NUREG/CR-4142
UCID-20330

A Review of the Millstone 3 Probabilistic Safety Study

A. A. Garcia, D. L. Bernreuter, T. E. McKone, P. D. Smith (LLNL), P. J. Amico (Applied Risk Technology Corporation), J. W. Reed, M. W. McCann, Jr. (Jack R. Benjamin & Associates, Inc.), P. R. Davis and G. Apostolakis (Consultants)

Prepared for
U.S. Nuclear Regulatory Commission

Lawrence
Livermore
National
Laboratory

NOTICE

NOTICE

Availability of Reference Materials Cited in NRC Publications

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

1. The NRC Public Document Room, 1717 H Street, N.W.
   Washington, DC 20555

2. The Superintendent of Documents, U.S. Government Printing Office, Post Office Box 37082,
   Washington, DC 20013-7082

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

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

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

The following documents in the NUREG series are available for purchase from the GPO Sales Program: formal NRC staff and contractor reports, NRC-sponsored conference proceedings, and NRC booklets and brochures. Also available are Regulatory Guides, NRC regulations in the *Code of Federal Regulations,* and *Nuclear Regulatory Commission Issuances.*

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

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

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

Single copies of NRC draft reports are available free, to the extent of supply, upon written request to the Division of Technical Information and Document Control, U.S. Nuclear Regulatory Commission, Washington, DC 20555.

Copies of industry codes and standards used in a substantive manner in the NRC regulatory process are maintained at the NRC Library, 7920 Norfolk Avenue, Bethesda, Maryland, and are available there 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 the American National Standards Institute, 1430 Broadway, New York, NY 10018.

NUREG/CR-4142
UCID-20330

A Review of the Millstone 3 Probabilistic Safety Study

Manuscript Completed: December 1985
Date Published: April 1986

Prepared by
A. A. Garcia, D. L. Bernreuter, T. E. McKone, P. D. Smith* (LLNL), P. J. Amico (Applied Risk Technology Corporation), J. W. Reed, M. W. McCann, Jr. (Jack R. Benjamin & Associates, Inc.), P. R. Davis and G. Apostolakis (Consultants)

Lawrence Livermore National Laboratory
7000 East Avenue
Livermore, CA 94550

Prepared for
Division of Safety Technology
Office of Nuclear Reactor Regulation
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555
NRC FIN No. A0447

* EQE, Incorporated, San Francisco, CA

CONTENTS

Page

1. EXECUTIVE SUMMARY 1-1

1.1 Internal Events 1-2
1.2 External Events 1-4

1.2.1 Earthquakes 1-4
1.2.2 Fires 1-4
1.2.3 External Flooding 1-6
1.2.4 Internal Flooding 1-6
1.2.5 Extreme Winds 1-7
1.2.6 Aircraft Accidents 1-7
1.2.7 Hazardous Materials 1-7
1.2.8 Turbine Missiles 1-8

1.3 References for Section 1 1-8

2. INTRODUCTION 2-1

2.1 Background 2-1
2.2 Scope 2-1
2.3 Review Assumptions 2-1
2.4 References for Section 2 2-2

3. INTERNAL EVENTS ANALYSIS 3-1

3.1 Initiating Events 3-1

3.1.1 Completeness of Initiating Events Considered 3-1
3.1.2 Frequency of Initiating Events 3-3
3.1.3 Issues of Importance to the NRC 3-9
3.1.4 References for Section 3.1 3-11

3.2 Event Trees 3-11

3.2.1 General Event Tree Findings 3-12
3.2.2 Specific Event Tree Findings 3-30
3.2.3 Issues of Importance to the NRC 3-34
3.2.4 References for Section 3.2 3-38

3.3 Success Criteria 3-38

3.3.1 Emergency Core Cooling Early 3-38
3.3.2 Emergency Core Cooling Late 3-40
3.3.3 Containment Heat Removal 3-40
3.3.4 Revised Success Criteria 3-40
3.3.5 References for Section 3.3 3-40

Page

3.4 Systems 3-43

3.4.1 Main Electrical System 3-44
3.4.2 120V AC Vital Bus 3-52
3.4.3 Engineered Safety Features Actuation System 3-55
3.4.4 Emergency Generator Load Sequencer (EGLS) System . . . 3-57
3.4.5 Auxiliary Feedwater System 3-60
3.4.6 High Pressure Safety Injection System 3-63
3.4.7 Low Pressure Safety Injection System 3-64
3.4.8 Main Steam Isolation System 3-68
3.4.9 Quench Spray Steam 3-69
3.4.10 Safety Injection Pump Cooling System 3-73
3.4.11 Charging Pump Cooling 3-75
3.4.12 Low Pressure Recirculation System 3-77
3.4.13 High Pressure Recirculation System 3-78
3.4.14 Containment Recirculation Spray System 3-81
3.4.15 Service Water System 3-82
3.4.16 Vital DC System 3-86
3.4.17 General Comments Regarding the Millstone 3 System Fault Trees 3-90
3.4.18 References for Section 3.4 3-90

3.5 Human Factors 3-91

3.5.1 Operator Actions Modeled on the Event Trees 3-91
3.5.2 Operator Actions Modeled on the Fault Trees 3-95
3.5.3 References for Section 3.5 3-96

3.6 Failure Data 3-98

3.6.1 Random Component Failure Rates 3-98
3.6.2 System Failures 3-111
3.6.3 Requantification of Accident Sequences Based on System Failure Rate Revisions 3-119
3.6.4 References for Section 3.6 3-119

3.7 Operating Experience Analysis 3-121

3.7.1 Initiating Events 3-121
3.7.2 Component Failures 3-122
3.7.3 Human Errors 3-123
3.7.4 Concluding Remarks on Operating Data Analysis 3-124
3.7.5 References for Section 3.7 3-124

3.8 Analysis Codes 3-124

3.8.1 Introduction 3-124
3.8.2 WAMBAM 3-125
3.8.3 WAMCUT 3-125
3.8.4 Comments 3-126
3.8.5 References for Section 3.8 3-126

Page

3.9 Accident Sequences 3-126

3.9.1 Comments on MP 3 PSS Assessment of Accident Sequences 3-126
3.9.2 Conclusions 3-134
3.9.3 References for Section 3.9 3-134

3.10 Dependencies 3-134

3.10.1 Common-Cause Initiating Events 3-135
3.10.2 Intersystem Dependency 3-137
3.10.3 Common-Cause Failure Analysis 3-139
3.10.4 References for Section 3.10 3-140

3.11 Quantification 3-140

3.11.1 Development of Quantitative Results in the Millstone 3 PSS 3-141
3.11.2 Quantification of Uncertainties 3-141

3.12 Requantification Summary for the Internal Event Accident Sequences 3-144

4. EXTERNAL EVENT ANALYSIS 4-1

4.1 Seismic Events 4-1

4.2 Fire Events 4-1

4.2.1 Overall Assessment 4-2
4.2.2 Discussion of Findings 4-3
4.2.3 References for Section 4.2 4-6

4.3 External Flooding 4-7

4.3.1 References for Section 4.3 4-8

4.4 Internal Floods 4-8

4.4.1 Overview of the Millstone 3 Internal Flood Analysis . 4-9
4.4.2 State-of-the-Art in Flood Risk Analysis 4-10
4.4.3 Comments on the Internal Flooding Analysis in the Millstone 3 PSS 4-11
4.4.4 Conclusions 4-12
4.4.5 References for Section 4.4 4-13

4.5 Extreme Winds 4-13

4.5.1 References for Section 4.5 4-14

4.6 Aircraft Accidents 4-14

4.6.1 References for Section 4.6 4-16

4.7 Hazardous Materials 4-16

4.7.1 Identification and Screening of Hazardous Materials Initiators 4-16
4.7.2 Comments 4-18
4.7.3 References for Section 4.7 4-18

4.8 Turbine Missiles 4-18

4.8.1 References for Section 4.8 4-20

5. SUMMARY AND CONCLUSIONS 5-1

5.1 Dominant Sequences Corresponding to Each Plant Damage State . . 5-1

5.1.1 Internal Events 5-1
5.1.2 Requantification Results 5-2
5.1.3 External Events 5-9

5.2 Treatment of Uncertainties 5-10

5.2.1 Treatment of Uncertainties for Internal Events 5-11
5.2.2 Treatment of Uncertainties for External Events 5-12
5.2.3 Comment on the Treatment of Uncertainties 5-12
5.2.4 References for Section 5.2 5-13

5.3 Insights 5-13

5.3.1 Internal Event Insights 5-13
5.3.2 External Event Insights 5-20
5.3.3 References for Section 5.3 5-21

Appendix A Review of the Original Millstone Unit 3 Probabilistic Safety Study Seismic Event Ealuation.

Appendix B Review of the Millstone Unit 3 Probabilistic Safety Study Seismic Fragility, Wind, and External Flooding (Jack R. Benjamin & Associates, Inc.)

Appendix C Review of the Revised Millstone Unit 3 Probabilistic Safety Study Seismic Fragility (Jack R. Benjamin & Associates, Inc.)

LIST OF TABLES

Page

1-1 Plant damage state frequencies for internal events (per reactor-year) 1-5

3.1-1 Internal initiating events for Millstone Unit 3 3-2
3.1-2a PCA available transients for Millstone Unit 3 3-4
3.1-2b Loss of PCS transients for Millstone Unit 3 3-5
3.1-3 Internal initiating event frequencies for Millstone Unit 3 . . 3-6
3.2-1 Event tree top event definitions 3-13
3.2-2 Plant damage state descriptions 3-14
3.3-1 Millstone 3 PSS functional success criteria 3-41
3.3-2 Revised Millstone 3 PSS functional success criteria 3-42
3.4-1 Results of the system fault tree analysis 3-44
3.4-2 Support state definitions 3-44
3.4.1-1 Dominant cut sets for failure of the main electrical system . . 3-47
3.4.2-1 Dominant cut sets in the PSS for the unavailability at the 120V vital AC 3-55
3.4.3-1 Dominant cut sets in the PSS for the unavailability of an actuation signal on one train of the ESF actuation system . . . 3-57
3.4.5-1 Summary of unavailability results for the auxiliary feedwater system 3-62
3.4.5-2 Dominant contributors to unavailability for cases A-F in the PSS 3-63
3.4.6-1 High pressure safety injection system unavailability results in the PSS 3-65
3.4.6-2 High pressure safety injection system dominant contributors . . 3-65
3.4.7-1 Dominant contributors to LPSI system unavailability in the PSS 3-67
3.4.9-1 Quench spray unavailability 3-72
3.4.10-1 Dominant cut sets in the PSS for the safety injection pump cooling system 3-74
3.4.11-1 Dominant cut sets in the PSS for the charging pump cooling system 3-76
3.4.12-1 Low pressure recirculation system unavailability results in the PSS 3-78
3.4.13-1 High pressure recirculation system unavailability results in the PSS 3-80
3.4.14-1 Containment recirculation spray system unavailability results in the PSS 3-83
3.4.15-1 System unavailabilities in the PSS for service water system 3-85
3.5-1 Human error probabilities for operator actions in event trees . 3-92
3.5-2 Human error probabilities for fault tree analysis human error rate 3-93
3.6-1 Fluid system components - comparison of component failure rate data 3-100
3.6-2 Electrical/electronic system components - comparison of component failure rate data 3-104
3.6-3 Comparison of MP 3 PSS and NREP/IREP component failure rates. . 3-109

Page

3.6-4 Comparison of MP 3 PSS and Zion PRA component failure rates . . 3-110
3.6-5 MP 3 component failure rates significantly different from both NREP/IREP and Zion PRA values 3-111
3.6-6 Comparison of system failure rates 3-113
3.6-7 Comparison of low pressure safety injection system failure rates 3-117
3.6-8 Requantification of core melt frequency based on revisions to system failure rates 3-120
3.7-1 Dependence of Millstone initiating events on operating experience 3-123
3.10-1 Support state definitions 3-136
3.10-2 Conservatisms claimed in PSS systems analysis 3-138
3.11-1 Internal Plant Damage State Matrix (M) 3-142
3.12-1 Initiating event frequencies 3-146
3.12-2 Support state probabilities 3-147
3.12-3 System failure and human error event probabilities 3-148
3.12-4 Offsite power recovery factors 3-151
3.12-5 System failure and human error probabilities for the ATWS event tree 3-152
3.12-6 Event tree top event definitions 3-153
3.12-7 Support state definitions 3-154
3.12-8 Plant damage state descriptions 3-155

4.2-1 Results of the sensitivity analysis 4-4
4.4-1 Plant systems considered as credible flood sources 4-10

5.1-1 Plant damage state frequencies for internal events 5-3
5.1-2 Dominant sequences by plant damage state 5-4
5.1-2 Legend 5-6
5.2-1 Sources of uncertainty and their treatment in the Millstone 3 PSS 5-12
5.3-1 Matrix of elements from core melt frequency dominant accident sequences 5-16
5.3-2 Contribution of CMF from dominant accident sequence elements . 5-17

LIST OF FIGURES

Page

3.2-1 Large LOCA event tree 3-16
3.2-2 Medium LOCA event tree 3-17
3.2-3 Small LOCA event tree (sheet 1 of 2) 3-18
3.2-3a Small LOCA event tree (sheet 2 of 2) 3-19
3.2-4 Incore instrument tube rupture event tree (sheet 1 of 2) . . . 3-20
3.2-4a Incore instrument tube rupture event tree (sheet 2 of 2) . . . 3-21
3.2-5 Steam generator tube rupture event tree 3-22
3.2-6 Steamline break inside (and outside) containment event tree . . 3-23
3.2-7 Power conversion system available event tree 3-24
3.2-8 Loss of power conversion system event tree 3-25
3.2-9 Loss of offsite power (support state 7) event tree 3-26
3.2-10 Spurious safety injection event tree 3-27
3.2-11 Anticipated transient without scram (ATWS) event tree 3-28
3.4.1-1 Main electrical system 3-48
3.4.1-2 Fault tree used to calculate the probability of loss of offsite power 3-49
3.4.1-3 Reduced fault tree for the loss of emergency power on one of the two emergency buses 3-50
3.4.1-4 Simplified fault tree for the main electrical system 3-51
3.4.2-1 Schematic of the VIAC-1 channel 3-53
3.4.9-1 Quench spray system 3-70
3.4.16-1 Simplified diagram of vital DC bus 125-VDC-1 3-87
3.4.16-2 Fault tree model of loss of vital DC bus 3-89
3.9-1 MP 3 PSS diagram of RHR suction 3-130
3.9-2 MP 3 simplified RHR system from S&W drawing no. 12179-EM-112A-1 (4-14-84) 3-131
3.9-3 Example event tree for V-sequence 3-133
3.12-1 Large LOCA event tree 3-156
3.12-2 Medium LOCA event tree 3-157
3.12-3 Small LOCA event tree (sheet 1 of 2) 3-158
3.12-3a Small LOCA event tree (sheet 2 of 2) 3-159
3.12-4 Incore instrument tube rupture event tree (sheet 1 of 2) . . . 3-160
3.12-4a Incore instrument tube rupture event tree (sheet 2 of 2) . . . 3-161
3.12-5 Steam generator tube rupture event tree 3-162
3.12-6 Steamline break inside (and outside) containment event tree . . 3-163
3.12-7 Power conversion system available event tree 3-164
3.12-8a Loss of power conversion system (support state 1, 2) event tree 3-165
3.12-8b Loss of offsite power (support states 5, 6) event tree 3-166
3.12-8c Loss of a single DC bus event tree 3-167
3.12-8d Loss of vital AC bus 1 or 2 event tree 3-168
3.12-8e Loss of vital AC bus 3 or 4 event tree 3-169
3.12-8f Loss of a single service water train event tree 3-170
3.12-9 Loss of offsite power (support state 7) event tree 3-171
3.12-10 Spurious safety injection event tree 3-172
3.12-11 Anticipated transient without scram (ATWS) event tree 3-173

ACRONYMS

AF	auxiliary feedwater
AFR	auxiliary feedwater recovery
AFW	auxiliary feedwater
AFWS	auxiliary feedwater system
AR BKR	reserve breaker
ASP	auxiliary shutdown panel
ATWS	anticipated transient without scram
BFR	binominal failure rate (model)
CCW	component cooling water
CDA	containment depressurization actuation
CMF	core melt frequency
COCO-class 9	(code used for accident analysis)
COMPBRN	(thermal model computer program)
CORCON-MOD1	(code used for accident analysis)
CPA	containment pressure change
CR	control room
CRS	containment recirculation system
CRSS	containment recirculation spray system
CSR	containment spray recirculation or cable spreading room
CVCS	chemical and volume control system
D&M	Dames and Moore
DG BKR	diesel generator breaker
DPD	discrete probability distribution
DWST	demineralized water storage tank
ECC	emergency core cooling
ECCS	emergency core cooling system
EGLS	emergency generator load sequencer
EPG	emergency procedure guideline
EPRI	Electric Power Research Institute
EPRI NP-XXXX	EPRI technical report
EUS	eastern United States
ESF	engineered safety features

ESP-NOAH	(internal flood risk analysis code package)
FCSD	(design capacity safety factor)
FCSM	(material strength safety factor)
FRE	(safety factor for equipment responses)
FRSS	(spectral shape factor in seismic fragility analysis)
FSAR	final safety analysis report
HEP	human error probability
HPI	high pressure injection
HPRS	high pressure recirculation system
HPSI	high pressure safety injection system
IPPSS	Indian Point Probabilistic Safety Study
IREP	Interim Reliability Evaluation Program
IRR	Instrument rack room
JBA	Jack R. Benjamin and Associates, Inc.
LER	licensee event report
Limerick SARA	Limerick Severe Accident Risk Assessment
LLNL	Lawrence Livermore National Laboratory
LOCA	loss-of-coolant accident
LOSP	loss of offsite power
LOP	loss of power
LPRS	low pressure recirculation system
LPSI	low pressure safety injection (system)
LWR	light water reactor
MGAC	median ground-acceleration capacity
MOBV	motor-operated butterfly valve
MODMESH	(code used for accident analysis)
MOGLV	motor-operated globe valve
MOGV	motor-operated gate valve
MOV	motor-operated valve
MP 3 PSS	Millstone Point Unit 3 Probabilistic Safety Study
MSB	manual start block
MSI	main steam isolation
MTB	manual trip block
MSIV	main steam isolation valve

NRC	Nuclear Regulatory Commission
NREP	National Reliability Evaluation Program
NRR	Nuclear Reactor Regulation (NRC office)
NSST	normal station service transformer
NUREG	NRC technical report
NU	Northeast Utilities Service Company
ORNL	Oak Ridge National Laboratory
PCS	power conversion system
PGA	peak ground acceleration
PGV	peak ground velocity
PMH	probable maximum hurricane
PMP	probable maximum precipitation
PORV(s)	power operated relief valve(s)
PRA(s)	probabilistic risk assessment(s)
PWR	pressurized water reactor
RCP	reactor coolant pump
RECIRC	recirculation
RHR	residual heat removal
RPCCW	reactor plant component cooling water
RPS	reactor protection system
RSS	Reactor Safety Study
RSSMAP	Reactor Safety Study Methodology Applications Program
RSST	reserve station service transformer
RVR	reactor vessel rupture
RWST	refueling water storage tank
SDOF	single degree-of-freedom (model)
SEP	Systematic Evaluation Program (NRC)
SER	safety evaluation report
SGTR	steam generator tube rupture
SI	safety injection
SIS	safety injection system
SMA	Structural Mechanics Associates
SRSS	square root of sum of the squares
SSE	safe shutdown earthquake
SSMRP	Seismic Safety Margins Research Program

SSS	safeguard sequencer start
SWS	service water system
THERP	Technique for Human Error Rate Prediction
TPCCW	turbine plant component cooling water
USGS	U.S. Geological Survey
USNRC	United States Nuclear Regulatory Commission
WALLDI	(SMA proprietary seismic fragility analysis program)
WAM	(series of codes for fault tree quantification)
WAMBAM	(fault tree quantification code)
WAMCUT	(fault tree quantification code)
WCAP	Westinghouse technical report
WNTD	Westinghouse Nuclear Technology Division
WUS	western United States
ZPSS	Zion Probabilistic Safety Study

ABSTRACT

Lawrence Livermore National Laboratory (LLNL) has conducted a review of the Millstone Unit 3 (MP 3) Probabilistic Safety Study (PSS) for the Office of Nuclear Reactor Regulation, U.S. Nuclear Regulatory Commission (NRC). This probabilistic safety study was performed by Northeast Utilities (NU) in response to a 1981 request from the NRC. The objective of LLNL's review was to review those aspects of the MP 3 PSS leading to estimates of the plant core damage frequency. LLNL estimated core damage frequency from internal events at MP 3 to be about $1x10^{-4}$ per year. LLNL reviewed major areas of the PSS, including initiating events, event trees, success criteria, fault trees, human factors, component and operating experience data, and treatment of uncertainty. The review of external events included earthquakes, fires, external and internal flooding, extreme winds, aircraft accidents, hazardous materials, and turbine missiles. The MP 3 PSS treated external events, other than seismic and fire, in a cursory manner. LLNL's seismic review effort was curtailed by the staff because of ongoing seismic analysis revisions by NU.

