, which addresses failure to depressurize to low-pressure injection (LPI) system pressure following loss of HPI.

Duke assumed only one potential recovery.

Response 1b: The difference in the two operator actions is described in the fourth paragraph under **Modeling Assumptions**. Note that PCS-XHE-XM-CDOWN is not a recovery action; it addresses the potential to cool down and place the unit on decay heat removal (DHR) prior to the need for sump recirculation following an SLOCA.

Comment 1c: Duke assumed that it would be possible to depressurize the primary system and initiate DHR using the LPI system for medium-size LOCAs. This was applied as a "recovery" event for cut sets where both steam generator cooling and the LPI system were available. The NRC did not take credit for this potential recovery.

Response 1c: The medium-break LOCA model has been revised to address the potential use of fast depressurization, LPI, and low-pressure recirculation if HPI were to fail late in the injection phase. This is consistent with recovery actions included in the Oconee Individual Plant Examination (IPE) report.

Comment 2: The sensitivity analysis that considers the combined effect of the Unit 3 LDST reference leg leak and the Unit 2 HPI injection nozzle weld leak (LER No. 270/97-001) is not appropriate and adds no value to the analysis of the Unit 3 event. As discussed in the Duke letter of February 24, 1998, in response to the Preliminary Accident Sequence Precursor (ASP) Analysis of LER No. 270/97-001, the precursor treatment of the Oconee 2 HPI injection nozzle leak event is inappropriate. Superimposing this event on another unit's condition introduces additional extrapolations and produces questionable conclusions. Duke suggests that this sensitivity discussion be deleted.

Response 2: The sensitivity analysis has been retained in the analysis of this event. Exploration of the potential impact of a combined event involving an HPI line leak and HPI pump failures is reasonable, considering the timing of the two actual events. The response to comments on the precursor analysis of LER No. 270/97-001 addresses Duke comments on that event.

Comment 3: In conclusion, the NRC analysis of the Oconee event reported in LER No. 287/97-003 appears to have several differences from the Duke analysis of the same event. However, these are understandable differences in assumptions, and neither analysis appears to be in error. Even with these differences, both the NRC and Duke analyses concluded that the CCDP was in the range of 3×10^{-5} to 8×10^{-5} and that the CCDP is above the precursor threshold.

Response 3: The ASP analysis of LER No. 287/97-003 has been revised as described in the response to Comments 1 and 2. While this has resulted in a decrease in the CCDP estimated for the event from the preliminary analysis, it still satisfies the criteria for a precursor.

G.3.2 NRC Comments

No comments were provided by NRC.

G.4 LER Nos. 289/97-007, -008, -010

Event Description: Failure of both generator output breakers causes a LOOP

Date of Event: June 21, 1997

Plant: Three Mile Island, Unit 1

G.4.1 Licensee Comments

Reference: Letter from James W. Langenbach, Vice President and Director, Three Mile Island (TMI), to U. S. Nuclear Regulatory Commission (NRC), "GPU Nuclear Review of Preliminary Accident Sequence Precursor Analysis of Operational Event at Three Mile Island Nuclear Station, Unit No. 1," May 1, 1998.

Comment 1a: On page 1, under **Event Summary**, the fifth sentence states, "The unit was cooled by natural circulation cooling until offsite power was restored." This sentence should state, "The unit was cooled by natural circulation cooling until offsite power and forced cooling were restored." Per LER 97-009 pages 4 and 5, it took 1.5 h for offsite power to be restored. Another 7.5 h passed before forced cooling (RC-P-1A/B/C/D) was restored.

Response 1a: The proposed editorial change was made. This has no effect on the analysis results, but more accurately reflects the sequence of events depicted in the time line outlined in LER 97-009, pages 4 and 5.

Comment 1b: On page 1, under **Event Description**, first paragraph, the second sentence states, "On June 21, 1997, the B phase of the 230-kV power transformer developed a fault causing severe overheating and the subsequent ejection of the bushing and conductor from the breaker housing of output breaker GBI-02 (Fig. 1)." This sentence should state, "On June 21, 1997, the B phase of the 230-kV generator output breaker GBI-02 (Fig. 1) developed a fault causing severe overheating and the subsequent ejection of the bushing and conductor from the breaker housing." Per LER 97-007, there is no evidence that the fault location was in the power transformer.

Response 1b: The proposed editorial change was made. This has no effect on the analysis results.

Comment 1c: On page 1, under **Event Description**, second paragraph, the second to the last sentence states, "All control rods inserted to three-fourths insertion position within 2.2 s." This sentence should state, "All control rods inserted to the three-fourths insertion position well within 3.0 s." Per LER 97-008 there is no claim made that at the time of the reactor trip all control rods inserted to the three-fourths position within 2.2 s. The only claim is that retested rods came in at less than 2.2 s. The LER does indicate that the rods did insert to the three-fourths position well within 3.0 s at the time of the reactor trip.