1. EXECUTIVE SUMMARY

Lawrence Livermore National Laboratory (LLNL) has conducted a review of the Millstone Point Unit 3 (MP 3) Probabilistic Safety Study (PSS) (Ref. 1-1) for the Office of Nuclear Reactor Regulation (NRR), U.S. Nuclear Regulatory Commission (NRC). This probabilistic risk assessment (PRA) was performed by Northeast Utilities (NU) in response to a 1981 request from the NRC. The PSS was submitted to the NRC in August 1983. A project team composed of people from LLNL staff, subcontractors, and consultants began the review in September 1983 and completed a review draft in May 1984.

The project's objective was to review those aspects of the MP 3 PSS leading to estimates of the plant damage state frequencies and associated uncertainties to determine the accuracy of those estimates. The PSS results (Amendment 2) for core melt probabilities were 4.5E-5/RY for internal events and 2.2E-5/RY for external events. External events were dominated by contributions of 1.7E-5/RY from seismic events and 4.8E-6/RY for fires. The review included a simplified re-evaluation and quantification of the internal event analysis and estimates of the potential effects of changes to some external event analyses. The scope of the project included neither a review of offsite consequences nor extensive requantification.

The review process included several meetings with the plant owner and his subcontractors and consultants and two site visits. Formal communications between LLNL/NRC and the plant owner included detailed questions and answers.

Our review covered all major areas of plant analysis and evaluation in the PSS. These included initiating events, event trees, success criteria (for functions and systems), fault trees, human factors, component and operating experience data, and the treatment of uncertainty. The review of external events included earthquakes, fires, external and internal flooding, extreme winds, aircraft accidents, hazardous materials, and turbine missiles.

The review effort expended varied significantly in these areas, both because of the extent and detail of the analysis presented in the PSS, and because of the relative importances of specific areas. More effort was expended on those areas that were, or had the potential of being, significant contributors to core melt or public risk.

The scope of the review covered an examination of several issues of particular concern to the NRC. These included: (1) reactor coolant pump seal failure during station blackout, (2) depletion of station batteries during station blackout, (3) pressurized thermal shock, (4) steam generator tube rupture with stuck-open secondary steam relief valves, (5) anticipated transients without scram, and (6) stuck-open safety/relief valve. Some of these issues had an effect on system and/or sequence models and on requantification; others, such as pressurized thermal shock, could not be completely evaluated. In this example, an assessment of core melt frequency given the occurrence of pressurized thermal shock is well beyond the scope of the review, and very likely, beyond the present state-of-the-art.

We found no significant omissions which we could quantify in terms of an overall contribution to core melt frequency. Several significant omissions were found in terms of modeling errors that indicate an incomplete or different understanding of interactions between plant systems or between human beings (operators) and plant systems; these are described in the internal events section.

A particularly difficult problem arose with respect to the seismic evaluation of the plant. About the time the MP 3 PSS was submitted to the NRC, NU acknowledged that the evaluations of seismic hazard and seismic fragilities contained in the PSS were incorrect. They believed that both were excessively conservative and that the relatively large core melt frequency due to seismic events (which dominated the total core melt frequency) was due to these conservatisms. Northeast Utilities, in fact, commissioned new analyses of both areas to remove what they believed to be excessive conservatisms. LLNL recognized early in the review that the seismic hazard evaluation in the PSS was not conservative, but rather was optimistic, by perhaps an order of magnitude in the range of interest. In other words, our estimate of earthquake frequency was significantly larger than the PSS estimate and NU expected their new estimate to be smaller than the PSS estimate - so that a significant difference would exist in the ultimate results. This issue was not resolved by our review because we did not perform a complete review of the revised seismic evaluation submitted by NU to the NRC in PSS Amendment 2 after the project began.

The principal qualitative and quantitative conclusions of this review are briefly described below in general terms.

1.1 Internal Events

The extent and type of internal event initiators and their treatment is reasonable and consistent with those considered in other PRAs.

Except for the V-sequence, the systems analysis appears to be adequate and reasonably consistent with the state of the art. The support state methodology, however is judged to be inadequate with respect to the identification of inter-system dependencies. Use of the large event tree-small fault tree methodology where support states are defined for various conditions of initiating event occurrence and system or train availability, made the review and requantification more difficult. In fact, the use of support states appears to place undue emphasis on the analyst's ability to recognize all the dependencies not included in the (small) fault trees. This process does not provide assurance that subtle dependencies normally treated in the "small event tree-large fault tree" methodology are identified and adequately treated. In addition, with the exception of glaring errors, the use of support states in the PRA makes it virtually impossible to verify that inter-system dependencies received adequate treatment. This is largely due to difficulty in identifying all the places a given component or fault tree enters into the larger model, i.e., where all the interfaces are.

The event tree and systems models were, with some exceptions, found to be reasonable and appropriate. Major human errors of omission were included as events on the event trees in a consistent and correct manner; however, operator errors of commission due to incorrect interpretation of plant conditions (cognitive errors) were not treated, and we added two actions of this type to the event trees.

We found success criteria for the various emergency functions to be reasonable. Several minor changes were made, with the most significant being rejection of an optimistic PSS assumption that any one out of four HPSI pumps is capable of providing high pressure injection during small loss-of-coolant accident (LOCA) events. This success definition was revised into two separate success cases: the first allows success for one out of two charging pumps alone, but the second requires one out of two PORVs in combination with one out of two safety injection pumps.

The 16 system fault tree analyses in the PSS were found to be reasonable and acceptable, with a few exceptions. A significant modeling error was identified in which the dependence on the vital DC system by the vital ac system, the main electrical system, and the emergency generator load sequencer was not included on the corresponding fault trees. We were unable to estimate the quantitative effect of this error due to its pervasiveness and the nature of the event tree-fault tree/support system model, which makes requantification almost impossible.

Our review of the failure rate data used in the PSS consisted of a comparison of individual component failure rates with other sources, a review of system failure rates and unavailabilities, and a review of the common-cause failure assessment. Although we found notable differences with other sources, none of the component data differences (except possibly diesel generators) were judged to have significant impact on the core melt results. A simplified sensitivity evaluation for an increase by a factor of 5 in the failure rate of the emergency power system (based on the changed diesel generator rate) indicates that core melt frequency would increase by a factor of 3 over the PSS value for the first year or two of operation and would be only slightly larger than the PSS value thereafter. These results do not consider changes made to the models in other parts of the review.

The reviews of operational experience and analysis codes used in the PSS found both to be reasonable and acceptable.

A review of the severe accident sequence assessment, which included consideration of assumptions, analysis, and predicted phenomena, indicates that (1) the V-sequence evaluation in the PSS contains deficiencies which result in a conservative probability of core melt and public risk, and (2) many conservative assumptions were made in the PSS, but none have a significant influence on the results with the possible exception of the V-sequence, which we did not completely re-evaluate. This sequence was found to be a major risk contributor in the PSS where its evaluation was excessively conservative.

Consideration and treatment of dependencies in the PSS were evaluated in the review's three categories: common-cause initiating events, intersystem dependencies, and intercomponent dependencies. Numerous conservatisms identified in the area of common-cause initiating events appear to be largely insignificant. The review of intersystem dependencies identified the failure to treat loss of DC power in the support state analysis as a potentially significant deficiency if the auxiliary feedwater system requires DC power (which NU states is not necessary for successful AFW system operation). No errors were found in the intercomponent dependencies modeled in the PSS.

The overall quantification process used in the PSS is a natural product of the choice of methodology, i.e., the large event tree-small fault tree approach. No errors were found in the quantification process; however, we were unable to review the specific procedures of the discrete probability distribution (DPD) arithmetic used to propagate uncertainties since that information was not provided in the PSS.

A simplified requantification of the internal event sequences incorporated all structural changes to the event trees and revised data for both components and human errors. Our estimates of the effect of these changes on the core melt probability is compared to the original PSS mean values in Table 1-1.

1.2 External Events

External event types considered in the PSS are earthquakes, fires, external and internal flooding, extreme winds, aircraft accidents, hazardous materials, and turbine missiles. This range of event types was judged to be reasonable and consistent with other PRAs and with suggestions made in the PRA Procedures Guide (Ref. 1-2). It should be noted that external events other than seismic and fire were treated only in a cursory manner. Serious problems were identified in the application and execution of the methodologies and with input data.

The approach to the evaluation of external events in the PSS took the form of a screening evaluation to identify potentially significant events for more detailed assessments. Only earthquakes and fires survived the screening and were subjected to detailed assessments. More detail is provided below for the various event types.

1.2.1 Earthquakes

LLNL reviewed the entire seismic event evaluation in the original PSS and found (a) the seismic hazard evaluation to be optimistic and not consistent with the state of the art, and (b) the fragility analyis to be conservative and to contain errors. After the review of this material was completed, NU submitted a substantially revised seismic evaluation as PSS Amendment 2 (Ref. 1-3) in which extensively modified hazard and fragility curves were utilized. At NRC request, LLNL reviewed the revised fragility analysis, which was found to be consistent with the state of the art. The revised seismic hazard evaluation was not reviewed by LLNL.

1.2.2 Fires

The screening process used to identify critical areas was reasonable and complete; however, the methodology used in the remainder of the fire evaluation contains several notable errors. All fire areas deserving detailed analyses were identified. The fire frequencies in various compartments were estimated using acceptable methods and are reasonable.

Analysis of loss-of-safety functions due to fires in critical areas is not rigorous, not explicit, and not performed consistently with the state of the art; however, the effect of these deficiencies appears to be a conservative bias of about one order of magnitude for the conditional fraction of fires that result in loss-of-safety functions.

Table 1-1 Plant damage state frequencies for internal events (per reactor-year).

Name	Description	Pss mean	Review estimate[a]
AEC	Large LOCA, early melt	1.92E-06	8E-7
AEC'	Large LOCA, early melt, failure of recirc. spray	4.17E-09	--
AE	Large LOCA, early melt, no containment cooling	2.68E-09	--
ALC	Large LOCA, late melt	5.44E-06	2E-6
ALC'	Large LOCA, late melt, failure of recirc. spray	4.88E-07	1E-7
ALC"	Large LOCA, late melt, failure of quench spray	3.42E-09	--
AL	Large LOCA, late melt, no containment cooling	3.36E-10	--
SEC	Small LOCA, early melt	1.12E-06	2E-5
SEC'	Small LOCA, early melt, failure of recirc. spray	2.76E-09	--
SE	Small LOCA, early melt, no containment cooling	1.17E-07	6E-6
S'EC	Incore instrument tube LOCA, early melt	--	4E-7
S'E	Incore instrument tube LOCA, early melt no containment cooling	1.83E-09	--
SLC	Small LOCA, late melt	9.81E-06	3E-5
SLC'	Small LOCA, late melt, failure of recirc. spray	4.79E-07	1E-6
SLC"	Small LOCA, late melt, failure of quench spray	5.77E-08	--
SL	Small LOCA, late melt, no containment cooling	2.73E-09	--
S'L	Incore instrument tube LOCA, late melt	3.35E-10	1E-7
TEC	Transient, early melt	1.81E-05	3E-5
TEC'	Transient, early melt, failure of recirc. spray	3.46E-07	8E-7
TE	Transient, early melt, no containment cooling	5.31E-06	2E-6
TLC	Transient, late melt	--	2E-6
V2EC	Steam generator tube rupture, steam leak, early melt	1.11E-07	2E-6
V2EC'	SGTR, steam leak, early melt, failure of recirc. spray	1.03E-09	1E-7
V2E	SGTR, steam leak, early melt, no containment cooling	1.29E-08	--
V2LC	SGTR, steam leak, late melt	2.76E-09	
V2LC'	SGTR, steam leak, late melt, failure of recirc. spray	1.49E-10	--
V2LC"	SGTR, steam leak, late melt, failure of quench spray	1.77E-11	--
V2L	SGTR, steam leak, late melt, no containment cooling	8.40E-13	--
V	Interfacing systems LOCA	1.90E-06	8E-7
	Total[b]	4.53E-05	1E-4

[a] The preliminary review estimates provided are based on a number of simplifying assumptions and subject to a number of limitations discussed in Section 5.1.1. The reader is cautioned to keep these assumptions and limitations in mind when considering the various potential implications of these results.

[b] It is important to note that the plant damage state frequency increase does not necessarily immediately imply a corresponding increase in overall public risk.

The event tree analysis is reasonable, with one exception: the error rate for failure to switch control from the control room to the auxiliary shutdown panel (0.001 per demand) is judged to be too low by about a factor of 200. A rate of 0.23 per demand is suggested for this error.

The net effect of the two numerical changes discussed above is estimated to be an increase of a factor of 6 in the core melt frequency, from 4.8E-6 to 2.8E-5 per reactor-year.

Several issues of potential significance were not addressed in the PSS: (1) the impact of earthquakes on fires and fire protection systems; (2) the effects of the fire suppression agents on equipment; and (3) the response of equipment and cables to high heat fluxes and temperatures. The evaluation of the first two issues has not previously been addressed in any PRA.

1.2.3 External Flooding

A qualitative screening analysis in the PSS concluded that this event was an insignificant contributor to core melt frequency. No formal probabilistic analysis was performed and no point estimate values were provided to support or justify the conclusion. Although some of the judgments in the PSS are believed to be conservative, the absence of an uncertainty analysis is considered to be a serious omission. The large uncertainties which exist for water level exceeding the protected (water tight) elevation of 25.5 feet above mean sea level indicate that there is a possibility of a mean frequency of core melt larger than 1E-6 per reactor-year.

In the absence of an uncertainty analysis, the conclusion that this event's contribution is insignificant relative to other hazards is judged to be inadequately justified and unacceptable.

1.2.4 Internal Flooding

By performing a qualitative screening analysis, the PSS concluded that core melt induced by this event has an estimated frequency of 8.5E-7 per reactor-year, and that it does not significantly contribute to core melt frequency. The analysis includes several important conservative assumptions, including for example, that all components in a flood zone are disabled if a flood occurs in that zone. Individual zones were assumed to have a flood frequency of 2E-3 per reactor-year, based on an unexplained derivation from WASH-1400 (Ref.1-4) for breaks in pipes with a diameter greater than 6 inches. No estimate was made of the actual flood sources present in each zone.

Inadvertent actuation of fire protection equipment was not considered, and reactor trip was assumed to follow any flood-induced initiating event. Both assumptions are optimistic, but may not be significant.

The PSS conclusion that the contribution from this event is insignificant as a contributor to core melt, without detailed assessments of flooding in the cable spreading and switchgear rooms and in the absence of an uncertainty analysis, is judged to be inadequately justified and unacceptable.

1.2.5 Extreme Winds

A qualitative screening analysis in the PSS concluded that the effects are not significant contributors to core melt frequency. The basis for this finding is that the governing wind event is the occurrence of severe tornadoes, and all safety-related structures have been designed to resist tornado loads and resultant missiles for wind speeds up to 360 mph. The minimum thickness of reinforced concrete in the walls and roofs of these structures is 2 feet.

The site hazard for tornado winds exceeding 360 mph is given as 5.4E-6 per year. We believe this figure to be conservative and that justification exists (not provided in the PSS) to show that this probability is less than 1E-8 per year. This frequency of structural failure or missile-induced damage, given a 360 mph tornado, would be smaller that 0.1.

We agree that wind hazard is not a significant external event even though no fragility curves were developed, no systems analysis was performed, and no uncertainty analysis was included.

1.2.6 Aircraft Accidents

A quantitative assessment of the frequency of onsite aircraft crashes was performed in the PSS in accordance with the NRC Standard Review Plan (Ref. 1-5). The total frequency estimates for onsite accidents of 1.6E-6 per year is dominated by a contribution of 1.2E-6 per year from general aviation (light aircraft), whose damage potential is limited to the switchyard. The FSAR (Ref. 1-6) states that no increase in air traffic is projected in the vicinity of the site, but the PSS does not address this topic.

We judge the effective plant area and structures considered susceptible to damage by the various classes of aircraft to be reasonable and conservative. We also judge the analysis of crash frequencies to be conservative choices for the numbers and types of flights considered.

The conclusion that aircraft crashes are not significant contributors to core melt accidents, based on their low frequencies and the low likelihood of such an accident resulting in core melt, is judged to be reasonable and acceptable.

1.2.7 Hazardous Materials

The PSS performed a qualitiative assessment of the potential for offsite and onsite incidents involving the transportation and storage of hazardous materials and concluded that they were insignificant contributors to core melt.

The analysis considered road, rail and water transport routes, and offsite and onsite storage facilities and pipelines.

Numerical estimates of potential risk were made only for rail shipments of propane (a small contributor). All other potential sources were dismissed.

The conclusion that all of these accident types are relatively insignificant contributors to core melt is judged to be correct, but inadequately justified, particularly for accidents involving onsite storage of chlorine in railroad tank cars.

1.2.8 Turbine Missiles

A qualitative assessment in the PSS concluded that turbine missiles are not significant contributors to core melt frequency on the basis of their low frequencies.

In an analysis supplied by General Electric (Ref. 1-7), it is found that the use of a frequency of 1.4E-8 per year of missile generating turbine failures results in a frequency of significant damage to critical structures or components of 2.5E-10 per year. This low frequency does not account for recent NRC concerns with stress corrosion cracking.

Acknowledging this concern, a second calculation was performed in the PSS using 1E-4 per year for missile-generating turbine failures, as recommended in NRC Regulatory Guide 1.115 (Ref. 1-8). The result is a frequency of 1.8E-6 per year for significant damage to critical structures or components, which the PSS judges to be acceptable due to conservatism in the overall analysis. We agree that this conclusion is reasonable.

1.3 References for Section 1

1-1 Northeast Utilities, "Millstone Unit 3 Probabilistic Safety Study," August 1983.

1-2 U.S. Nuclear Regulatory Commission, "PRA Procedures Guide - A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants," USNRC Report NUREG/CR-2300, January 1983.

1-3 Northeast Utilities, "Millstone Unit 3 Probabilistic Safety Study, Amendment No.2," April 2, 1984.

1-4 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.

1-5 U.S. Nuclear Regulatory Commission, "Standard Review Plan," USNRC Report NUREG-0800, July 1981.

1-6 Northeast Utilities, "Final Safety Analysis Report, Millstone Unit 3," 1982.

1-7 General Electric Company, Hypothetical Turbine Missiles - Probability of Occurence, Memo Report, March 1983, Cited in G.C.K. Yey, "Probability and Containment of Turbine Missiles," Nuclear Engineering and Design, Vol. 37, 1976.

1-8 U.S. Nuclear Regulatory Commission, Regulatory Guide 1.115, "Protection Against Low Trajectory Turbine Missiles," Rev. 1, July 1977.

2. INTRODUCTION

LLNL has conducted a review of the Millstone Unit 3 (MP 3) Probabilistic Safety Study (PSS) (Ref. 2-1) for the Office of Nuclear Reactor Regulation (NRR) of the Nuclear Regulatory Commission (NRC). This project is one of several in a larger NRR probabilistic risk assessment (PRA) review program in which PRAs performed and submitted to the NRC by selected light water reactor (LWR) plants in response to regulator requests and/or requirements receive comprehensive review and evaluation.

2.1 Background

The roots of the PRA review program lie in the interest expressed in April 1980 by the NRC Commissioners in determining if there were any candidates for special risk studies at plant sites which may be risk outliers. The staff performed limited generic risk analyses for plant sites within the U.S., based on (1) weighted population density with a 30-mile boundary about the site, (2) plant power level, and (3) stage of construction. Three plant sites (Zion, Indian Point, Limerick) were found to have a weighted density factor 10 to 15 times higher than the median (SECY-81-25) (Ref. 2-2). These plants were required to perform a PRA. Eight plants were found to have a slightly lower weighted density factor (four to eight times the median), but only Millstone 3 and Bailey were in early construction stages where design modifications that might be suggested by PRA analysis would be most productive. On September 21, 1981 [letter from H. Denton (NRC) to W. G. Counsil (NU), "Risk Evaluation - Millstone Unit No. 3"] the staff requested Northeast Utilities to perform a PRA for Millstone 3. Northeast Utilities performed the analysis and submitted a completed PSS to the NRC IN August 1983.

2.2 Scope

The objective of this project was to perform a review of those Millstone 3 PSS aspects leading to teh estimates of frequencies of each plant damage state and the associated uncertainty spread to determine the accuracy of these estimates. Our review covered methodology, assumptions, data, information sources, models, plant understanding, completeness of the analysis, and other areas where inconsistencies could affect the quantitative or qualitative results.

The scope of the analysis did not include extensive re-evaluation or requantification of plant damage state frequencies, nor did it include a review of the consequence analysis included in the MP 3 PSS.

2.3 Review Assumptions

The review philosophy on this subject was simple, straightforward, and applied throughtout the review. Our approach was to examine the models and data in the MP 3 PSS with respect to appropriate selection, application, and proper execution; and to determine whether or not any validation was required. We assumed that the use of standard computer codes, data sources, system modeling techniques, human factors information, etc., was acceptable and did not require validation,except for specific application(s) in the analysis. We similarly assumed that the execution of a particular application was acceptable if it generally conformed with previous work in the PRA arena that had received peer review. Conversely, if the choice of model(s) or data, or the application to a particular problem, or the manner od execution was new and/or different than previously observed, and was not obviously correct, we did not accept the new data or approach unless appropriate justification was provided or the justification was known to, and could be provided by us.

We did not assume, a priori, that the application of a conservative, or very conservative approach necessarily provided an acceptable result. Although it is often assumed that this is not only a correct approach, but one where the analysis is consciously accepting a self-imposed penalty, we do not accept this argument. In many, if not most cases, we would agree that the conservative selection of general approach, model, or data, leads to acceptably conservative results. However, the object of a PRA is to identify the dominant contributors to core melt or to some other risk index, and the selection of excessively conservative models or data may produce results, especially qualitative results, that are essentially incorrect. This can occur beause components, systems, or even accident sequences are effectively promoted in relative imporatnce, so that they may mask important results. If realistic models are used, the problem does not occur, and both the qualitative and quantitative results would be easier to evaluate in terms of NRC concerns with public safety and the utility's use of the results for both public safety and plant reliability considerations.

This is not to say that we take issue with the concept of screening evaluations or the use of conservative models or data to simplify and make tractable what is already a very complex analysis. The choice of conservative assumptions in the analysis, with respect to models and data in a PRA, must be made with care so the results are not distorted in such a manner that important insights are lost due to incorrect identification of dominant contributors.

2.4 References for Section 2

2-1 Northeast Utilities, "Millstone Unit 3 Probabilistic Safety Study, Amendment No. 2," April 2, 1984.

2-2 SECY-81-25, W. J. Dircks to the Commissioners, "Performance of Probabilistic Risk Assessment or Other Types of Special Analyses at High Population Density Sites," January 12, 1981.

3. INTERNAL EVENTS ANALYSIS

The evaluation of internal events in the MP 3 PSS uses the large event tree-small fault tree methodology, where support states are defined for various conditions of initiating event occurrence and system or train availability. The internal initiating event evaluation is reported in PSS Section 1.1 and supported by PSS Appendices 1-A, and 1-D through 1-F. The plant and systems analyses are described in PSS Section 2, which constitutes a large fraction of the PSS, and supported by Appendices 2-A through 2-G and 2-L.

In very general terms, the internal event analysis is reasonable and consistent with the state of the art. Many minor deficiencies, both conservative and optimistic, and a few significant errors were identified.

Our review covers the entire internal event analysis in the PSS and is described in the sections which follow. These address, respectively, the topics listed below in the noted sections: initiating events (§3.1), event trees (§3.2), success criteria (§3.3), systems analysis (§3.4), human factors (§3.5), failure data (§3.6), operating experience (§3.7), analysis codes (§3.8), severe accident sequence progression (§3.9), dependencies (§3.10), and the approach to quantification (§3.11). We also performed a simplified requantification of internal events (§3.12) as part of the review. The requantification incorporated most of the various changes made to the event tree models and to the component and human error data.

3.1 Initiating Events

The MP 3 PSS evaluated more than 60 individual initiators in the process of defining a set of 21 classes of initiating events for the study. This section presents the results of a review of the completeness of the set of initiators considered and of the frequency estimates assigned to each.

3.1.1 Completeness of Initiating Events Considered

The PSS considered two general classes of initiating events, LOCAs and transients, in keeping with the traditional classifications established in previous PRAs. The LOCA classes were defined by examining those in WASH-1400 (the reactor safety study) (Ref. 3.1-1) and from an evaluation of the Millstone plant design to determine if any special LOCA evaluations were required. The transients were developed primarily from the pressurized water reactor (PWR) transient list contained in EPRI NP-2230, ATWS: A Reappraisal, Part 3: Frequency of Anticipated Transients (Ref. 3.1-2). This list was augmented by the development of plant-specific initiators selected because of their unique effects on plant response following the occurrence of the initiator. The list of initiators considered is consistent with those from previous PRAs, and the methodology used is consistent with those espoused in NUREG/CR-2728 (IREP Procedures Guide) (Ref. 3.1-3) and NUREG/CR-2815 (draft NREP Procedures Guide) (Ref. 3.1-4). No significant internal initiators were identified as having been omitted from the evaluation.

Table 3.1-1 lists the 21 initiator classes which were used in the PSS. These classes were developed to represent differences in plant response to each

Table 3.1-1 Internal initiating events for Millstone Unit 3.

Event class	Event name
1	Large LOCA
2	Medium LOCA
3	Small LOCA
4	Steam generator tube rupture
5	Steamline break inside containment
6	Steamline break outside containment
7	Loss of RCS flow
8	Loss of main feedwater flow
9	Primary-to-secondary power mismatch
10	Turbine trip
11	Reactor trip
12	Core power excursion
13	Spurious safety injection
14	Loss of offsite power
15	Incore instrument tube rupture
16	Special large LOCA initiators a. Interfacing systems LOCA b. Catastrophic reactor vessel rupture
17	Loss of a single service water train
18	Loss of a single vital DC bus
19	Total loss of vital DC power
20	Loss of vital AC bus 120-VAC-1 or 120-VAC-2
21	Loss of vital AC bus 120-VAC-3 or 120-VAC-4

initiator class. Most of the classes are reasonable and consistent with previous PRAs except for the division of the majority of the anticipated transients into six event classes (numbered 7 through 12 in the table). Although these groupings represent differences in the initial phenomenology of transients, they do not represent differences in the plant response or in their effects on mitigating systems. Further, these groupings do not account for the possibility of the power conversion system (PCS) being available (see Section 3.2.1.3). For these reasons, the events in these classes were regrouped for this review into two classes, one for loss of PCS and one for PCS available. These new classes are shown in Tables 3.1-2a and 3.1-2b, and it is noted that some transients appear on both lists. These transients, while not failing PCS, result in significant asymmetric perturbations of plant systems which are more likely to fail the PCS than other transients. The probability assignments for these transients were made on the basis that in 50% of these transients, the PCS would definitely fail and in the other 50% it would be available.

3.1.2 Frequency of Initiating Events

A list of the final initiating event classes used in the PSS and their mean and median frequencies are shown in Table 3.1-3. These values are compared with point (or best) estimate values from either NUREG/CR-2787 (Ref. 3.1-5) (ANO-1 IREP study) or from other sources recommended in the NREP Procedures Guide and presently available. The ANO-1 IREP study was used since it is the most recently completed and approved NRC-sponsored PRA for a pressurized water reactor (PWR). The point estimate values are used in the re-evaluation of the dominant core melt sequences for each plant damage state. The source of the point estimate values is also shown in the table. The remainder of this section discusses the methods used by the PSS to establish some of the values used in the study, and to explain the source of some of the point estimate values used in the requantification where the source of the values is not obvious and straightforward.

3.1.2.1 Quantification Methods

The PSS used very sophisticated calculational methods to develop frequencies for some of the initiating events. For the events involving pipe breaks, they took the 5th and 95th percentile frequencies from WASH-1400 and used them as the 20th and 80th percentiles of prior distributions for a Bayesian estimation of pipe failure rate distributions. Bayesian techniques were also utilized in the PSS for loss of offsite power, using the history of LOSP over the entire U.S. as the prior and the Millstone site specific data as the posterior. In the quantification of interfacing systems LOCA, the utilization of the log uniform distribution and discrete probability distribution (DPD) technique results in an unrealistically skewed distribution, with the mean value being more than two orders of magnitude higher than the median, and even slightly higher than the 90% confidence bound. This example demonstrates that the use of Bayesian techniques to incorporate "plant specificity" may not be meaningful in data bases this small. The deviations which are credited to plant-specific differences could also be caused by random distributions of occurrences within the general population.

3.1.2.2 Steam Generator Tube Rupture

The point estimate for steam generator tube rupture (SGTR) was developed from actual operating data for Westinghouse reactors in the U.S. A review of available data on steam generator tube leaks found four SGTR events through early 1982 (Ref. 3.1-6). This represented a total of 240 reactor-years of operating experience. The point estimate value is essentially identical to the median value used in the PSS.

Table 3.1-2a PCS available transients for Millstone Unit 3.

EPRI NP-2230 event no.	Transient name	Frequency (per year)
1	Loss of RCS flow	0.39
2	Uncontrolled rod withdrawal	0.02
3	CRDM problems and/or rod drop	0.65
4	Leakage from control rods	0.02
5	Leakage in primary system	0.08
6	Low pressurizer pressure	0.03
7	Pressurizer leakage	0.01
8	High pressurizer pressure	0.03
11	CVCS malfunction - boron dilution	0.04
12	Pressure/temperature/power imbalance	0.16
13	Startup of inactive coolant pump	0.00
14	Total loss of RCS flow	0.03
15	Loss or reduction in feedwater flow (1 loop) (50%)	0.94
17	Full or partial closure of MSIV (1 loop) (50%)	0.12
19	Increase in feedwater flow (1 loop) (50%)	0.35
23	Loss of condensate pump (1 loop) (50%)	0.04
26	Steam generator leakage	0.04
27	Condenser leakage	0.05
28	Miscellaneous leakage in secondary systems	0.08
33	Turbine trip, throttle valve closure, EHC problems	1.38
34	Generator trip or generator caused faults	0.38
36	Pressurizer spray failure	0.04
37	Loss of power to necessary plant systems (50%)	0.05
38	Spurious trips - cause unknown	0.14
39	Automatic trip - no transient condition	1.55
40	Manual trip - no transient condition	0.62
	Total - PCS available transients	7.24

Table 3.1-2b Loss of PCS transients For Millstone Unit 3.

EPRI NP-2230 event no.	Transient name	Frequency (per year)
10	Containment pressure problems	0.01
15	Loss or reduction in feedwater flow (1 loop) (50%)	0.94
16	Total loss of feedwater flow (all loops)	0.15
17	Full or partial closure of MSIV (1 loop) (50%)	0.12
18	Closure of all MSIV	0.03
19	Increase in feedwater flow (1 loop) (50%)	0.35
20	Increase in feedwater flow (all loops)	0.01
21	Feedwater flow instability - operator error	0.15
22	Feedwater flow instability - misc. mechanical causes	0.21
23	Loss of condensate pump (1 loop) (50%)	0.04
24	Loss of condensate pumps (all loops)	0.00
25	Loss of condenser vacuum	0.20
30	Loss of circulating water	0.06
31	Loss of component cooling	0.00
37	Loss of power to necessary plant systems (50%)	0.05
	Total - Loss of PCS transients	2.32

3.1.2.3 Steamline Breaks

The PSS apparently made an error in its selection of data for the steamline break events. The PSS states that one of the causes of steamline break inside containment is "...steam generator relief valve failures..." This is a reasonable statement, since "inside containment" here refers to cases where the break path originates upstream of the main steam isolation valves, regardless of where the break ultimately discharges the steam. The concern is whether or not MSIV closure will terminate break flow rather than where the steam actually goes. However, in the quantification of steamline break events, event 29 from EPRI NP-2230 (sudden opening of steam relief valves) was added to the steamline break outside containment category. This event logically belongs in the inside containment category, and it is the dominant

Table 3.1-3 Internal initiating event frequencies for Millstone Unit 3 (frequencies in events/reactor-year).

		Event frequencies			Point
Event class	Event name	PSS mean	PSS median	Point estimate	estimate source
1	Large LOCA	3.88E-4	1.40E-4	1E-4	ANO-1 IREP
2	Medium LOCA	6.11E-4	2.56E-4	3E-4	ANO-1 IREP
3	Small LOCA	9.07E-3	2.33E-3	1E-3	Sec. 3.1.2.8
4	Steam generator tube rupture	3.92E-2	1.33E-2	4E-2	Sec. 3.1.2.2
5	Steam line break inside containment	3.88E-4	1.40E-4	4E-2	Sec. 3.1.2.3
6	Steam line break outside containment	3.78E-2	1.40E-2	1E-4	EPRI NP-2230
7	Loss of RCS flow	4.91E-1	3.26E-1		
8	Loss of main feedwater flow	7.29E-1	4.77E-1	7.24[a]	
9	Primary-to-secondary power mismatch	3.83	2.53		Sec. 3.1.2.4
10	Turbine trip	2.33	1.99	2.32[b]	
11	Reactor trip	3.03	2.32		
12	Core power excursion	7.18E-2	3.17E-2		
13	Spurious safety injection	4.99E-2	1.83E-2	6E-2	EPRI NP-2230
14	Loss of offsite power	1.1E-1	9.23E-2	1E-1	Sec. 3.1.2.5
15	Incore instrument tube rupture	9.2E-4	4.37E-4	4E-4	Sec. 3.1.2.6
16	Special LOCA initiators				
	a. interfacing sys. LOCA (event V)	1.9E-6	7.4E-9	8E-7	Sec. 3.1.2.7
	b. catastrophic reactor vessel rupture	3.0E-7	1.0E-7	1E-7	WASH-1400
17	Loss of a single service water train	1.27E-2	7.23E-3	3E-2	EPRI NP-2230
18	Loss of a single vital DC bus	3.91E-3	2.79E-3	3.6E-2[c]	ANO-1 IREP
19	Total loss of vital DC power	1.4E-8	9.91E-9	ε	ANO-1 IREP
20	Loss of vital AC bus 120VAC-1 or -2	6.15E-2	1.72E-2	7.0E-2[d]	ANO-1 IREP
21	Loss of vital AC bus 120-VAC-3 or-4	6.15E-2	1.72E-2	7.0E-2[d]	ANO-1 IREP

[a] PCS available transients

[b] Loss of PCS transients

[c] This point estimate value, for two buses, is twice the ANO-1 IREP frequency of 1.8E-2/bus.

[d] This point estimate value, for two buses, is twice the ANO-1 IREP frequency of 3.5E-2/bus.

contributor to the frequency of steamline breaks inside containment. The case of steamline break outside containment is dominated by large pipe breaks and would have a frequency identical to large LOCAs, which is consistent with assumptions made in previous PRAs.

3.1.2.4 Anticipated Transients

The discussion in Section 3.1.1 describes the regrouping of transient classes 7 through 12 into two classes representing the condition of the PCS following the initiator. Tables 3.1-2a and 3.1-2b show the point estimate frequency calculations for these two classes. The frequencies for individual transient types were taken directly from EPRI NP-2230. The frequency of events which appear in both classes was split equally between the classes. There is no significant difference between the total frequency of classes 7 through 12 from the PSS and the frequency of the two new classes developed here, since the same basic data source was utilized for both.

3.1.2.5 Loss of Offsite Power

The Bayesian treatment of this event in the PSS is judged to be reasonable. The historical frequency of LOSP events at the Millstone site (one event in 13 years) cannot be statistically demonstrated to be significantly different from other sites in the region. On the other hand, there is sufficient evidence to suggest that the regional grid is a contributor to differences in LOSP frequency across the country. That is, statistical evidence shows that plant location (in a regional sense) does have an effect on LOSP frequency. Although it is by no means the only effect, it is one which has easily accessible data. The point estimate for the historical LOSP frequency for the nuclear sites in the Northeast Power Coordinating Council (from NUREG/CR-2815, the NREP Procedures Guide) is 0.3 LOSP events per year. The value for LOSP used in the PSS is 0.11, substantially lower but not unreasonably so, and there appears to be evidence to support this number. The PSS, however, did not provide adequate justification for the use of this lower number.

The recovery of offsite power values developed in the PSS were also reviewed. This analysis utilized data specifically pertaining to facilities in the Northeast Power Coordinating Council. The PSS, however, did not include the 1976 event at Millstone Point which resulted in an extended loss of offsite power. They removed this event from the data base because they felt that improvements in switchyard design completely eliminated this specific failure mode. In addition, the length of the outage reported for this event is noted to be conservative, because offsite power was recovered earlier but the operators chose to stay on emergency power since it was available. The PSS values were compared with the recovery values developed for the same site during the Millstone 1 IREP study which were taken directly from EPRI NP-2301, Loss of Offsite Power in Nuclear Power Plants: Data and Analysis (Ref. 3.1-7). Although the PSS values are somewhat more optimistic than the IREP values, they are surprisingly close, especially in the early time frame (less than a factor of 2 reaching about a factor of 2 at two hours and about a factor of 5 at eight hours). Thus, the offsite power recovery values developed in the PSS were judged to be acceptable, with recognition of the fact that use of the EPRI/IREP values would affect the values of extended total station blackout sequences by factors of 2 to 5.

3.1.2.6 Incore Instrument Tube Rupture

It is unclear how the PSS came up with its values for this event, other than a statement that the values are based on WASH-1400 and utilize the Bayesian techniques previously discussed. We performed a simple bounding calculation based on the assumption that each tube is a single pipe segment of less than 3-inch diameter and thus has a failure rate of 1E-9/hour (from WASH-1400). We estimated that there are approximately 40 such tubes. This results in a frequency for the tube rupture event of approximately 4E-4/year, which we will use as our point estimate value. This is the same as the PSS median value for this event.