Response 1c: The sentence was changed to, "All control rods inserted to the three-fourths insertion position within 3.0 s." LER 97-008 only indicates that rod insertion times were below 3.0 s without quantifying any specific rod drop times during the reactor trip. Therefore, the times were not categorized as being "well below 3.0 s." This has no effect on the analysis results.

Comment 1d: On page 1, under **Event Description**, third paragraph, the second sentence states, "Nonvital loads, including circulating water and main condenser vacuum pumps, were not energized." This sentence should state, "Nonvital loads, including main feedwater, condensate, circulating water, and main condenser vacuum pumps, were not energized." The more important non-vital loads per LER 97-007 page 2 were omitted from the event description.

Response 1d: The proposed editorial change was made. This has no effect on the analysis results, but more accurately reflects the scope of major loads lost following the loss of offsite power (LOOP) event.

Comment 1e: On page 2, under **Event Description**, last paragraph, the last sentence states, "After the operators established the main condenser heat sink, the reactor coolant pumps were restarted, returning the reactor coolant system to forced circulation cooling." This should state, "After the operators established the main condenser heat sink, the reactor coolant pumps were restarted. Since the natural circulation cooling of the reactor coolant system was stable, the reactor coolant system was not returned to forced circulation cooling until 9 h after the reactor trip."

Response 1e: LER 97-007 does not indicate that the delay was based on the stability of natural circulation cooling. The last two sentences were changed to, "After operators established the main condenser heat sink, the reactor coolant pumps were restarted. The reactor coolant system

was returned to forced circulation cooling ~9 h after the unit tripped." This has no effect on the analysis results.

Comment 1f: On page 6, Fig. 1: change breaker identification from 1B-14 to 1B-12 per Gilbert/Commonwealth drawing 229-002.

Response 1f: The proposed figure change was made. This has no effect on the analysis results.

Comment 2a: On page 2, under **Additional Event-Related Information**, the first and second paragraphs are considered to place too much emphasis on the power-operated relief valve (PORV) being inoperable. The reactor coolant system pressure did not approach the PORV set point at any time during the LOOP event. Therefore, the PORV being inoperable was not a factor during the LOOP event.

Response 2a: The Accident Sequence Precursor (ASP) Program deals with the probability that the PORV set point may be reached following any LOOP event or that feed-and-bleed cooling operations may be required if emergency feedwater were to fail. In a generic analysis, cut sets would exist in the analysis output indicating that the PORV had opened. However, to correctly model this specific event, the basic event governing the PORV opening needed to be set to TRUE (would not open). Some discussion was required to establish the basis for this basic event change. Because these two paragraphs provide essentially all of the information on the inoperable PORV (there is one sentence under **Modeling Assumptions**), no change in the PORV discussion was made in the analysis.

Comment 2b: On page 2, under **Additional Event-Related Information**, last paragraph, the second and third sentences state, "Additionally one EDG from TMI 2 is available as an alternate ac power source during a station blackout (SBO). The alternate EDG, which is manually started from the control room, can be aligned to either engineered safeguards bus 1D or 1E within 10 min following an SBO." These sentences more correctly should state, "Additionally, one EDG previously from TMI 2 is available as an alternate ac power source during a station blackout (SBO). The alternate EDG, which is manually started from the control room, can be aligned to either engineered safeguards bus 1D or 1E or balance of plant (BOP) bus 1C within 10 min following an SBO."

Response 2b: The proposed editorial changes were made. This has no effect on the analysis results.

Comment 2c: On page 2, under **Additional Event-Related Information**, last paragraph, the last sentence states, "Operators must close two breakers and any desired loads must be manually loaded onto the bus selected to be reenergized." This sentence should state, "Operators must close two breakers and open/lockout two breakers, and any desired loads must be manually loaded onto the bus selected to be reenergized." Per abnormal procedure 1202-2, the operator must open/lockout two breakers in addition to closing two breakers to correctly align the SBO diesel with bus 1D or 1E.

Response 2c: The proposed editorial changes were made. This has no effect on the analysis results because the operator response was not considered on a breaker by breaker basis. The response was simply assumed to be a procedure-based action with a nominal probability of failure to perform the procedure of 1.0×10^{-2} , which is consistent with similar operator responses.

Comment 3a: (1) On page 3, the first paragraph should give a reference for the reliability value used for OEP-XHE-NOREC-SB in Table 1 (of the preliminary analysis).