3.1.2.7 Interfacing Systems LOCA (Event V)

The PSS determined that the frequency of event V is dominated by the RHR suction line valve failure and that injection line valve failure is not significant. This is logical since the injection lines contain three valves and the suction line only two. Both NUREG/CR-2787 (ANO-1 IREP) and NUREG/CR-2515 (Crystal River-3 Safety Study) (Ref. 3.1-8) concluded that these frequencies were small. The Crystal River study estimated that the frequency of event V was approximately 1E-9 per injection path for paths containing two check valves and a normally open, motor-operated valve which could be closed following initial blowdown. Using the same method as used in the Crystal River study, we performed a simple bounding calculation for a point estimate of event V in either of the two RHR suction lines at Millstone. Using a failure rate of 1E-7/hour for catastrophic internal leakage in a motor-operated valve (from the NREP Procedures Guide), and assuming that the inboard valve must fail first before the outboard valve is exposed to high pressure, the frequency of event V is estimated to be:

$$(2) * (1\text{E-}7/\text{hr} * 8760\text{hr/yr}) * (1/2\ \text{yr} * 1\text{E-}7/\text{hr} * 8760\text{hr/yr}) = 8\text{E-}7/\text{year} \qquad (3\text{-}1)$$

As previously stated, the presence of an additional valve in the injection paths would make the contribution to event V from these other paths negligible. Thus, our point estimate is based only on the RHR suction path. The sophisticated treatment of this event in the PSS by the use of DPD arithmetic is not considered justified since it results in a remarkably skewed distribution for this event, as discussed in Section 3.1.2.1. Although this result is a consequence of the consistent application of the techniques utilized throughout the study, which were based on the NREP Procedures Guide, the result should have been recognized by the PSS study team as being unrealistic. This particular case is clearly an exception to the general rule governing the use of a loguniform distribution, and a distribution should have been found which had a lower mean/median ratio and which did not place the mean near the 90% confidence bound. This problem is particularly meaningful in this case since this event is the dominant contributor to the final risk results for internal events in the PSS, so that the final risk curves for early fatalities have the same distribution as this event. Thus, the conclusions drawn from the risk curves are driven solely by the statistical technique utilized rather than the plant model itself; this fact alone argues for the rejection of the PSS distribution. It was replaced with the above-calculated best estimate in our requantification.

3.1.2.8 Small LOCA

The PSS combined classical and Bayesian analyses to determine the frequency of the small LOCA event. Bayesian analysis was utilized to evaluate the frequency of random pipe breaks of this size range and classical analysis was utilized to evaluate the frequency of reactor coolant pump (RCP) seal LOCAs, which also fall into this break size. The PSS does not make clear where the data for the classical analysis comes from. It is clear, however, that this data does not agree with the estimate of RCP seal LOCAs from the ANO-1 IREP study. Further, the Millstone plant has loop isolation valves which could be used to isolate RCP seal LOCAs but they took no credit for this action even though procedure guidelines exist. Thus, we believe that a different value for small LOCAs should be used. The basis for this value will be the ANO-1 IREP frequencies for small pipe breaks and RCP seal LOCAs, adjusted for recovery. The ANO-1 values are 1E-3/year and 0.02/year respectively. An examination of the operator actions used in the PSS pertaining to small LOCAs reveals that, in general, the operator has on the order of 30 minutes to mitigate this event if the automatic systems fail. Thus, we conclude that if the operator can isolate the break within 30 minutes, the small LOCA event will be terminated. This recovery would apply only to RCP seal LOCAs, which would always occur between the loop isolation valves. Using the cognitive error model recommended in the NREP Procedures Guide (NUREG/CR-2815), the probability of the operator failing to diagnose and take proper action within 30 minutes is 0.01/demand. Since the valve failure rates per demand are approximately an order of magnitude lower than the operator error probability, the total failure probability for this action can be estimated as 0.01/demand. Thus, the total frequency of small LOCAs is estimated to be:

$$F(\text{S-LOCA}) = (1\text{E-}3) + (.02)(.01) = 1\text{E-}3/\text{year} \qquad (3\text{-}2)$$

This value is used in the recalculation of plant damage state frequencies contained herein. One additional important note is that it is not clear how the ability of the operator to perform this action will be affected by the support system state. Therefore, this value will be used only for support state 1, where all support systems are available. For all other support states it will be assumed that at least one of the loop isolation valves cannot be closed and the frequency of small LOCAs will be estimated as 0.02 for these support states. This conservative assumption is not believed to have a significant impact on the results.

3.1.3 Issues of Importance to the NRC

In their instructions for this review, the NRC listed certain issues of concern to them. They wanted to know how these issues were treated in the PSS. Some of those issues were either treated or should have been treated in the initiating event analysis and are discussed in this section.

3.1.3.1 Issues Directly Included as Initiating Events

A number of the issues of concern were directly included in the analysis as initiating events. This was accomplished in one of two ways. Some of the events became specific initiator classes. Other events were subsets of other initiator classes and were included as contributors to those classes. Whenever a comment in parentheses refers to "now..." it means that the event in question has been regrouped into one of the two new initiator classes discussed in Section 3.1.1. The events which become initiator classes are:

- loss of DC power
- loss of instrument and control power
- steam generator tube rupture
- loss of service water
- turbine trip (now divided between loss of PCS and PCS available)
- loss of main feed (now part of loss of PCS)

The events which were subsets of another initiator class (and which class) are:

- loss of component cooling water (loss of main feed)
- reactor coolant pump seal failure (small LOCA)
- boron dilution (core power excursion, now PCS available)
- excess feedwater flow (primary/secondary power mismatch, now loss of PCS)
- loss of instrument or control air (turbine trip, now loss of PCS)

3.1.3.2 Loss of Component Cooling Water (CCW)

Although this event was treated as part of another initiator class, further discussion is warranted. The CCW system has been shown to be a significant dependency in previous PRAs because it usually serves to provide cooling to many key components and systems. At Millstone, however, the design is very different: first, Millstone has two CCW systems, one for the turbine plant (TPCCW) and one for the reactor plant (RPCCW); second, neither CCW system provides cooling to any safety-related equipment. Unlike other designs, essential cooling to the safety-related equipment is provided directly by the service water system without the use of an intermediate loop. The TPCCW cools a number of components in the secondary cycle, but no safety-related equipment would fail due to loss of this system so that this event has no effect worse than any loss of PCS event. Likewise, the RPCCW cools a number of components in the primary system, but also likewise, no safety-related equipment would fail due to loss of this system. Therefore, this event has no effect worse than any PCS available event.

3.1.3.3 Multiple Instrument Tube LOCA Below Core Level

The PSS does not treat this event. It does treat the single-tube LOCA as a special class of small LOCA. Since the small LOCA category ranges up to a 2-inch equivalent diameter break, multiple breaks would still fall generally into the small LOCA class. However, no specific analysis was performed to determine if the behavior of multiple tube rupture events was essentially identical to the single tube events. This event has not been modeled in previous PRAs, and it is beyond the scope of this review to perform a detailed analysis of these types of events.

3.1.3.4 Pipe Breaks in the Auxiliary Building

This class of events, as well as pipe breaks in all other plant areas, was evaluated in the external events portion of the PSS in the analysis of internal flooding mechanisms. Our review of these events is discussed in Section 4 of this report.

3.1.3.5 Loss of Ventilation in the Auxiliary Building

Loss of ventilation events are not treated as initiators in the PSS. In general, previous PRAs have not considered these events as initiators. This approach is considered to be reasonable since loss of ventilation to specific plant areas are not likely to result in plant trip and degradation of mitigating systems in ways not foreseen by other initiators. It is our judgment that the omission of this event as an initiator does not affect the study results.

3.1.4 References for Section 3.1

3.1-1 U.S. Nuclear Regulatory Commission, "Reactor Safety Study - An Assessment of Accident Risks in U.S. Commerical Nuclear Power Plants," USNRC Report WASH-1400 (NUREG-75/014), October 1975.

3.1-2 Electric Power Research Institute, "ATWS: A Reappraisal, Part 3: Frequency of Anticipated Transients, EPRI Report NP-2230, January 1982.

3.1-3 D. D. Carlson et al., Sandia National Laboratories, "Interim Reliability Evaluation Program Proceduces Guide," USNRC Report NUREG/CR-2728, January 1982.

3.1-4 I. A. Papazoglou et al., Brookhaven National Laboratory, "National Reliability Evaluation Program (NREP) Procedures Guide," USNRC Report NUREG/CR-2815, (Final Draft), September 9, 1982.

3.1-5 G. J. Kolb et al., Sandia National Laboratories, "Interim Reliability Evaluation Program: Analysis of the Arkansas Nuclear One - Unit 1 Nuclear Power Plant," USNRC Report NUREG/CR-2787, June 1982.

3.1-6 J. H. Morehouse et al., "Value-Impact Analysis of Recommendations Concerning Steam Generator Tube Degradation and Rupture Events," USNRC Generic Letter 82-83, September 1982.

3.1-7 Electric Power Research Institute, "Loss of Offsite Power at Nuclear Power Plants: Data and Analysis," EPRI Report NP-2301, March 1982.

3.1-8 A. A. Garcia et al., Science Applications, Inc., "Crystal River - 3 Safety Study," USNRC Report NUREG/CR-2515, December 1981.

3.2 Event Trees

The MP 3 PSS constructed 22 event trees to represent plant response to the initiators discussed in Section 3.1. We have reviewed these trees to determine if they are a reasonable representation of that response. The assumptions which went into the tree construction were compared to assumptions used in previously performed PRAs. Where there were notable differences, these differences were evaluated to determine if they were reasonable. Each of these differences is discussed in this section. Additionally, a number of issues of specific interest to the NRC were also examined. The final set of event trees, which include all revisions and modifications we considered necessary, are shown in Figs. 3.2-1 through 3.2-11. We have retained the sequence number used in the PSS where possible to allow direct comparison between the trees in the PSS and those here. All top events in our event trees are defined in Table 3.2-1. The plant damage states into which the accident sequences are assigned are described in Table 3.2-2.

3.2.1 General Event Tree Findings

This section presents the results of our evaluation for items which pertain to more than one event tree.

3.2.1.1 Treatment of Operator Action

The event trees were constructed by including major operator actions as events on the trees. The inclusion of these actions for the purpose of crediting successful operator response to the mitigation of accident conditions was performed in a consistent and correct manner. However, the possibility of erroneous operator action due to incorrect interpretation of plant conditions was not treated. In particular, this pertains to the operator performing one of the major actions modeled during a sequence of events when the operator action is not required. Since these actions are called for in procedures, it certainly seems to be possible for this type of error to occur. For most of the operator actions modeled this is not a problem, since they involve backup methods of performing safety functions. Performing these actions when they are not required would not degrade performance of the function. However, there are two actions which involve shutting down or reducing flow from safety systems. Performing these actions at the improper time could result in a situation where there is insufficient core cooling. Thus, it was considered necessary to include two additional actions on the event trees.

- Operator Action OA-2-E, Improper Throttling of HPI: The operator has determined that he can conserve RWST inventory by reducing HPI flow. In performing this action he does not correctly determine how far he can throttle HPI, and he throttles it back too far resulting in insufficient injection flow. He fails to notice this in time and therefore does not recover his error, resulting in core melt. He also overrides quench spray actuation to further conserve RWST inventory, resulting in the sprays being unavailable. This error is applicable to small LOCA and incore instrument tube rupture events. The event trees have been modified to incorporate this new event. Figures 3.2-3 and 3.2-4 show the revised trees, with the revisions appearing mainly on sheet two of each figure.

- Operator Action OA-6-E, Erroneous Shutdown of HPI: The operator believes that a spurious safety injection event has occurred and that auxiliary feedwater is operating. Following procedure, he shuts down the HPI system. He fails to notice his error in time and a core melt results.

Table 3.2.1 Event tree top event definitions.

Symbol	Definition
ACC	Failure of accumulators
AF1	Failure of auxiliary feedwater
AF2	Failure of auxiliary feedwater (SGTR and steamline breaks)
AF3	Failure to recover auxiliary feedwater motor pumps (LOSP)
E60	Failure to restore offsite power for 1 hour
E120	Failure to restore offsite power for 1 to 2 hours
HP2	Failure of high pressure injection
LP	Failure of low pressure injection
OA1	Operator fails to blow down SGs and initiate LPI
OA2	Operator fails to conserve RWST inventory (control flow)
OA2E	Operator overthrottles HPI resulting in inadequate flow
OA3	Operator fails to establish primary bleed
OA4	Operator fails to blow down SGs during SGTR
OA5	Operator fails to establish primary bleed during SGTR
OA6	Operator fails to prevent pressurizer overfill (control HPI)
OA6E	Operator erroneously terminates high pressure injection
OA7	Operator fails to establish primary bleed and feed
OA8	Operator fails to establish emergency boration during ATWS
OA8R	Operator fails to establish HPI during ATWS consequential LOCA
OA9	Operator fails to delay recirculation when sump empty
OA10	Operator fails to control HPI during SGTR
PCS	Failure of power conversion system
PL	ATWS pressure spike exceeds Service Level C (unfavorable MTC)
PR	Consequential LOCA due to moderate ATWS pressure spike
QS	Failure of quench spray
QS'	Failure to recover quench spray (i.e., restore OSP in 2-8 hours)
RPS(E)	Failure to scram - electrical failure of RPS
RPS(M)	Failure to scram - mechanical failure of RPS
RT1	Failure of automatic reactor scram
RT3	Operator fails to manually scram reactor
RT4	Failure of both automatic and operator manual reactor scram
R1	Failure of low pressure recirculation
R2	Failure of high pressure recirculation
R3	Failure of containment spray recirculation
SA	Failure of safety injection actuation
SBI	Consequential steamline break inside containment
SBO	Consequential steamline break outside containment
S2	Consequential small LOCA
SL	Consequential steamline leak during SGTR
TK	Failure of RWST
TT	ATWS turbine trip fails

Note: Tree top events which are "primed" (e.g., OA7') and not listed individually on this table have the same definition as the "unprimed" version, but are quantified differently to account for differences in the particular scenarios in which they appear.

Table 3.2.2 Plant damage state descriptions.

Symbol	Description
AEC	Large LOCA, early melt
AEC'	Large LOCA, early melt, failure of recirculation spray
AEC"	Large LOCA, early melt, failure of quench spray
AE	Large LOCA, early melt, no containment cooling
ALC	Large LOCA, late melt
ALC'	Large LOCA, late melt, failure of recirculation spary
ALC"	Large LOCA, late melt, no containment cooling
SEC	Small LOCA, early melt
SEC'	Small LOCA, early melt, failure of recirculation spray
SEC"	Small LOCA, early melt, failure of quency spary
SE	Small LOCA, early melt, no containment cooling
SLC	Small LOCA, late melt
SLC'	Small LOCA, late melt, failure of recirculation spray
SLC"	Small LOCA, late melt, failure of quench spary
SL	Small LOCA, late melt, no containment cooling
TEC	Transient, early melt
TEC'	Transient, early melt, failure of recirculation spary
TEC"	Transient, early melt, failure of quench spary
TE	Transient, early melt, no containment cooling
TLC	Transient, late melt
TLC'	Transient, late melt, failure of recirculation spray
TL	Transient, late melt, no containment cooling
S'EC	Incore instrument tube LOCA, early melt
S'E	Incore instrument tube LOCA, early melt, no cont. cooling
S'L	Incore instrument tube LOCA, late melt, no cont. cooling
V2EC	Steam generator tube rupture, steam leak, early melt
V2EC'	SGTR, steam leak, early melt, failure of recirc. spary
V2EC"	SGTR, steam leak, early melt, failure of quench spray
V2E	SGTR, steam leak, early melt, no containment cooling
V2LC	SGTR, steam leak, late melt
V2LC'	SGTR, steam leak, late melt, failure of recirc. spray
V2LC"	SGTR, steam leak, late melt, failure of quench spray
V2L	SGTR, steam leak, late melt, no containment cooling
V	Interfacing systems LOCA

This event applies to the spurious SI and steamline break (inside or outside containment) events when auxiliary feedwater has failed, and also to a misdiagnosis of small LOCA, incore instrument tube rupture, and steam generator tube rupture events. The event trees for these five initiators have been modified to incorporate this new event. These are shown, respectively, in Figs. 3.2-10. 3.2-6, 3.2-3, 3.2-4 and 3.2-5.

3.2.1.2 Use of Secondary Depressurization

The Millstone 3 PSS assumes that it is possible to provide safety injection during small- and medium-sized LOCA events when HPI is unavailable, by depressurizing the secondary and using low pressure injection (event OA-1). The phenomenology assumed is that by opening the secondary atmospheric relief valves, the increased heat removal rate will depressurize the primary sufficiently to allow the accumulators to inject, which will reduce pressure further until it is below the RHR pump discharge shutoff head. This method has not been credited in previous PRAs. However, calculations by Westinghouse published in WCAP-9754 (Ref. 3.2-1) have shown that this method will work and they have included instructions on performing it is the emergency procedure guidelines for this type of plant. This technique is considered viable and we have no reason to believe that the Westinghouse calculations are incorrect. Thus, credit for this scenario is assumed to be justified.

3.2.1.3 Availability of the Power Conversion System

No credit is taken in the PSS for cooldown following plant trip using the power conversion system (PCS).[a] The assumption made is that whenever a plant trip occurs, the PCS will be caused to trip. Previous PRAs have determined that for some transients, the PCS will be available to provide the necessary cooling. Discussions with Millstone 3 operations personnel have verified that the PCS will often be available following plant trip. Not taking credit for this capability is a conservative assumption that will result in an overestimation of risk for these transients which do not affect secondary systems operation. A revised transient event tree is shown in Fig. 3.2-7 to represent plant response to transients where the PCS remains available. The transients which fall into this class were discussed in Section 3.1.

The loss of feedwater event tree from the PSS shown in Fig. 3.2-8 can be used to evaluate the loss of PCS events. This tree would be used not only to evaluate the event class referred to as loss of PCS, but also all other transient event classes which result in loss of PCS. In this case, these would be all of the other transient events included in the study (e.g., loss of offsite power, loss of service water, loss of an electrical bus, etc.).

3.2.1.4 Containment Spray Recirculation

The PSS does not consider that core melt may result from the failure to provide containment cooling during recirculation. Previous PRAs have assumed that even when core recirculation cooling is provided, in many cases it is still necessary to provide containment spray recirculation (CSR) in order to prevent containment overpressure failure. The failure of the containment in this way would result in recirculation sump steam flashing with associated cavitation and failure of all recirculation pumps, resulting in core melt. The PSS assumes that core recirculation alone is sufficient to prevent the addition of heat (i.e., steam) to the containment in amounts significant enough to cause containment rupture. This assumption was initially considered unjustified for sequences where all the heat is dumped to the containment prior to being transferred to the ultimate heat sink. However, NU provided

[a] The power conversion system is defined as the main steam, turbine or turbine bypass, main condensor, condensate, and feedwater systems operating at sufficient capacity to remove primary heat.