(2) The two events described in Table 1 of the preliminary ASP analysis, EPS-XHE-NOREC (operator fails to recover emergency power) and OEP-XHE-NOREC-SL (operator fails to recover offsite power before RCP seals fail), should be replaced by the non-recovery values REA and REC given in Table B.1-12 of the TMI Individual Plant Examination¹ (IPE). REA is the nonrecovery factor for SBO sequences in which the emergency feedwater (EFW) operates successfully. REC is the nonrecovery factor for SBO sequences in which EFW does not operate successfully. Both REA and REC were evaluated under the assumption that at least two EDGs are recoverable.

(3) REA and REC were calculated by Monte Carlo simulation techniques as described in Sect. B.1.3.4 of the TMI IPE. Recovery of the TMI 2 emergency diesel generator (EDG) was not credited in the simulation. The result of the simulation shows that if EFW is unavailable, the mean time to core uncover is 3.4 h or 10.3 h if EFW is available. The time interval of 2.1 h to core uncover mentioned in the IPE was used as input to the STADIC code and was assumed to occur after a loss of all ac power. The STADIC model did not assume that all onsite ac power would fail at time $t = 0$ when offsite power is lost. In other words, the time to core uncover was assessed in the IPE (page B.1-16) as the time of onsite power failure, plus 2.1 h.

Response 3a: (1) The text reference to the basic event OEP-XHE-NOREC-SB on page 3 of the analysis was changed to, "Potential recovery actions were modeled (using data from NUREG-1032)

by the addition of a basic event (OEP-XHE-NOREC-SB) under the OP-SBO top event (OP-2H) on the LOOP event tree (Fig. 2)."

(2) In the SBO sequences, the probability of a reactor coolant pump (RCP) seal loss of coolant accident (LOCA) and the probability of failing to recover ac power at various points in time are calculated using a convolution approach that recognizes that all probabilities are a function of time. A Weibull distribution is used to predict the LOOP-related parameters applicable for TMI as defined in ORNL/NRC/LTR-89/11 (Ref. 2). Probabilities associated with the failure to recover ac power and the potential for an RCP seal LOCA are calculated given that ac power was not restored in the short term (30 min). Additionally, the probability for the operator failure to restore emergency power is based on the assumption that the median repair time for an EDG is 4 h, as developed in NUREG-1032. The TMI IPE split fractions, REA and REC, are based on different assumptions concerning LOOP and EDG recovery as a function of time. The electric power recovery analysis described in Appendix B.1 to the TMI IPE imbedded the potential for an RCP seal LOCA within the calculation of REA and REC and did not separately address the potential for short- and long-term recovery of ac power. Because basic events EPS-XHE-NOREC and OEP-XHE-NOREC-SL in the IRRAS model do not represent the same conditional probability that split fractions REA and REC represent, the free substitution of individual split fractions from the IPE into the Integrated Reliability and Risk Analysis System (IRRAS) model is inappropriate without making further adjustments to the other LOOP-related parameters in the IRRAS model.

(3) The ASP IRRAS models do not currently simulate the potential for a delayed failure of EFW. EFW is assumed to essentially fail at event $t = 0$, and the time to core damage under station blackout was assumed to be 2.1 h per Sect. B.1.3.3.3 of the TMI IPE.

Comment 3b: In general, the probabilities for failure of restoration of offsite power, onsite emergency power, and reactor coolant pump seals may be reduced from those assumed in the analysis because operators have the following procedures listed below for guidance. Also, the June 21, 1997, event was successful in that offsite power was restored in 90 min, emergency onsite sources started and loaded as designed, and there was no RCP seal damage.

- Emergency Procedure 1202-2, Rev. 44, "Loss of Station Power," which was used during the TMI 1 event, includes steps (3.10 and Attachment 4) for restoring offsite power. Because of these operator actions the probability of not restoring offsite power (IE-LOOP) should be lower than 5.0×10^{-1} .
- Emergency Procedure 1202-2, Rev. 44, "Loss of Station Power," which was used during the TMI 1 event, includes steps (3.11 and Attachment 1) for starting and loading the EDGs, assuming the EDGs did not automatically start and load. In addition, the

procedure includes steps (3.12 and Attachment 1) for starting and loading the SBO diesel assuming the Class 1E diesel(s) did not automatically start. Because of these operator actions, the probability of all diesels failing (EPS-DGN-CF-ALL) should be lower than 9.5×10^{-4} .

- Emergency Procedure 1202, Rev.44, "Loss of Station Power," which was used during the TMI 1 event, includes Attachment 2, which may be used to restore RCP seals. The restoration would be performed in a controlled manner to limit damage to the seals and pumps if injection and intermediate closed cooling water (ICCW) are lost for a long time period. Because of these operator actions, the probability of RCP seal failure (RCS-MDP-LK-SEALS) should be lower than 4.0×10^{-2} .

Response 3b: Human response is considered in the numerous system-specific operator nonrecovery probabilities within the TMI IRRAS model. The fact that procedural guidance exists is accounted for by the nonrecovery probability basic events. The IE-LOOP initiating event represents the probability that ac power is not restored in the short term and is based on historical data gathered on specific categories of LOOP events. The probability of not recovering offsite power in the short term is included in the initiating event probability (IE-LOOP). That is, the probability of a LOOP is 1.0. The probability that offsite power is not recovered in ~30 min is 0.5, based on the data distributions provided in NUREG-1032, *Evaluation of Station Blackout Accidents at Nuclear Power Plants*.³ Consequently, IE-LOOP was set to the probability of failing to recover offsite power in the short term (5.0×10^{-1}) following a plant-centered LOOP. The conditional probability that a LOOP is not recovered in times greater than 30 min is considered in the calculation of probabilities for basic events OEP-XHE NOREC-SB, -SL, and -BD. Hence, the existence of procedural guidance impacts the historical data and subsequently the value calculated for these probabilities.

With respect to the LOOP event at TMI on June 21, 1997, success of specific systems or components does not change the probability that the LOOP could have lasted longer than 90 min and that core damage could occur. Therefore, the original analysis basic event values were not adjusted for the final report based on the existence of numerous emergency procedures.

- As noted above, the probability that offsite power is not recovered in ~30 min is 0.5, based on the data distributions provided in NUREG-1032 (Ref. 3). The existence of procedural guidance impacts the historical data and subsequently the value calculated for IE-LOOP. The IPE (Table B.1-5) indicates that the probability that offsite power is not recovered in ~30 min is 0.67, which is compatible with the value of 0.5 calculated from the data distributions in NUREG-1032.
- The common-cause failure probability of all three EDGs failing to start and run (EPS-DGN-CF-ALL) is based on data distributions contained in INEL-94-0064, *Common-Cause Failure Data Collection and Analysis System* (Ref. 4, Table 5-8: alpha

factor distribution summary – fail to start, CCCG = 3, $\alpha_{3S} = 0.0224$; and Table 5-11: alpha factor distribution summary – fail to run, CCCG = 3, $\alpha_{3R} = 0.0232$). Because α_3 is equivalent to the β factor of the multiple Greek letter method used in the IRRAS models, the common-cause failure probability of the EDGs was adjusted from 1.6×10^{-3} based on two EDGs to 9.5×10^{-4} based on two EDGs and an SBO diesel generator.

- The probability of an RCP seal LOCA following a postulated SBO event was developed based on data distributions contained in NUREG-1032 and the RCP seal LOCA models that were developed as part of the NUREG-1150 probabilistic risk assessment (PRA) efforts described in *Revised LOOP Recovery and PWR Seal LOCA Models*.² The probability of an RCP seal failure calculated from this source, assuming power is not restored in the short-term (30 min), is 4.0×10^{-2} .

Comment 4: Based on the variation in the combination of events and modeling assumptions used by the NRC in the analysis of the operational event at TMI as described in the preliminary ASP analysis, the estimate of the conditional core damage probability (CCDP) of the LOOP was determined to be 9.6×10^{-6} . Using the combination of events and modeling assumptions of the TMI 1 PRA (Level 1) Update, December 1992, "Appendix B – Special Analysis", which gives consideration to both the REA and REC factors, GPU Nuclear estimates the CCDP of the LOOP to be 9.53×10^{-7} .

Response 4: Numerous basic events in the IRRAS model are based on the conditional probability that an ac power source is not reestablished within 30 min. This is the reason, for example, that the initiating event probability (IE-LOOP) is 0.5 although a LOOP actually occurred. The TMI IPE incorporates these time conditional probabilities into split fractions REA and REC. IE-LOOP would have to be adjusted to 1.0 to accommodate the use of split fractions REA and REC. Adjusting IE-LOOP would subsequently require numerous other basic events to be modified.

As discussed in the response to Comment 3a, the use of a mix of basic event probabilities from the TMI IPE and IRRAS models is not appropriate without accounting for the underlying assumptions associated with substituted values. Collapsing the ASP model SBO sequences to two scenarios, one with EFW available and one with EFW failed, and applying ac power nonrecovery probabilities equivalent to REA and REC, results in an estimated CCDP of $\sim 1.0 \times 10^{-5}$. This is the CCDP for a "nominal" LOOP using nonrecovery probabilities as described in Appendix B.1 of the TMI 1 IPE. Because it was not possible to revise REA and REC to reflect the plant-centered nature of the LOOP, it was not possible to directly compare the impact of REA and REC if they were used in the analysis. Since a plant-centered LOOP is more easily recovered than a nominal LOOP, the associated CCDP would be expected to be lower than the estimate for a nominal LOOP—typically by a factor of 2 to 3. Hence, the plant-centered LOOP at TMI using TMI-developed nonrecovery distributions (from App. B.1 of the TMI IPE) should be in the mid- 10^{-6} range. The original

analysis result, which calculated a CCDP of 9.6×10^{-6} , appears to be a reasonable estimate of the importance of this event.