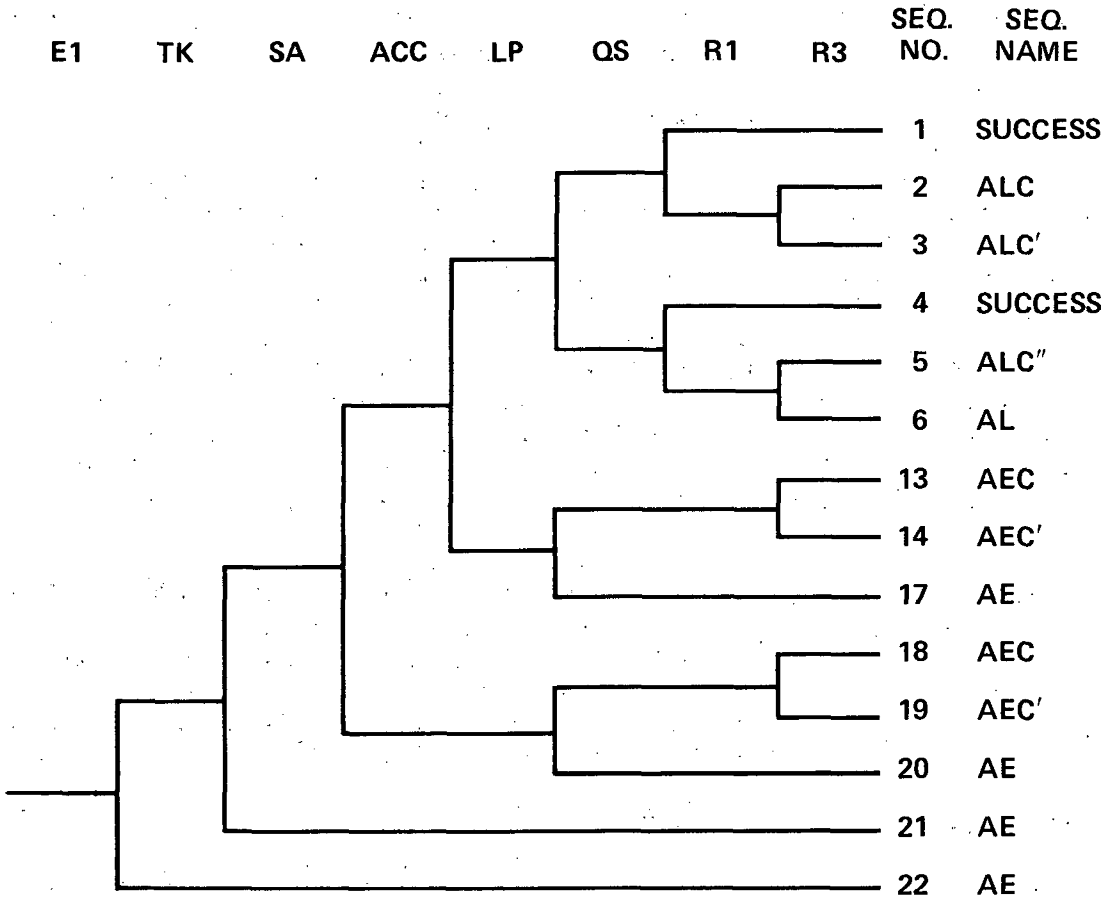


Fig. 3.2-1 Large LOCA event tree.

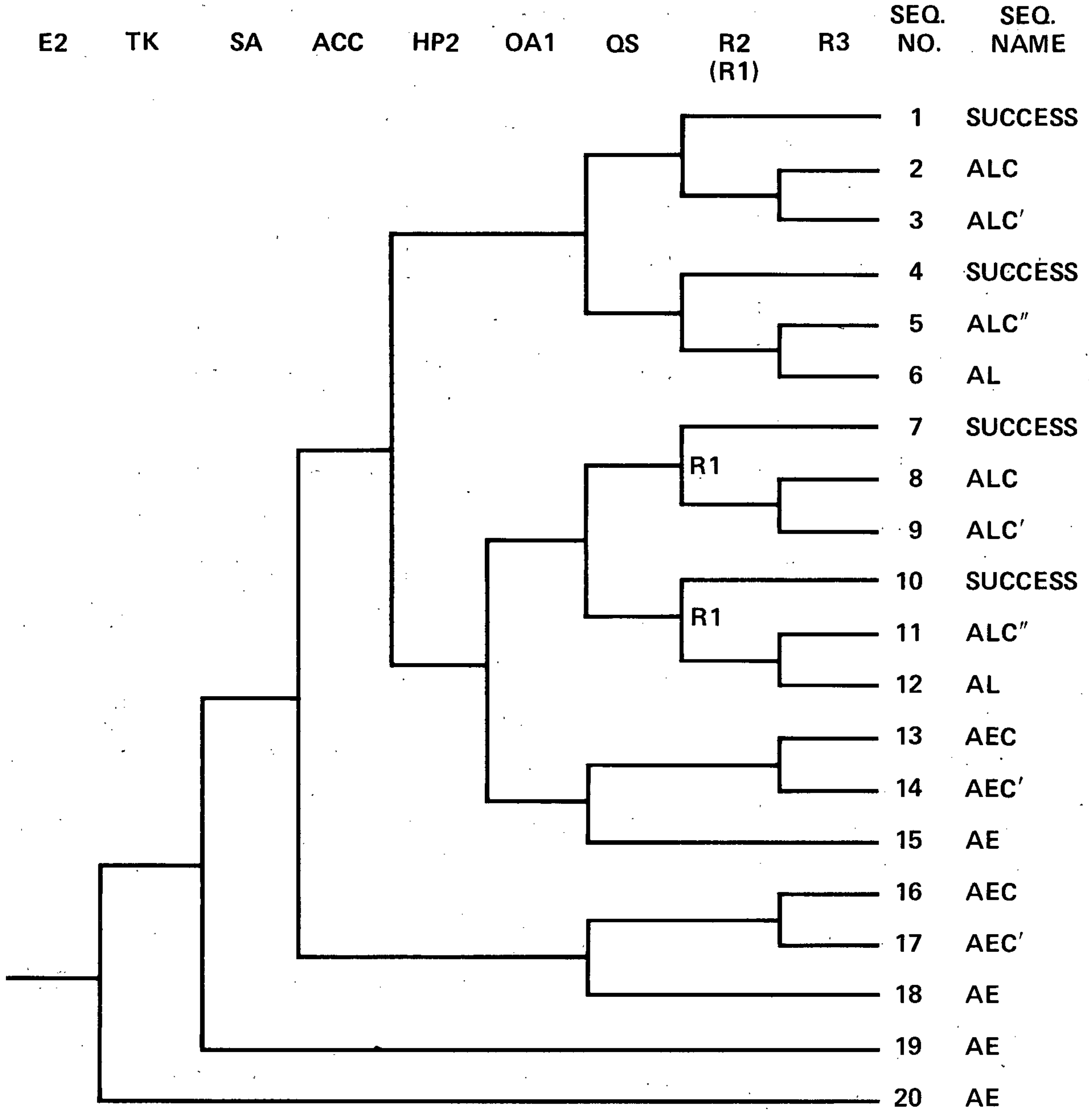


Fig. 3.2-2 Medium LOCA event tree.

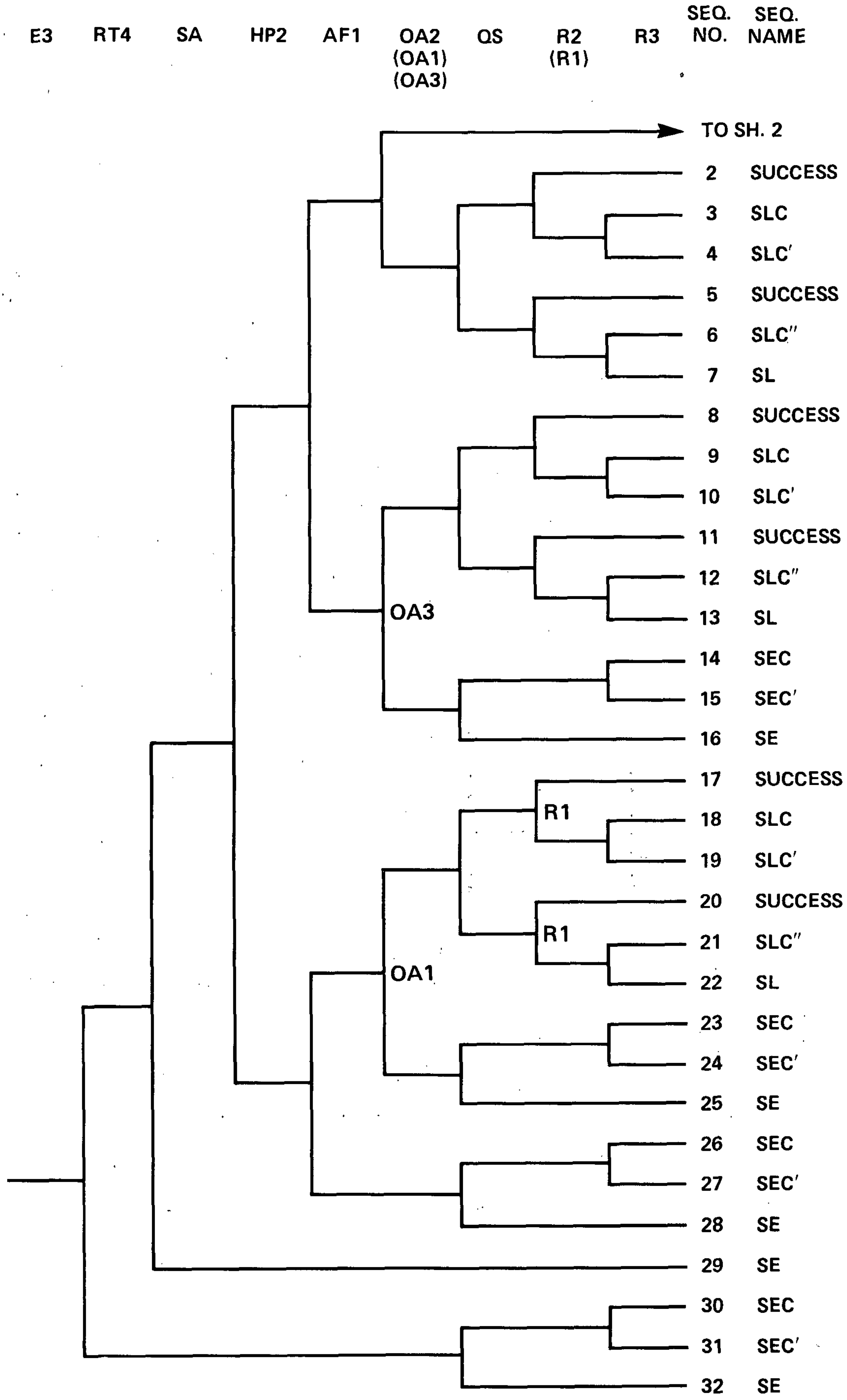


Fig. 3.2-3 Small LOCA event tree (sheet 1 of 2).

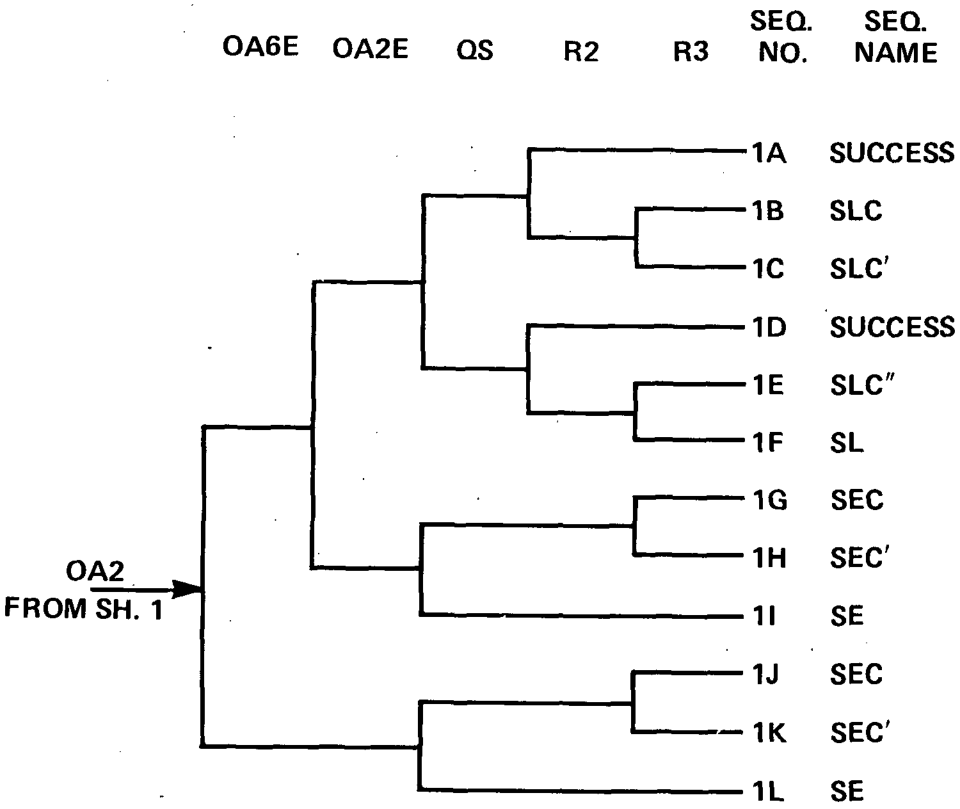


Fig. 3.2-3a Small LOCA event tree (sheet 2 of 2).

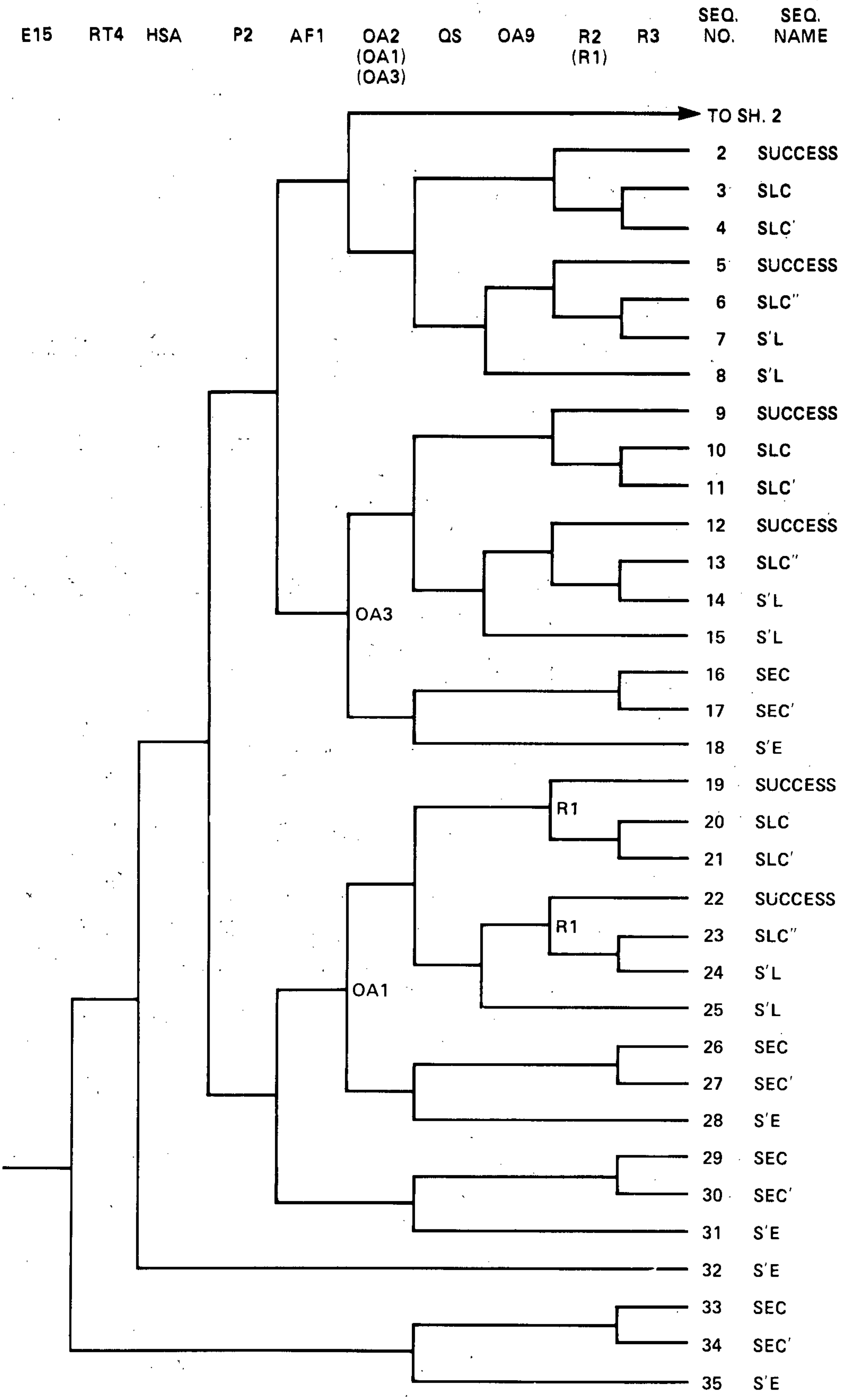


Fig. 3.2-4 Incore instrument tube rupture event tree (sheet 1 of 2).

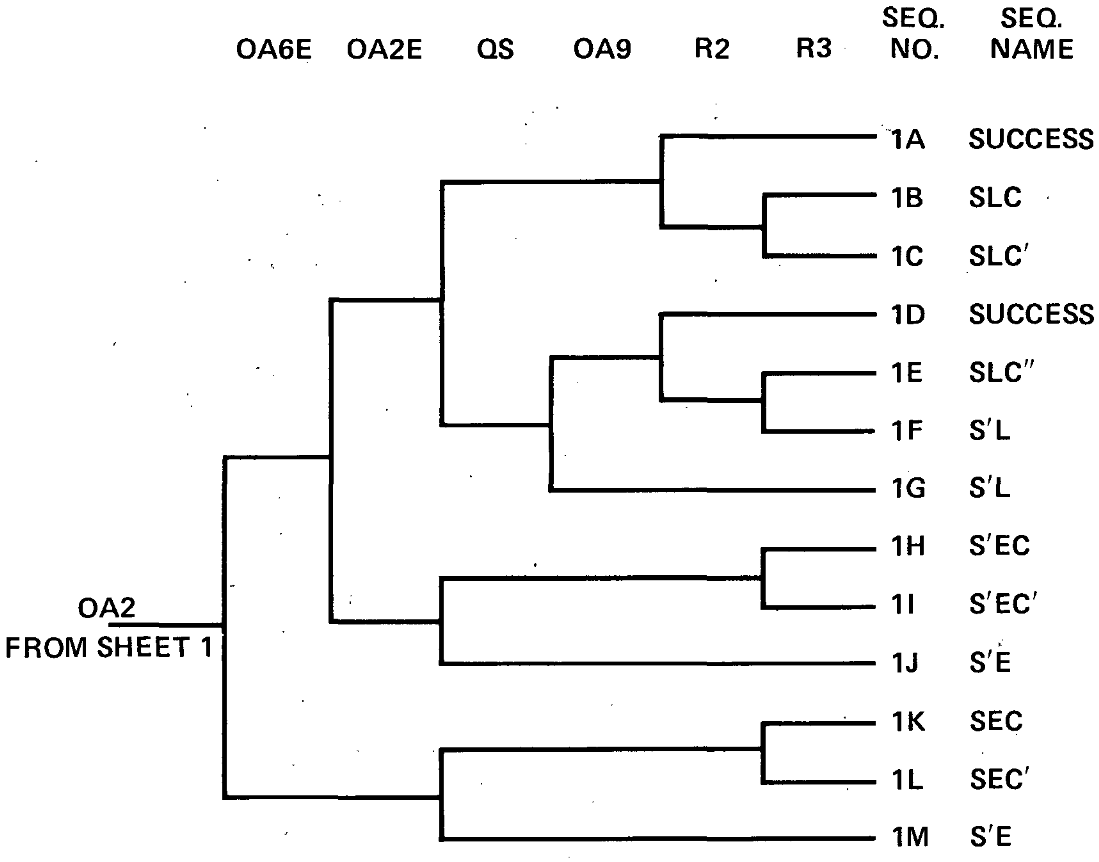


Fig. 3.2-4a Incore instrument tube rupture event tree (sheet 2 of 2).

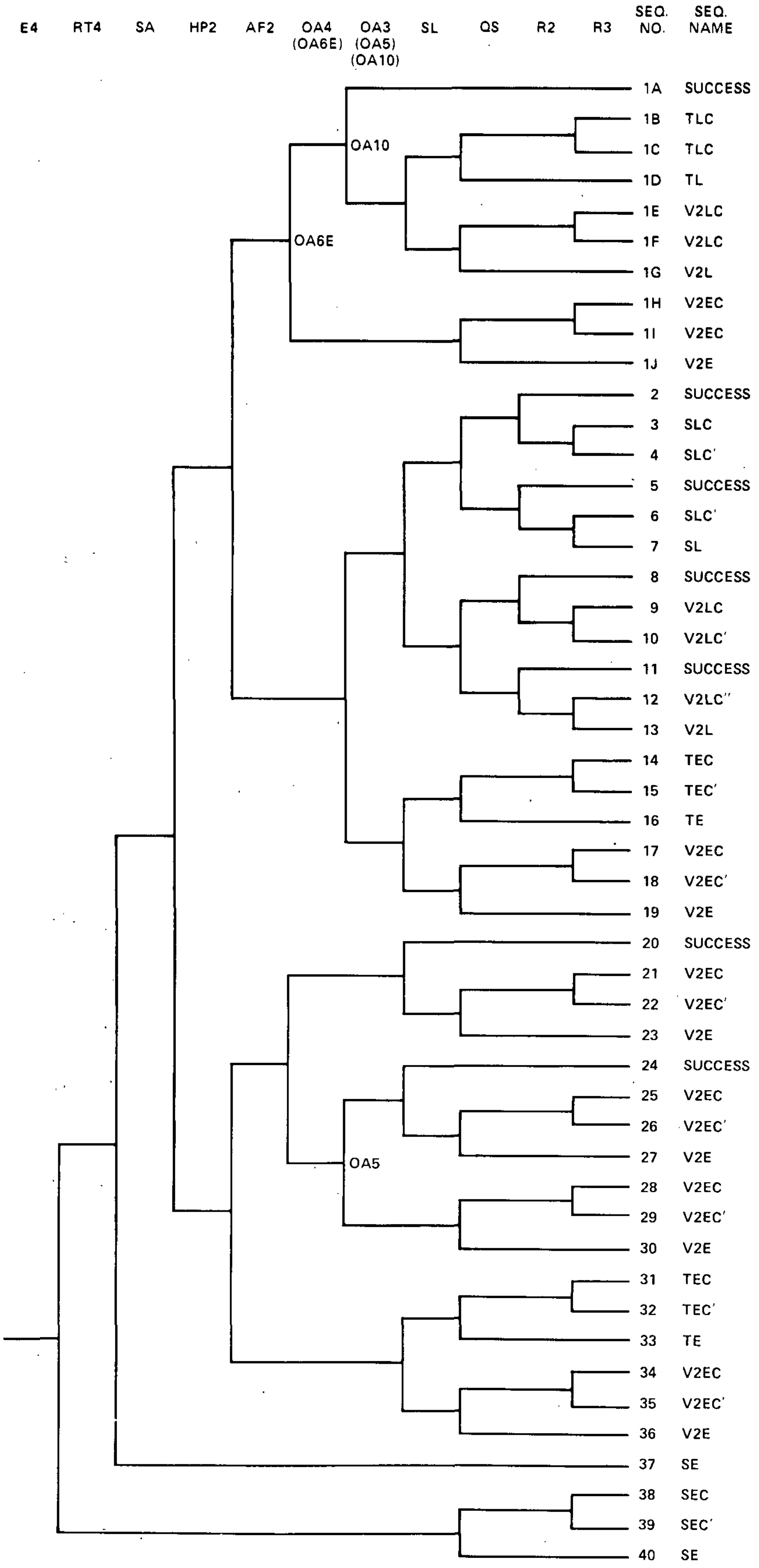


Fig. 3.2-5 Steam generator tube rupture event tree.

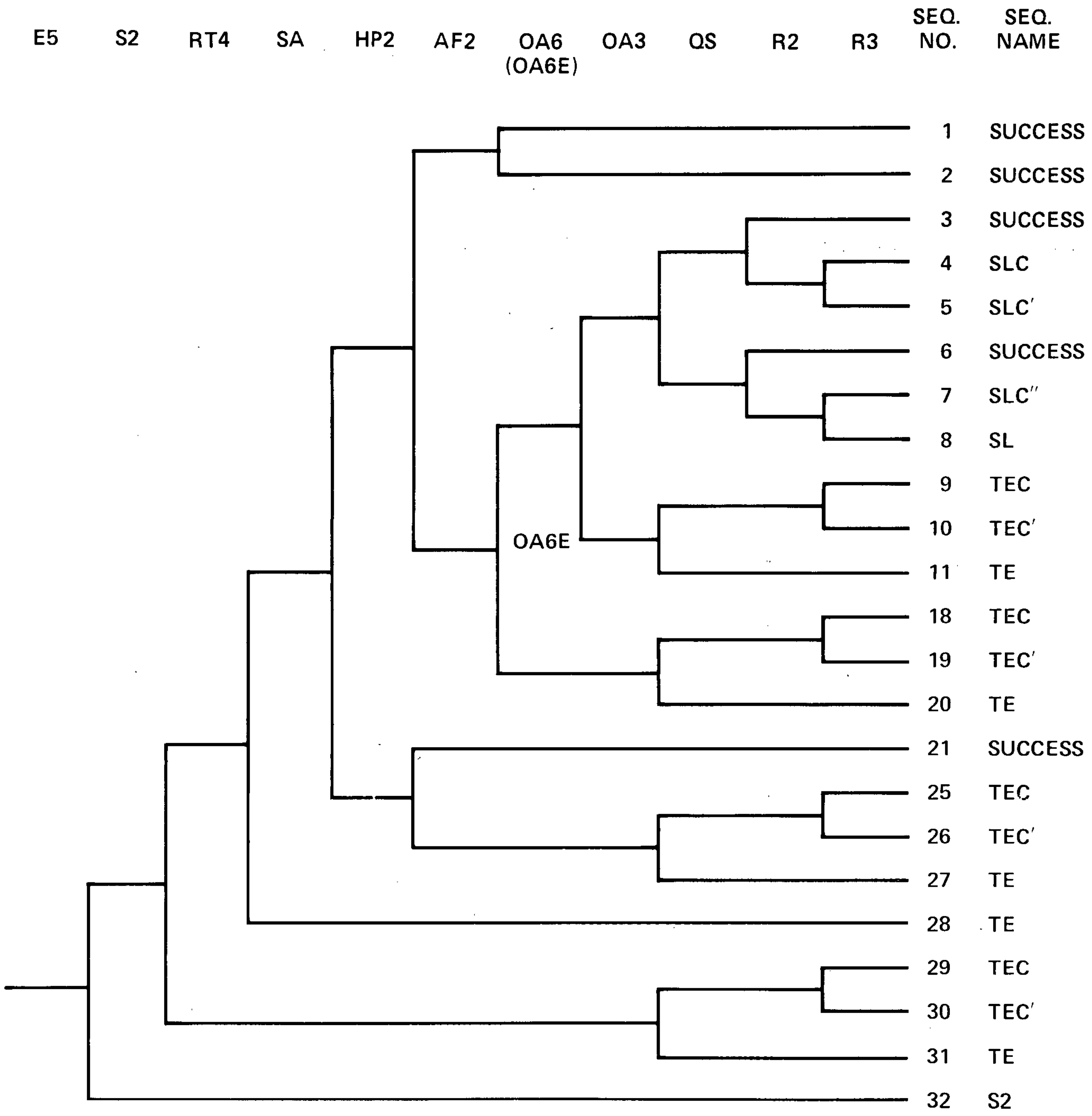


Fig. 3.2-6 Steamline break insure (and outside) containment event tree.

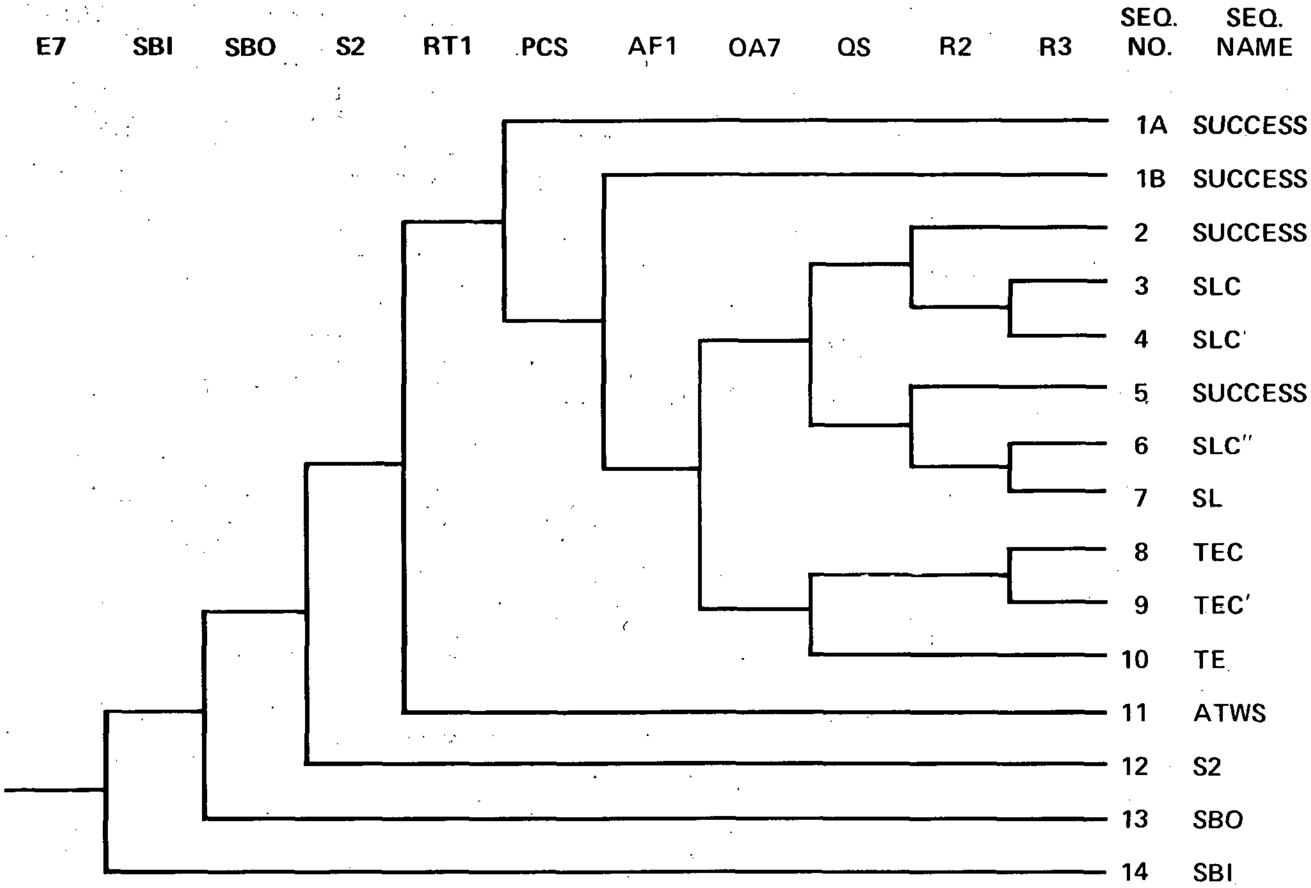


Fig. 3.2-7 Power conversion system available event tree.

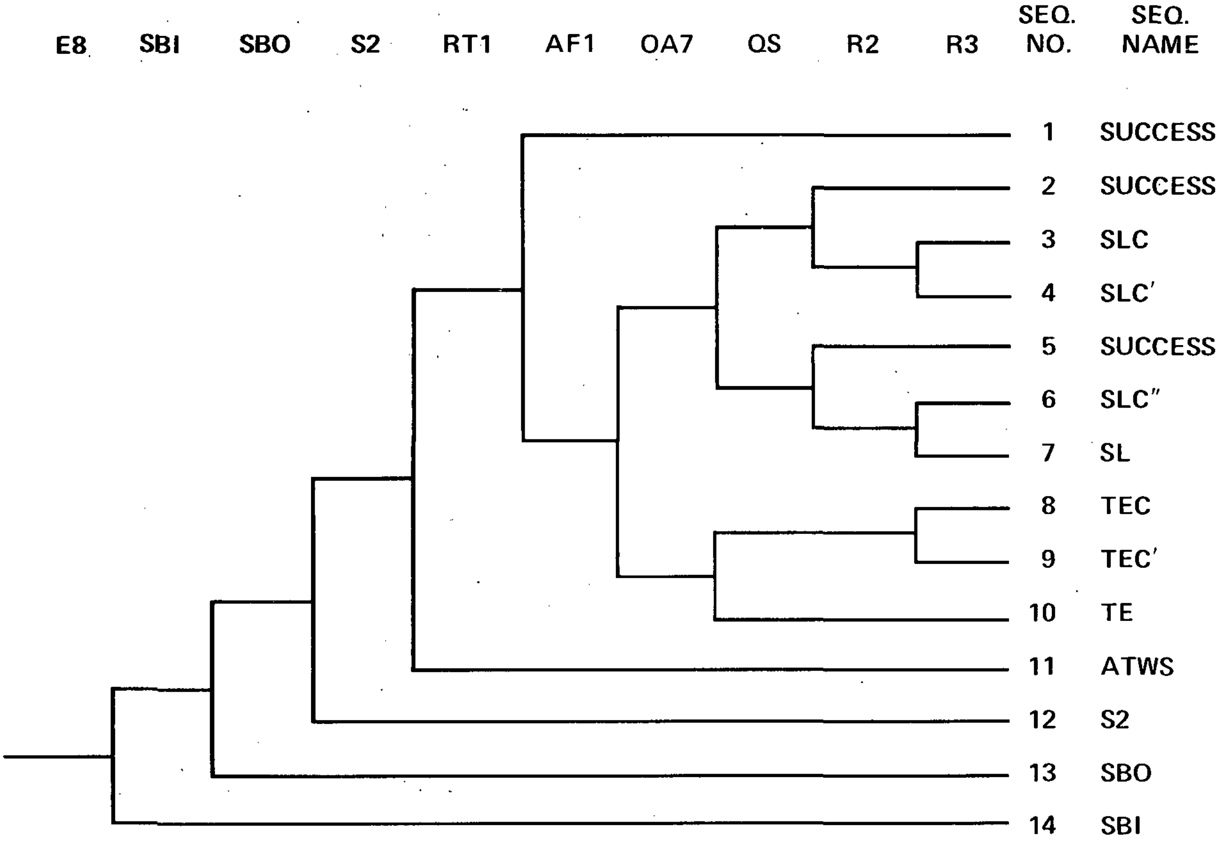


Fig. 3.2-8 Loss of power conversion system event tree.

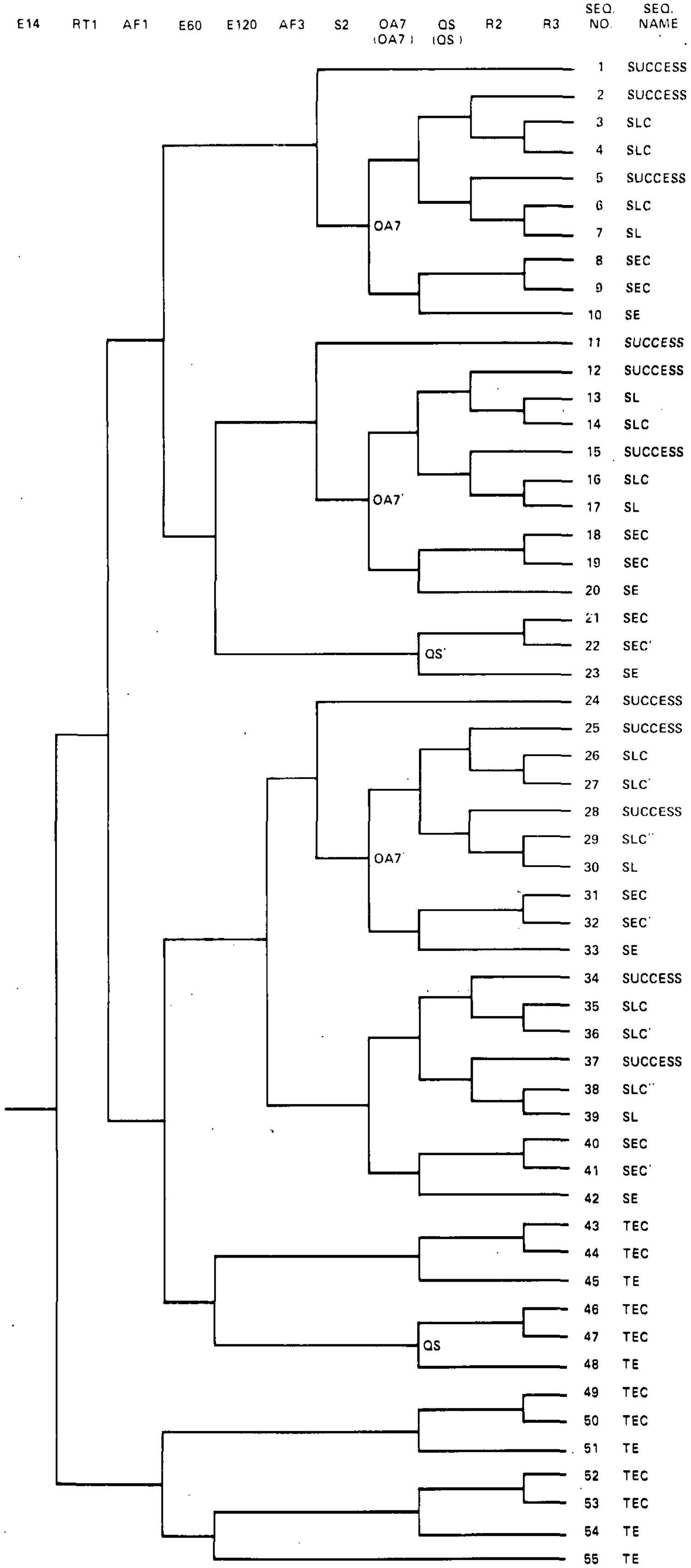


Fig. 3.2-9 Loss of offsite power (support state 7) event tree.