G.4.2 NRC Comments

No comments were provided by the NRC to date.

G.4.3 References:

1. Three Mile Island, *Individual Plant Examination*.
  2. *Revised LOOP Recovery and PWR Seal LOCA Models*, Report ORNL/NRC/LTR-89/11, August 1989.
  3. P. W. Baranowsky, *Evaluation of Station Blackout Accidents at Nuclear Power Plants*, USNRC Reoprt NUREG-1032, June 1988.
  4. Marshall and Rasmuson, *Common-Cause Failure Data Collection and Analysis System*, INEL-94/0064, December 1995.
-

G.5 LER No. 309/97-004

Event Description: Reactor coolant system hot-leg recirculation valves subject to pressure locking because of post-LOCA thermal expansion of the trapped water

Date of Event: January 22, 1997

Plant: Maine Yankee

G.5.1 Licensee Comments

Reference: Letter from James R. Hebert, Manager Regulatory Affairs Department – Maine Yankee Atomic Power Station, to U. S. Nuclear Regulatory Commission, “Review of Preliminary Accident Sequence Precursor Analysis of Operational Condition at Maine Yankee Atomic Power Station, dated September 3, 1997,” October 15, 1997.

Comment 1: The Analysis Results indicate a core damage probability (CDP) increase of 1.3×10^{-5} . A single “sequence accounts for almost 100% of the total contribution to the increase in the CDP.” It is also stated that “There is substantial uncertainty in this estimate because of the uncertainty in the frequency of a large-break loss of coolant accident (LBLOCA) (none have occurred) and the likelihood of motor-operated valves (MOVs) failing under post-LOCA conditions.”

In fact this “result” is considerably more uncertain than stated; it is based almost solely on assumptions; it probably represents a significant overestimate of the CDP. This analysis unrealistically assumes no credit for any recovery action. The single sequence is calculated from the following:

Sequence Element	Value	Source
LBLOCA frequency	2.7×10^{-5} /year	Maine Yankee Individual Plant Examination (IPE)
Fraction of LBLOCAs in cold leg	0.5	Assumption
Plant availability	0.7	Not stated (agrees with IPE)
Hot-leg recirculation failure	0.1	Assumption
Nonrecovery probability	1.0	Assumption

Response 1: In the proposed LBLOCA event tree, there are only two sequences leading to core damage that involve a failure of the hot-leg recirculation valves. One sequence involves a failure of the high-pressure safety injection (HPSI) system, which has a relatively low probability. Therefore, it is not surprising that the remaining sequence is responsible for essentially all of the predicted increase in the core damage probability.

Because the Maine Yankee Final Safety Analysis Report (FSAR) and IPE did not provide any estimate of the parameters necessary to calculate the increase in the CDP, reasonable assumptions were required. The licensee was requested to provide pertinent information to allow more realistic probability estimates where assumptions were used. Because of the utilities' decision to shut down the unit permanently and the corresponding reduction in staff, no additional information was provided.

First, lacking any details on volume or length of piping, it was assumed that a leak was equally likely to occur in either the hot leg or the cold leg (i.e., the probability that the LOCA occurs in a cold leg = 0.5). The factors that influence the likelihood of a pipe break not only include length of pipe, but also the greater propensity for a cold-leg break based on the size, shape, and weld zone risks for the cold leg compared to the hot leg.¹ No data were available to support a probability value other than 0.5.

Second, the LER did not include any estimate of the probability that the containment environmental conditions required to pressure lock the loop-fill MOVs would still exist when hot-leg recirculation was initiated. So, a reasonable estimate that all three loop-fill MOVs would simultaneously fail was made based on the assumption that each valve would become pressure locked one-half of the time if the necessary environmental conditions existed when hot-leg recirculation was initiated (i.e., the probability that a valve would become pressure locked is 0.5). Because only one significant figure is available, the probability of hot-leg recirculation failing is 0.1 rather than 0.121. A more detailed description of determining this probability was added to the event analysis.

Finally, it was assumed that personnel entering containment after the loop-fill valves failed would not be feasible. Therefore, no recovery credit was given if the valves did fail (i.e., probability of nonrecovery = 1.0).

Comment 2: The Event Description reasonably reflects the LER event description; however, two points are unclear:

1. The event involved identification of the potential for thermal pressure locking of certain MOVs; the discussion makes it clear that hydraulic pressure locking did not occur; it is not clear that thermal pressure locking did not occur either.

2. Most importantly, the description states that "Boron precipitation . . . could lead to core damage . . ."; although this generally reflects LER supplied information, it may lead to inappropriate success criteria for a realistic risk analysis.