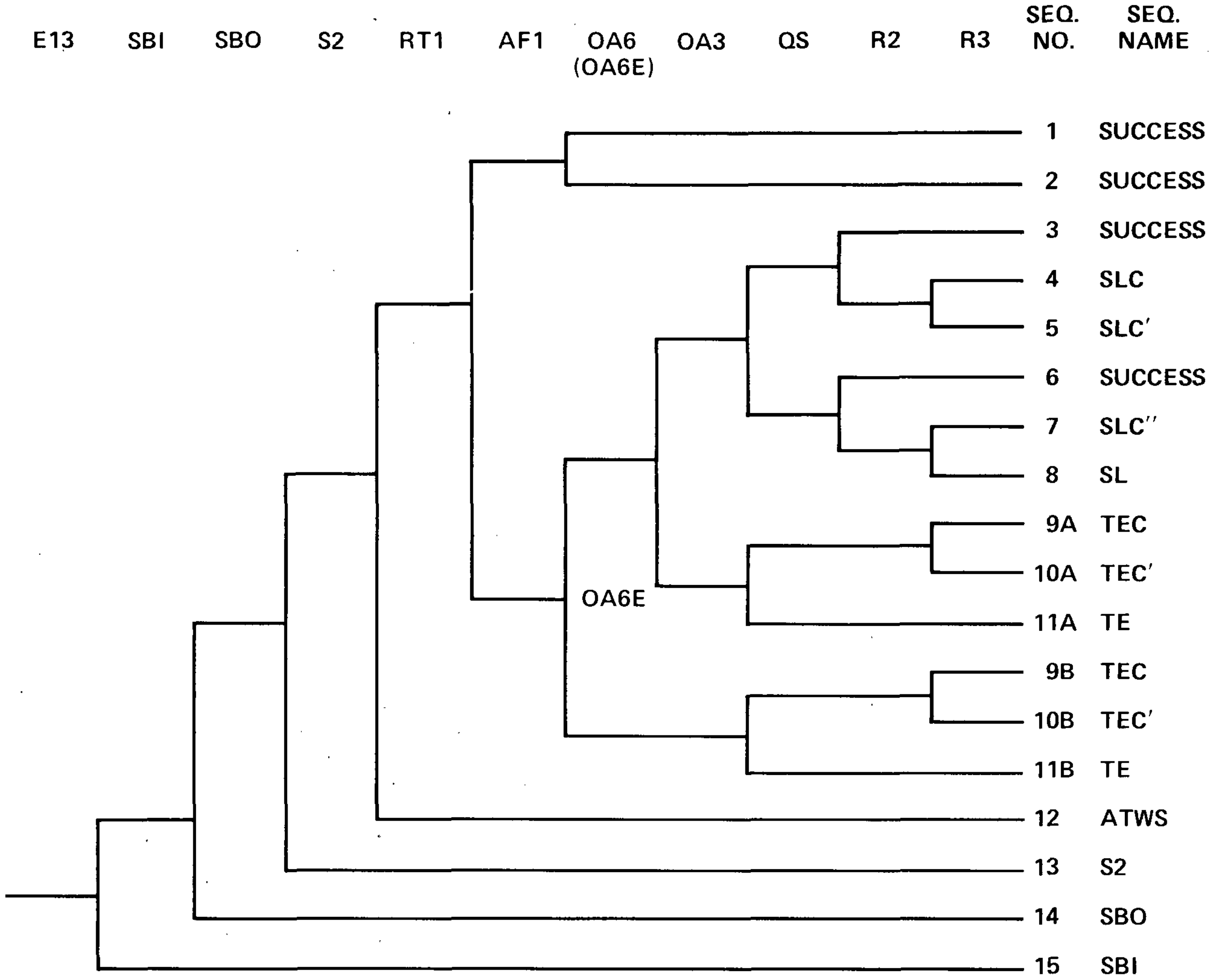


Fig. 3.2-10 Spurious safety injection event tree.

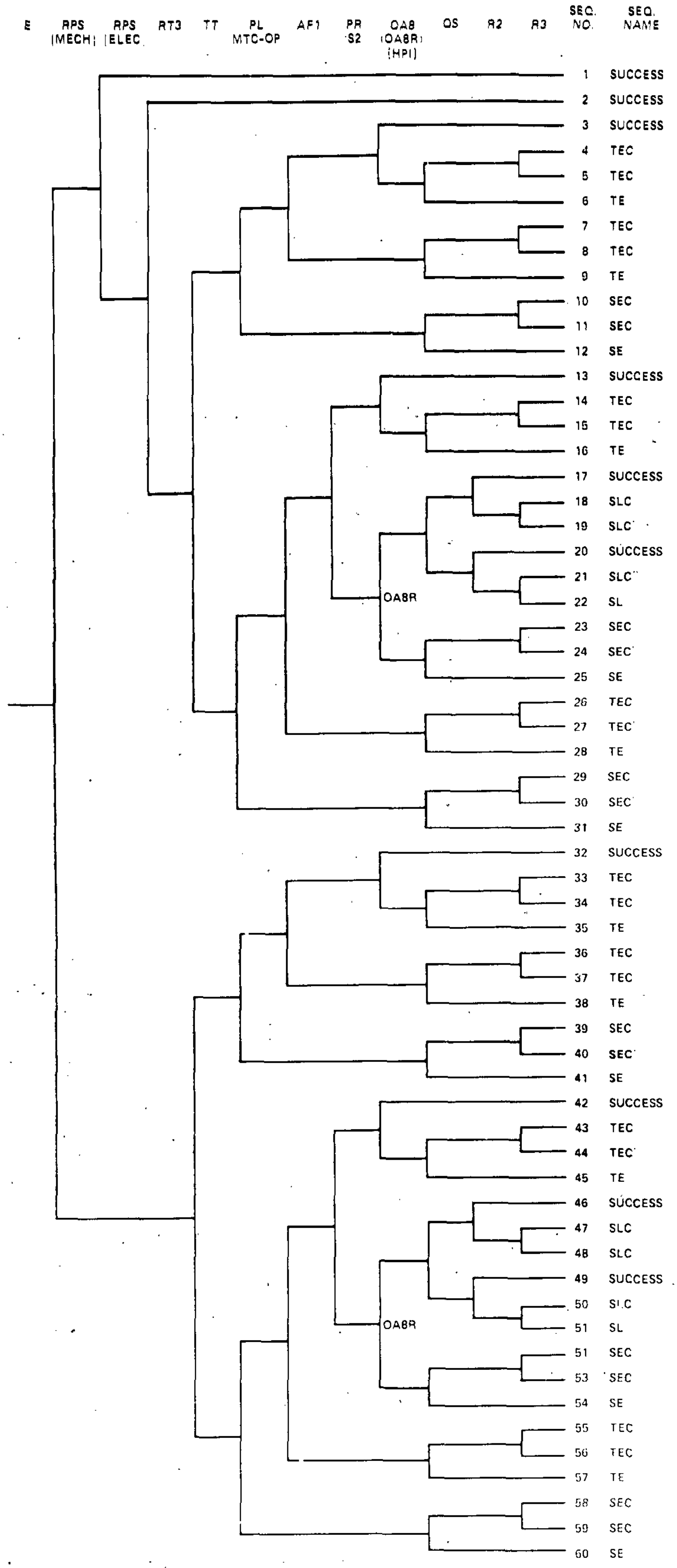


Fig. 3.2-11 Anticipated transient without scram (ATWS) event tree.

the reviewers with additional MARCH 1.1 calculations in response to questions about this scenario. These calculations showed that containment pressure would not exceed design for at least 30 hours for both large and small LOCAs with core recirculation and no sprays at all. The calculations were considered to provide adequate justification for the assumption and no changes were made to the event trees. Prior to being transferred to the ultimate heat sink. However, NU provided the reviewers with additional MARCH 1.1 calculations in response to questions about this scenario. These calculations showed that containment pressure would not exceed design for at least 30 hours for both large and small LOCAs with core recirculation and no sprays at all. The calculations were considered to provide adequate justification for the assumption and no changes were made to the event trees.

3.2.1.5 Primary Bleed and Feed (Once Through) Cooling

In scenarios where auxiliary feedwater is needed for heat removal but is unavailable, the PSS considers providing the necessary cooling by opening the pressurizer power-operated relief valves (PORVs) and using high pressure injection pumps to supply sufficient cooling flow to the core. This technique, referred to as bleed and feed, or once-through cooling, has been determined to be a reasonable cooling method for certain PWRs. It has been shown not to apply in every case. In the case of Millstone-3 class plants, Westinghouse has performed an analysis which shows this method to be viable. The analysis has been published in WCAP-9744 (Ref. 3.2-2). Westinghouse has included bleed and feed in the emergency procedure guidelines for implementation in the plant procedures. It is concluded that the credit taken in the Millstone 3 event trees for this cooling method (OA-3 for small LOCAs and steamline breaks, OA-7 for transients) is appropriate.

3.2.1.6 Conserving RWST Inventory

For small LOCAs and incore instrument tube rupture initiators, the PSS takes credit for the operator taking action to conserve RWST inventory when both high pressure injection and auxiliary feedwater are available, thus extending the injection phase of the accident. This action, referred to as controlled primary depressurization (OA-2), has the operator throttling back HPI in conjunction with depressurizing the secondary, which will reduce break flow and therefore the need for HPI flow. Further, the operator will act to shut down quench spray to further conserve RWST inventory. The combination of these two actions is assumed in the PSS to allow core cooldown without the need for recirculation.

This action has not been credited in previous PRAs, and appears to be a somewhat optimistic view of the scenario. While the break flow is reduced, it is not apparent that it can be terminated by this means. Therefore, although the injection phase can be extended, the need for recirculation is not completely eliminated. This is especially true of the instrument tube rupture event, which would logically be expected to be below the core level so that it would be impossible to stop the break flow. At some point, the RWST will be depleted and recirculation will be required to replenish the continued leakage from the break. The utility supplied additional information regarding this scenario, but it is insufficient to justify the sequence. The only information provided is an emergency procedure guideline (EPG) which instructs the operator how to perform this action. The procedure by which this action is performed is very complex and the EPG contains a number of caveats which indicate there is no guarantee that recirculation can be avoided. Specifically, the EPG instructs the operator to abandon this procedure and switch immediately to recirculation if the RWST level reaches a certain point. It also instructs the operator to return to the LOCA procedure if certain conditions are not met. No calculations were referenced which support the time frames specified by the utility regarding the extension of the injection phase beyond 24 hours. Thus, it is considered that the only credit which is justified for this action is an extension of the time available for other operator actions and recovery actions. Therefore, the applicable trees,which are shown in Figs. 3.2-3 and 3.2-4, have been modified to reflect the eventual need for recirculation during these event sequences.

3.2.2 Specific Event Tree Findings

This section presents review results applicable only to specific event trees.

3.2.2.1 Steamline Breaks (Inside or Outside Containment)

For steamline breaks, the PSS assumes that the failure of main steam isolation (MSI) results in the failure of auxiliary feedwater. The basis for this assumption is unclear, and there seems to be no reasonable explanation for it. In most previous PRAs, main steam isolation has not been assumed to have any affect on the availability of safety systems and was considered only as a key part of the containment isolation system. In the case of auxiliary feedwater, the worst one could assume is that the failure of MSI could affect the availability of the steam-turbine-driven AFW pump due to steam diversion, although this would be unlikely, since very little steam is required to operate this pump. Specifically, for the most likely break, a stuck-open secondary steam relief valve, the flow diversion would be small enough that the steam supply to the turbine would still be sufficient to provide required feedwater flow regardless of the state of MSI. For the less likely case of a major rupture of the steam line, the turbine-driven pump would definitely fail if none of the steam generators were isolated from the break. In either case, the ability of the motor-driven pumps to supply water to the steam generators would not reasonably be expected to be affected. As long as water is supplied in sufficient amounts, cooling will be established regardless of main steam isolation. This assumption is conservative and unjustified. The steamline break trees shown in Fig. 3.2-6 have been modified to reflect this judgment.

3.2.2.2 Steam Generator Tube Rupture (SGTR)

The PSS gives credit for three alternative methods of cooling following SGTR if either high pressure injection or auxiliary feedwater are unavailable.

Each of these methods requires operator action. When auxiliary feedwater is unavailable, the necessary cooling is provided by initiating bleed and feed cooling as discussed in Section 3.2.1.5. When HPI is unavailable, it is required to find alternate means of maintaining primary inventory while AFW is utilized for heat removal. One way to do this is to prevent inventory loss as opposed to replenishing lost inventory. The PSS assumed this could be accomplished in one of two ways. The preferred method is to use secondary depressurization to reduce the primary pressure to below that of the secondary in order to terminate the break flow (OA-4). Failing that, the primary could be depressurized directly by opening a PORV (OA-5), with the same overall effect. The key to the use of these methods is performing the action quickly enough so that the break flow is terminated prior to core uncovery, thus eliminating the need to replenish inventory. If this is accomplished, cooling can be performed by auxiliary feedwater through the unaffected steam generators. These methods have been analyzed by Westinghouse and found to be viable, and they have been included in the emergency procedure guidelines. The credit given to these procedures in the event tree are considered to be reasonable and justified.

Another assumption the PSS makes is that if HPI and AFW are both available following an SGTR event, the event is terminated successfully without further action. This does not seem reasonable, since the primary would be kept at high pressure by the HPI pumps and water would continuously be pumped out of the RCS and into the steam generator. Eventually, the RWST would empty with the RCS still at high pressure with no recirculation available. It seems that some additional operator action is required to gain control of the scenario following the start of HPI and AFW. Discussions with plant personnel indicated their agreement that some operator action is required. The emergency procedure guideline for this event instructs the operator to reduce pressure and terminate HPI flow. It does not imply that this is required to prevent core melt, but rather is intended to reduce the release of primary coolant (and thus, radioactivity) through the secondary. The reviewers, however, consider this action to be ultimately required to prevent core melt due to pumping the entire contents of the RWST out of the containment. A new operator action has been defined to cover this case as described below.

- Operator Action OA-10, SGTR - Control HPI Flow (when both HPI and AFW are available): The operator takes manual control of the HPI flow, throttling it down to reduce the primary pressure to below the secondary pressure. When primary pressure is below secondary pressure, HPI is terminated. We estimate that this action is required in the time frame of approximately 19 hours, based on the results of MARCH calculations for small LOCA events provided by Northeast Utilities. Precision is not required for the 19-hour estimate because the numerical results are essentially insensitive to any change within plus or minus five hours.

The SGTR tree shown in Fig. 3.2-5 has been modified to include this action.

3.2.2.3 Large LOCA

The PSS assumes that high pressure injection (HPI) is sufficient to provide coolant injection for the large LOCA event. Previous PRAs have usually assumed that the HPI system is not capable of supplying this function for large breaks. Part of the reason is that these systems are usually not sized to provide the amounts of flow required to replenish the coolant lost during large LOCAs. This, however, is only a secondary concern. The major concern is that the HPI pumps are designed to provide flow against relatively high pressure. They utilize a great deal of power to produce the required head. When a pump of this type pumps against minimal or no head, as is the case for a large LOCA, the power which usually goes to overcoming the pressure at the pump discharge is converted to greatly increased flow. In this case, the tendency is for the pump speed to increase, due to the decreased resistance, beyond the point at which the pump is still capable of drawing sufficient amounts of water through the suction lines. At this point, pump cavitation could occur and the pump could trip on low suction pressure or overspeed. If pump trips are not provided, as is the case at Millstone, the pumps could be destroyed. In either case, the pumps would not be able to provide coolant to the RCS. There is no reason to believe that the Millstone pumps are immune to this phenomenon, and the assumption that HPI could supply injection during large LOCAs is not justified. The event tree shown in Fig. 3.2-1 has been modified to reflect this judgment.

In addition, the original event tree showed a decision point for event R-1, low pressure recirculation cooling in sequences where no injection cooling was available. Due to the design of this plant, it is possible for this to occur. However, this does not change the outcome of the event, as seen on the tree. Regardless of the state of R-1, an early core melt still occurs. Although the presence of this decision point on the tree does not impact the study's results, it has been removed from our modified tree because it is meaningless.

3.2.2.4 Spurious Safety Injection

The use of operator action OA-7, primary bleed and feed, is incorrect on this tree. While bleed and feed cooling is valid for this event, OA-7 includes the unavailability of HPI in its unavailability value. The initiating event itself implies that HPI is already operating. Further, the other events on the tree, such as OA-6, assume that HPI is already operating. Thus, the proper event to use on the tree would be operator action OA-3, primary bleed. This would serve to establish bleed and feed cooling. The modified event tree is shown in Fig. 3.2-10.

3.2.2.5 Anticipated Transients Without Scram (ATWS)

We have reviewed the PSS analysis of ATWS within the context of the recently released NRC ATWS rule (Federal Register Notice SECY-83-293, Memo from J. M. Fenton to S. J. Chilk, 12/8/83) (Ref. 3.2-3). We have found a number of areas which we felt were improperly treated in the PSS and felt it was necessary to construct a new ATWS event tree, which is shown in Fig. 3.2-11. The justification for our version of the ATWS tree is discussed in the remainder of this section.

The PSS took credit for operator action to manually trip the reactor if the automatic trip failed. We believe it is valid to consider this type of recovery, but disagree with the PSS assumption that it can be applied to all RPS failures. We believe that this recovery action can only be applied to electrical failures. Thus, we have divided RPS failures into electrical and mechanical as in the NRC ATWS Rule (2E-5 and 1E-5 failure probability, respectively), with one difference: the Rule defined electrical failures as including failures of the breakers, and we have defined electrical failures as failure to produce a trip signal at the breakers. This is based on the detailed analysis of a Westinghouse RPS system contained in the Ringhals PRA (Refs. 3.2-4 and 3.2-5), which is the most detailed probabilistic fault tree analysis of a Westinghouse RPS known to us. The analysis shows that the total RPS failure probability is about 3E-5 per demand and that about one-third of this quantity is due to potentially non-recoverable (in the short term) common mode breaker faults (mechanical) and the remainder consists of recoverable (by manual scram) electrical signal faults, often combined with test outages (also recovered by manual scram). Common mode control rod and drive failures did not contribute. Since this analysis is much more detailed that the one contained in the ATWS Rule or the PSS, we have used the results (Ref. 3-25,a) and applied the operator recovery event RT3 to the electrical failures only.

We then considered the occurrence of turbine trip as was done in the PSS. This was used to determine two things: the probability that very high pressure resulting in core melt would occur and whether there would be additional stress on the primary relief and safety valves. The PSS considered that the probability of extremely high pressure (represented by the event PL, which the ATWS rule refers to as event MTC) was the same for all cases. The NRC rule concluded that this was dependent on the occurrence of turbine trip. We believe that the NRC position is more reasonable, and thus have used their position and values for this event (0.01 with turbine trip, 0.1 without turbine trip). The PSS also assumed that even when this extreme overpressure occurred, it was still possible to prevent core melt. The NRC rule concluded that whenever extreme overpressure occurred, defined as exceeding Service Level C, core melt would result. While this is likely to be conservative, the uncertainty of RCS performance at these pressures leads us to conclude that this is the most reasonable assumption to make at this time. Thus, all sequences on our tree where PL fails are core melt sequences. We have also assumed that MP 3 will have a diverse turbine trip (independent of RPS).

The PSS also assumes that it is possible, depending on plant conditions, to mitigate an ATWS with either auxiliary feedwater or high-pressure injection. In sequences where auxiliary feedwater succeeds, the PSS simply ends the event with success. In the sequences where the initial power level is less than 25% or the moderator temperature coefficient is more negative than -5pcm/°F, and auxiliary feedwater is unavailable, the PSS assumes that it is possible to effect reactor shutdown and cooling by using emergency boration with PORVs locked open. This would provide boration to shut down the reactor simultaneously with bleed and feed cooling. This method has not been considered in other PRAs, and appears questionable since we wonder how much coolant can be pumped in under the conditions which would be present and how long it would take to effect the shutdown. This assumption takes an inordinately large amount of credit for the ability of HPI to provide flow at reactor pressure. It would seem that at best only the charging pumps would be capable of pumping anything at all, as the pressure should be too high for the safety injection pumps. Also, there would be much greater amounts of heat to be removed through the PORVs with makeup flow than for a normal bleed and feed scenario. It is not clear how this heat can be removed and the reactor shut down under these conditions without assistance from the auxiliary feedwater system. The NRC rule states that both auxiliary feedwater and HPI are always required. It is our feeling that the NRC rule is again more realistic, since in all cases HPI/emergency boration will eventually be required to effect reactor shutdown, although this will not be required for a long time period unless there is a LOCA. Thus, our tree reflects the need for both systems to mitigate an ATWS (events AF1 and OA8).