Maine Yankee's design basis accident analysis does require hot-leg recirculation within 19 h of a cold-leg LBLOCA. The potential for this not to be provided due to thermal pressure locking of MOVs was reported via the subject LER. The success criteria involved in such a design basis analysis are well known to be conservative, often very conservative. It is common for probabilistic risk analysis (PRA) to use alternate, more realistic success criteria. For example, as stated in the subject analysis, "Hot-leg recirculation is not addressed in the [Maine Yankee] IPE; however, the LER for this event indicated that the switch-over to hot-leg recirculation is required 19 h after a large cold-leg break."

The subject analysis is based on the LER statement, which reflects design basis. Such conservative design-basis success criteria are inappropriate for use in risk analysis, especially when that analysis is stated to be "as realistic as possible" (September 3, 1997, transmittal letter, D. Dorman to M. Sellman).

While it may be possible to experience some limited, local damage to fuel in the event of boron precipitation following failure of hot-leg recirculation, it may be unrealistic to assume significant "core damage" (in the sense PRAs/IPEs use the term). It would seem reasonable to expect, for example, that precipitated boron might go back into solution in the event of core heatup. If more realistic success criteria were considered, rather than reliance on conservative design-basis criteria, this analysis might find the CDP contribution to be zero.

Response 2: The analysis did not imply that an actual event involving thermal pressure locking of the loop-fill MOVs had occurred. The *Event Summary* indicates that "... coolant trapped between the containment integrity check valve and the loop-fill motor-operated valves (MOVs) could cause [emphasis added] the loop-fill MOVs to become pressure locked following a loss-of-coolant accident (LOCA)." Likewise, the *Event Description* states that "... [piping bounded by] the loop-fill MOVs (RC-M-15, 25, 35) was susceptible to thermal pressure locking following a LOCA (Fig. 1)." Consequently, the probability of failure of the hot-leg recirculation valves due to pressure locking (basic event HPR-MOV-CF-HOT) was set to 0.1.

The Maine Yankee FSAR is considered to be an adequate source document for design-basis limitations. Both the FSAR² and LER No. 309/97-004 (Ref. 3) indicate that hot-leg recirculation is required to protect the core from being damaged within 19 h of an LBLOCA in a cold leg. The licensee was requested to provide information that would support a more realistic assessment of the need for hot-leg recirculation and the impact of failure of hot-leg recirculation on core cooling. Because of the utilities' decision to shut down the unit permanently and the corresponding reduction in staff, no additional information was provided.

Based on the licensee discussion in the event report, there were two possible failure mechanisms for each loop-fill MOV. The event report³ indicated that "... based on engineering judgment it has been determined that [a LOCA induced] pressure increase [in the adjacent piping] could render the loop-fill valves inoperable either by physically damaging the valves or hydrostatically locking the valve disk in place." The event report also indicated that check valve leakage on the opposite end of the affected pipe run could prevent any impact on the loop-fill MOVs (i.e., the probability of the valves becoming pressure locked = 0.0). Lacking more explicit detail, in the preliminary analysis, all three of these possibilities were considered equally likely to occur. If a loop-fill MOV was damaged (probability = 0.33), it was assumed that the valve would not open when required (i.e., the probability of the valves failing to operate = 1.0). If a loop-fill MOV disk was hydrostatically locked in place (probability = 0.33), there was assumed to be some chance of the motor torque overcoming the pressure lock as the hot water that expanded into the disk cavity cooled. According to the FSAR², in the worst case, the containment temperature will peak within 10 s at ~135°C (275°F) [the initial temperature was 41°C (105°F)]. After 19 h the temperature is predicted to be ~82°C (180°F). This is about one-half of the peak temperature. Therefore, it was assumed that the probability of the motor torque being insufficient to overcome the loop-fill MOV disk pressure given that the valves would initially have been hydraulically pressure locked was essentially 0.5. As a result, the common-cause failure probability for the three loop-fill valves was set to

$$[(0.0 \times 0.33) + (1.0 \times 0.33) + (0.5 \times 0.33)]^3 = 0.1$$

for basic event HPR-MOV-CF-HOT in the preliminary analysis of this event.

For this event to fail to make the ASP Program's conditional core damage probability (CCDP) threshold of 1.0×10^{-6} , the probability that the check valve leakage on the opposite end of the affected pipe run could prevent any impact on the loop-fill MOVs would have to be 0.74 (versus the 0.33 used in the preliminary analysis). Assuming the two failure mechanisms are equally likely to occur means that the probability that a loop-fill MOV disk was damaged is 0.13 and that the probability that a loop-fill MOV disk was hydrostatically locked in place is also 0.13. With these assumptions, the common-cause failure probability for the three loop-fill valves would be

$$[(0.0 \times 0.74) + (1.0 \times 0.13) + (0.5 \times 0.13)]^3 = 0.0074.$$

Replacing this value (0.0074) for basic event HPR-MOV-CF-HOT in the preliminary analysis results in a CCDP of 1.0×10^{-6} . There is insufficient information available to support such a finding.

Comment 3: Post-recirculation actuation signal/post-LOCA recirculation cooling, with containment spray pumps feeding charging/HPSI pumps is train dependent. That is Train A spray feeds Train

A HPSI only (similar for B). The event tree analysis included appears to consider a "1 out of 2" success criteria for top event "HPSI" and for top event "COLDLEG". It is unclear whether the train-wise dependence has been modeled. Successful cold-leg recirculation requires the same train of HPSI and spray to be operating (cross train alignment is possible with manual recovery action).

Response 3: The fault tree for the HPSI system and for recirculation does consider the train dependency of the spray pumps and the HPSI pumps.

Comment 4: Success criteria "2" on page 3 of the subject analysis indicates that an LBLOCA can be mitigated with "no HPSI, two LPSI, one accumulator, and successful switch over to cold-leg recirculation." Since cold-leg recirculation requires HPSI, it cannot be accomplished with "no HPSI". Although this dependence is acknowledged later on page 3 under "HPSI", it is unclear how this is actually modeled. It would appear that sequences 7 through 9 of the event tree (Fig. 2, page 7) are impossible; if so, all sequences below 6 could be condensed into a single sequence with HPSI failure leading to "CD".

Response 4: Table D-1b (page D-6) of the Maine Yankee IPE indicates that a LBLOCA can be mitigated without any HPSI pumps running, but the subsequent success of recirculation would be required. This was credited to mean that adequate decay heat could be removed initially following an LBLOCA without the HPSI pumps, but the HPSI system would have to be recovered before recirculation was required. Some operator recovery probability is credited within the HPSI fault tree (i.e., operator fails to recover HPSI was set to the nominal value of 0.84). Therefore, consistent with the Maine Yankee IPE, sequences 7 through 9 of the LBLOCA event tree are possible if the HPSI system is recovered before recirculation is required.

G.5.2 NRC Comments

No comments were provided by NRC.

G.5.3 References:

1. H. M. Thomas, "Pipe and Vessel Failure Probability," *Reliability Engineering*, Vol. 2, 1981, p. 83-124.
  2. Maine Yankee Atomic Power Company, *Final Safety Analysis Report*.
  3. LER 309/97-004, Rev. 0, "RCS Loop-Fill Header MOV Overpressure," February 24, 1997.
-

G.6 LER No. 335/97-011

Event Description: Non-conservative recirculation actuation signal set point

Date of Event: November 2, 1997

Plant: St. Lucie, Unit 1

G.6.1 Licensee Comments

Reference: Letter from J. A. Stall, Vice President, St. Lucie Plant, to U. S. Nuclear Regulatory Commission, "LER 335/97-011 Comments on Preliminary Accident Sequence Precursor Analysis," May 21, 1998.

Comment 1: There may be some unquantifiable conservatism in the assumptions and the human error probability in the Analysis and Evaluation of Operational Data (AEOD) study. This is identified in the sensitivity analysis of the AEOD study and is reasonable.

Response 1: No response is required.

Comment 2: The probability of "Operator fails to initiate recirculation" was estimated to be 1.2×10^{-1} . This is a factor of two times our [Florida Power and Light (FPL)] estimated number of 6.0×10^{-2} , but within the bounds of uncertainty.

Response 2: The probability of "Operator fails to initiate recirculation" was estimated using data provided by FPL from a single simulator test on an operating crew (40 s response). As suggested by the *Human Reliability and Safety Analysis Data Handbook*,¹ some variability (60 s) for post-accident task actions (page 66), must be assessed for postdiagnosis actions (e.g., travel time and manipulation time). Hence, a median response time of 100 s was established for the operator to manually initiate recirculation. This correlates well with the expected time response of 90 s specified by FPL in LER 335/97-011 (Ref. 2). This median time was then input into a time-reliability correlation (TRC) as described in *Human Reliability Analysis*.³ The time available before equipment damage occurs, which would lead to core damage, was assumed to be 230 s. Operator response was favorably assumed to be rule-based and without hesitancy, yielding an error factor of 3.2. This TRC gives a probability of operator failure of 1.2×10^{-1} . A TRC without any time allowed for postdiagnosis actions (i.e., 40 s response

time) is 6.9×10^{-2} . Hence, using a probability of 6.9×10^{-2} does not leave any time for post diagnosis actions. This does not appear to be a realistic assumption. Consequently, the 1.2×10^{-1} value is considered to be appropriate for this analysis.

Comment 3: The probability of "Operator fails to secure spray pumps" was estimated to be 5.2×10^{-1} , assuming that this action is rule-based, but with hesitancy, because conditions to secure the spray pumps are not met immediately. This value appears high when compared to the simulator run and more detailed consideration of the emergency operating procedure (EOP). FPL believes that the value of 1.9×10^{-1} used in the sensitivity study is a more reasonable representation.

Response 3: In lieu of simulator data, the probability of "Operator fails to secure spray pumps" in the ASP analysis was estimated using rough graphical data from the Final Safety Analysis Report for St. Lucie⁴ regarding containment pressure following a large-break loss-of-coolant accident (LOCA). This graph indicated that the time frame for securing the spray pumps would be in close proximity to when operators would need to manually initiate recirculation. Also, the instructions for securing the spray pumps would not have been read immediately prior to the action taking place. Considering this timing for securing spray and the fact that this action is not normally an urgent action, a 5-min delay time suggested by the *Human Reliability and Safety Analysis Data Handbook*¹ for post-accident task actions (page 66), was added to the 1-min response time. This provides a nominal response time of 6 min. However, because operator actions can have a high degree of variability, two sensitivity studies on the operator response time were presented as part of the analysis. The sensitivity studies, summarized below, are intended to scope some of the uncertainty in the estimated conditional core damage probability (CCDP).

Response time	operator failure probability	CCDP
—	$1.0 \times 10^{+0}$	4.9×10^{-5}
6 min	5.2×10^{-1}	3.4×10^{-5}
3 min	1.9×10^{-1}	2.3×10^{-5}

The first sensitivity study assumes that the operators fail to secure the containment spray pumps ($p = 1.0 \times 10^{+0}$). The other sensitivity study assumes that the operators secure the containment spray pump in 3 min ($p = 1.9 \times 10^{-1}$). The 3 min response is simply based on one-half of the assumed nominal response time of 6 min. Because securing the spray pumps is not normally an urgent action, we believe that a 6 min response is more realistic than a 3 min response. Nevertheless, with all of the uncertainties involved in probabilistic

calculations, there is essentially no difference between the resulting conditional core damage probability (CCDPs) calculated for the various cases.

Comment 4: Based on our [FPL] simulator run and the more detailed review of the EOP, we [FPL] believe that the CCDP of 2.3×10^{-5} [presented in one of the sensitivity studies] is a more realistic estimate.

Response 4: The simulator run was considered, but the fact that this represented a single data point was also factored into the analysis process per the response to Comment 2. The difference between the sensitivity study result of 2.3×10^{-5} (3 min to secure the containment spray pumps) and the nominal analysis result of 3.4×10^{-5} (6 min to secure the containment spray pumps) is quite small, especially for a probabilistic assessment. Additionally, LER No. 335/97-011 estimated the CCDP to be 3.0×10^{-5} , which correlates well with the results from the nominal assessment and the sensitivity studies. Certainly all of these estimates are well within any uncertainties surrounding the large-break loss of coolant accident (LBLOCA) frequency, human performance probabilities, and component failure rates. Because the results of the nominal analysis and the sensitivity study provide essentially the same value, no change to the nominal analysis results is warranted.

G.6.2 NRC Comments

No comments were provided by the NRC to date.

G.6.3 References

1. D. I. Gertman and H. S. Blackman, *Human Reliability and Safety Analysis Data Handbook*, John Wiley and Sons, 1994.
2. LER 335/97-011, Rev. 0, "Non-Conservative Recirculation Actuation Signal Set Point Resulted in Operation Prohibited by the Technical Specifications," December 2, 1997.
3. E. M. Dougherty and J. R. Fragola, *Human Reliability Analysis*, John Wiley and Sons, 1988.
4. St. Lucie, *Final Safety Analysis Report (Updated Version)*.

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. 26

2. TITLE AND SUBTITLE

Precursors to Potential Severe Core Damage Accidents: 1997, A Status
Report

3. DATE REPORT PUBLISHED

MONTH	YEAR
November	1998

4. FIN OR GRANT NUMBER
B0435

5. AUTHOR(S)

R. J. Belles, J. W. Cletcher, D. A. Copinger, B. W. Dolan*, J. W. Minarick*,
M. D. Muhlheim

6. TYPE OF REPORT

Technical

7. PERIOD COVERED (Include Dates)

8. PERFORMING ORGANIZATION - NAME AND ADDRESS (If NRC, provide Division, Office or Region, U.S. Nuclear Regulatory Commission, and mailing address; if contractor, provide name and mailing address.)

Oak Ridge National Laboratory
Oak Ridge, TN 37831-8065

*Science Applications International Corporation
Oak Ridge, TN 37830

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)

This report describes the five operational events in 1997 that affected five commercial light-water reactors (LWRs) and that are considered to be precursors to potential severe core damage accidents. 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 first computer-screening the 1997 licensee event reports from commercial LWRs to identify those events that could be precursors. Candidate precursors were 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 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 1969-1996 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 the events.

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

Federal Recycling Program