It was previously mentioned that the failure of turbine trip would affect the stress on the primary relief and safety valves. This is dealt with by using the PSS event PR for those sequences where turbine trip fails and extreme pressure does not occur (event PL succeeds). This event changes the time frame for the need for HPI (event OA8). As discussed above, OA8 is normally not required for a long time period (>60 minutes is a sufficient definition for the purpose of quantifying the operator error probability). However, if a LOCA is present this time frame would be shortened to on the order of 20 minutes since a constant coolant loss would be taking place. Event OA8R represents this shortened time frame on the event tree. It is important to note that no mention was made of small LOCAs resulting from relief valve failures when this additional stress is not present, i.e., resulting from the normal opening of the valves at the start of the event. That is because the PSS deals with this cause of LOCA directly on each initiator event tree prior to considering ATWS, and then branches to the small LOCA event tree where ATWS is considered to be a core melt. This conservative assumption has no effect on the results and thus we determined that it would not be necessary to modify it.

The remaining events in our tree are concerned with long-term cooling. They are modeled in the same way as other trees depending on whether the sequence resembles a transient or a LOCA. This is because once the initial phase of an ATWS is over, the remainder of the sequence behaves like any other accident. The completed tree is shown in Fig. 3.2-11.

3.2.2.6 Summary of Assumptions for ATWS Event Tree

(1) RT3 operator recovery only applied to electrical RPS failures.

(2) Turbine trip success/failure determines probability of extreme overpressure.

(3) Extreme overpressure leads to core melt (ATWS rule).

(4) Turbine trip failure causes additional stress on primary relief valves (need to consider event PR-S2).

(5) HPI is always eventually required (ATWS rule) (event OA8 is HPI/emergency boration).

(6) If no LOCA (PR-S2 not considered or PR-S2 success) need for HPI is long term (>60 minutes). If LOCA, need for HPI is short term (~20 minutes).

(7) HPR required for LOCA only.

3.2.3 Issues of Importance to the NRC

In their instructions for this review, the NRC listed certain issues which were of concern to them. They wanted to know how these issues were treated in the PSS. This section discusses the issues which affect the event tree analysis.

3.2.3.1 Reactor Coolant Pump Seal Failure During Station Blackout

The reactor coolant pump seal failure is an imporant contributor to core damage. While the method for treating this event in the PSS is considered satisfactory, some of the input values used are considered completely unjustified.

This event is explicitly considered on the loss of offsite power event tree for support state seven. It is included in the frequency of consequential S2 LOCA and the failure probability has different values related to the length of the blackout: for less than one hour P(S2) = 0.0858, from one to two hours P(SW) = 0.164, and for greater than two hours P(S2) = 1.0.[a] In the PSS section on recovery, credit is taken for the capability of the seals to hold out even longer, such that the probability of core uncovery in under 6.5 hours is only 2% [P(S2) = 0.02]. The PSS obtained the initial values by applying the standard exponential failure rate equation, using a failure rate obtained from a Westinghouse internal letter. This information was not available to us, but the results obtained contradict the present NRC position on RCP seal failures, which is that Westinghouse tests performed through June 1983 have failed to confirm the ability of the seals to survive, although they agree that there is insufficient information for a final judgment. The method utilized in the PSS to justify the 6.5-hour number appears inappropriate and arbitrary. It is stated in the PSS that eight incidents of loss-of-seal-cooling ranging in duration from 2 minutes to 65 minutes have occurred at operating nuclear plants without a seal failure. This is said to represent 66 O-ring hours without a failure. They also include tests on mainloop stop valve O-rings, which they say are sufficiently similar, to bring the total to 186 O-ring hours without failure.

This treatment is considered to be completely unjustified. First, the inclusion of the stop valve O-ring experience is unfounded. These O-rings and their application are similar only in that they see the same temperature and pressure and are nominally of the same material. This is insufficient justification for including them in the data base. Second, describing the RCP O-ring data as "66 hours without a failure" is simply wrong. This implies that data for three O-rings without cooling for one hour each is the same as data for one O-ring without cooling for three hours. This treatment is then used to justify a distribution which will be used to quantify failure of O-rings due to continuous loss of cooling. Since the whole problem of seal failure is based on continued exposure to heat and pressure without cooling, this type of analysis cannot be used. The fact is, no seal has survived such exposure for longer than 65 minutes without failure, and there is no reason to believe that it is possible for a seal to survive for as long as two hours without failure. The probability of seal failure in the one- to two-hour time frame should be considered as certainty [P(S2) = 1.0]. Thus, a LOCA will occur if offsite power is not recovered after one hour without cooling. However, it is believed justified that core melt can be averted if power is recovered and HPI restored within two hours. This essentially eliminates sequence 11 on the loss-of-offsite power (support state 7) event tree (see Fig. 3.2-9) since its probability goes to zero. This leaves the problem of determining a value to use for the probability of seal failure in the first hour. Utilizing the Chi-squared zero failure technique used in IREP (see e.g., Millstone 1 IREP, NUREG/CR-3085, Chapter 4) (Ref. 3.2-6), it can be

[a] The PSS calculated other numbers in addition to these, including a probability for the time period out to four hours. However, the values shown here were actually used in the initial quantification.

stated that the value lies somewhere between the zero failure value based on eight trials (the number of loss of cooling events) and the value based on one trial (the number of events actually lasting one hour). These values are:

$$P[S2(8)] = [(1/8)*1.386]/2 = 0.09$$
$$\text{and, } P[S2(1)] = [(1/1)*1.386]/2 = 0.7 \qquad (3\text{-}3)$$

For the purpose of the simplified requantification contained in this review, a simple average of these two numbers is taken to represent a reasonable approximation of the probability of seal failure in the first hour of loss of cooling, i.e., P(S2) = 0.4.

One additional modification to the event tree is required due to the consideration of RCP LOCA. The long-term blackout sequences numbered 21 through 23 should result in plant damage states SEC, SEC', and SE rather than TEC, TEC', and TE, as shown in the PSS. In these sequences, secondary cooling is available and the RCS is initially intact, which would normally result in a success sequence. Core melt results only because the extended blackout causes an RCP seal LOCA, so that the small LOCA plant damage states are appropriate. The similar sequences numbered 43 through 48 remain assigned to the transient plant damage states because core melt in these sequences results from the lack of secondary cooling, regardless of the eventual occurrence of an RCP seal LOCA.

3.2.3.2 Depletion of DC Batteries During Station Blackout

This event is included implicitly in the loss of offsite power event tree for support state 7. For events where the blackout lasts longer than two hours, a core melt is assumed. However, recovery of quench spray is considered as a means to reducing consequences. This recovery is limited to the time period from two to eight hours, which corresponds to the estimated eight hour lifetime of DC batteries. Limiting the recovery of quench spray to eight-hours therefore implicitly deals with the depletion of DC batteries in that time frame.

The NRC has voiced concern that, absent additional information from the applicant, the appropriate battery lifetime to use in the review requantification should be two to three hours, based on licensing criteria and analysis. This position is considered to be excessively conservative, especially in view of the five-hour time used in NUREG/CR-3226 (Ref. 3.2-7). The detailed assessment performed in NUREG/CR-3226 included surveys and interviews of a number of utilities, and reviews and analyses of LERs and other relevant documentation. Battery lifetimes for all plants included in this review ranged from 2 to 16 hours. A large majority had a four- to six-hour range, and most of these were clustered around five to six hours. The long lifetimes resulted from detailed analyses which used realistic loads and took credit for the operator following a procedure to accomplish load shedding. The very short (two-hour) lifetimes took no credit for load shedding, and they tended to occur in older plants with undersized batteries. This information provided the basis for selecting five hours as a reasonable estimate for battery life. It was supported by a sensitivity analysis that showed battery lifetimes as short as 2 hours or as long as 12 hours generally had very little effect on core melt frequency. In addition, the operator has at least one hour to perform load shedding and thereby significantly extend battery lifetime, so that credit for this action is appropriate. If we were to use the NREP cognitive error model for this time period, the probability of early battery failure due to operator failure to shed load is 0.001, while the probability of late battery failure is 0.999. Each of these arguments provides additional support to the conclusion that the eight-hour battery lifetime used in the PSS is a more reasonable value than two to three hours.

3.2.3.3 Pressurized Thermal Shock (PSS)

The PSS does not deal explicitly with the issue of pressurized thermal shock, although sequences resulting in this event are included in the event trees. For example, sequence 2 on the spurious safety injection and steamline break (inside and outside containment) trees, where the operator fails to control HPI (OA-6), are pressurized thermal shock events. The PSS considers these sequences to be "success" and does not carry the analysis any further. Since the sequences exist, it is possible to calculate the frequency of PTS from these trees. However, the probability of core melt given PTS is not straightforward and is not described in the PSS. It is beyond the scope of this review to attempt to determine this probability, so that only the frequency of PTS events can be determined from the PSS and not the frequency of PTS-induced core melt.

3.2.3.4 Steam Generator Tube Rupture (SGTR) With Stuck Open Secondary Steam Relief Valves (SRVs)

This event is modeled directly on the SGTR event tree as the steam leak event. It explicitly models instances where the occurrence of a steam leak precludes preventing core melt. Also, in sequences where a core melt would occur regardless of the presence of a steam leak, the tree differentiates in the plant damage state. A core melt in conjunction with a steam leak will always result in an interfacing systems LOCA plant damage state, whereas without a steam leak, the result will be either a transient or small LOCA plant damage state.

3.2.3.5 Anticipated Transients Without Scram (ATWS)

The analysis of ATWS is handled explicitly on its own event tree as a consequential event following each of the initiator classes. Each of the event trees for the various initiators has a branch for failure to scram which transfers to the ATWS tree.

3.2.3.6 Stuck Open Primary Safety/Relief Valve (S/RV)

The stuck open S/RV is dealt with explicitly on each non-LOCA event tree. It is included in the frequency calculation of consequential S2 LOCA and results in a transfer to the small LOCA event tree whenever this branch occurs. The PSS uses a value of 3E-5 for the occurrence of this event. This value is based on three factors: (1) that the valves are demanded, (2) that at least one valve sticks open, and (3) that the operator fails to recover by closing the appropiate PORV block valve. The values used for these parameters have been reviewed and found to be reasonable; thus the ultimate value used is valid except for ATWS and total loss of all feedwater. In this situation, the only way to prevent core melt is to utilize feed and bleed, which would require the PORVs to be open anyway. The treatment of ATWS pressure relief on the ATWS tree, while being somewhat out of sequence, adequately represents the overall scenario of concern and thus no overall improvement on the answer would be attained through further modifications to the tree.

3.2.4 References for Section 3.2

3.2-1 C. M. Thompson et al., Westinghouse Electric Corporation, "Inadequate Core Cooling Studies of Scenarios with Feedwater Available," Westinghouse Report WCAP-9754, June 1980.

3.2-2 W. Tauche, Westinghouse Electric Corporation, "Loss of Feedwater Induced Loss of Coolant Accident Analysis Report," Westinghouse Report WCAP-9744, May 1980.

3.2-3 SECY-83-293, J. M. Felton to S. J. Chilk, 10CFR50, "Reduction of Risk from Anticipated Transients Without Scram (ATWS) Events for Light-Water-Cooled Nuclear Power Plants," December 1983.

3.2-4 NUS Corporation, "Ringhals Unit 2 Probabilistic Safety Study."

3.2-5 P. J. Amico "Fault Tree Analysis of Westinghouse Solid State Protection System Scram Reliability", *Proceedings of the International Meeting on Thermal Nuclear Reactor Safety*, September 1984.

3.2-6 P. J. Amico et al., Science Applications, Inc., "Interim Reliability Evaluation Program: Analysis of the Millstone Point Unit 1 Nuclear Power Plant," USNRC Report NUREG/CR-3085, February 1983.

3.2-7 A. M. Kolaczkowski et al., Sandia National Laboratories, "Station Blackout Accident Analysis (part of NRC Task action Plan A-44)," USNRC Report NUREG/CR-3226, May 1983.

3.3 Success Criteria

The success criteria used in the PSS for the functions of emergency core cooling early, emergency core cooling late, and containment heat removal are shown in Table 3.3-1. Review of these criteria determined that they are, for the most part, reasonable. Where criteria used differed from criteria used in the past for similar reactors, examination of the bases of the criteria was undertaken to determine if they were valid. Some of these were discussed in the section on event trees (Section 3.2). A summary of our findings for each function evaluated is discussed below.

3.3.1 Emergency Core Cooling Early

3.3.1.1 High Pressure Injection During Large LOCA events

The PSS assumes that HPI can be utilized for this function during large LOCA events. This is not consistent with previous PRAs and it is not considered justified for the reasons discussed in Section 3.2.2.3.

3.3.1.2 High Pressure Injection During Medium LOCAs

The PSS assumes that any one-out-of-four HPSI pumps are capable of providing this function during medium LOCA events. Previous PRAs for plants of this type have assumed that one-out-of-two charging pumps AND one-out-of-two safety injection pumps are required for this function, based on analysis provided in plant FSARs. Plant-specific calculations performed by Westinghouse and documented in calculation number CN-PRA-83-022 (Ref. 3.3-1) determined that any one-out-of-four pumps is sufficient. The calculation appears to be reasonable in removing excess conservatisms in the analysis codes used for FSAR calculations. The PSS assumption is therefore considered reasonable and acceptable.

3.3.1.3 High Pressure Injection During Small LOCAs

The PSS assumes that any one-out-of-four HPSI pumps are capable of providing this function during small LOCA events. Based on the discussion above, it seems reasonable on the surface that if this is true of the medium break, it should also be true of the small break. However, this does not account for the slower pressure drop for these breaks, which may keep the RCS pressure above the safety injection pump shutoff head. The PSS alludes to this by mentioning that for some small breaks the operator may have to depressurize using a PORV if only a safety injection pump is available. However, the PSS does not deal with this problem. In order to remove this optimistic assumption, it has been assumed that one-out-of-two charging pumps is sufficient but that one-out-of-two safety injection pumps is valid only in combination with one-out-of-two PORVs.

3.3.1.4 Secondary Depressurization and Low Pressure Injection

On Table 3.3.1 for medium LOCA, small LOCA, and incore instrument tube rupture events, success criteria (b), (c), and (c), respectively, refer to the use of secondary depressurization to reduce primary pressure. This is intended to allow the use of low pressure injection cooling in sequences that would otherwise require high pressure injection. Although inconsistent with previous PRAs, these criteria are based on improved analysis and appear to be reasonable. Our reasoning is discussed in Section 3.2.1.2.

3.3.1.5 Bleed and Feed Cooling

The PSS assumes that bleed and feed cooling can be utilized for small LOCAs, incore instrument tube rupture, steam generator tube rupture, steamline breaks, and transients. This is represented by criterion (b) on Table 3.3-1 for each of these initiators. The success criteria presented appear to be reasonable. Our reasoning is discussed in Section 3.2.1.5.

3.3.1.6 Primary Depressurization for Steam Generator Tube Rupture

Success criteria (c) and (d) on Table 3.3-1 for the SGTR initiator represent the PSS assumption that it is possible to depressurize the primary rapidly enough during this event to terminate break flow prior to core uncovery. This allows the use of auxiliary feedwater alone to provide the required core cooling. This scenario has not been credited in previous PRAs, but there is sufficient justification to accept the success criteria presented. Our reasoning is discussed in Section 3.2.2.2.

3.3.1.7 Main Steam Isolation During Steamline Breaks

The PSS assumes that main steam isolation is required during steamline break events in order for auxiliary feedwater to function. This assumption is conservative for the reasons discussed in Section 3.2.2.1. Isolation is not required.

3.3.1.8 Power Conversion System During Transients

The PSS assumes that the power conversion system is never available to provide cooling during transients. This assumption is conservative for the reasons discussed in Section 3.2.1.3. The PCS should be included as a valid success criteria.

3.3.2 Emergency Core Cooling Late

The success criteria for this function are reasonable and consistent with the plant FSAR and the corresponding early cooling success criteria, with one exception. The PSS assumes that it is possible to avoid recirculation for small LOCAs and incore instrument tube ruptures by conserving RWST inventory. This is represented on Table 3.3-2 by late success criteria (a) and (c), respectively. These criteria allow late cooling to be provided by injection in the same manner as early cooling. This criteria are considered unjustified for the reasons discussed in Section 3.2.1.6.

3.3.3 Containment Heat Removal

The success criteria for this function is reasonable and consistent with the plant FSAR and previous PRAs.

3.3.4 Revised Success Criteria

The revised success criteria shown in Table 3.3.2 are based on the discussions above. These criteria are used for the requantification of the dominant core melt sequences.

3.3.5 References for Section 3.3

3.3-1 Westinghouse Electric Corporation, "Millstone Unit 3 Plant Specific Transient Analysis," Westinghouse Report CN-PRA-83-022, March 1983.

Table 3.3-1 Millstone 3 PSS functional success criteria.

Initiator	Emergency core cooling early	Emergency core cooling late	Containment heat removal
Large LOCA	(a) 1/2 LPSI + 3/3 ACC or (b) 2/4 HPSI + 3/3 ACC	(a) 1/2 LPSR	1/2 CSR (core melt only)
Medium LOCA	(a) 1/4 HPSI + 3/3 ACC or (b) 1/3 AFWS + SSR + 1/2 LPSI + 3/3 ACC	(a) 1/2 HPSR or (b) 1/3 AFWS + SSR + 1/2 LPSR	same
Small LOCA	(a) 1/4 HPSI + 1/3 AFWS or (b) 1/4 HPSI + 2/2 PORV or (c) 1/3 AFWS + SSR + 1/2 LPSI	(a) 1/4 HPSI + AFWS + SSR or (b) 1/2 HPSR or (c) 1/3 AFWS + SSR + 1/2 LPSR	Same
SGTR	(a) 1/4 HPSI + 1/3 AFWS or (b) 1/4 HPSI + 2/2 PORV or (c) 1/3 AFWS + SSR or (d) 1/3 AFWS + 1/2 PORV	(a) 1/3 AFWS or (b) 1/2 HPSR	Same
Incore instrument Tube rupture	(a) 1/4 HPSI + 1/3 AFWS or (b) 1/4 HPSI + 2/2 PORV or (c) 1/3 AFWS + SSR + 1/2 LPSI	(a) 12 QS + 1/2 HPSR or (b) 1/2 QS + 1/3 AFWS + SSR + 1/2 LPSR or (c) 1/4 HSPI + 1/3 AFWS + SSR	Same
Steamline breaks	(a) 1/3 AFWS + MSI or (b) 1/4 HPSI + 2/2 PORV	(a) 1/3 AFWS or (b) 1/2 HPSR	Same
Transients	(a) 1/3 AFWS or (b) 1/4 HPSI + 2/2 PORV	(a) 1/3 AFWS or (b) 1/2 HPSR	Same

Table 3.3-2 Revised Millstone 3 PSS functional success criteria.

Initiator	Emergency core cooling early	Emergency core cooling late	Containment heat removal
Large LOCA	(a) 1/2 LPSI + 3/3 ACC	(a) 1/2 LPSR	1/2 CSR (core melt only)
Medium LOCA	(a) 1/4 HPSI + 3/3 ACC or (b) 1/3 AFWS + SSR + 1/2 LPSI + 3/3 ACC	(a) 1/2 HPSR or (b) 1/3 AFWS + SSR + 1/2 LPSR	same
Small LOCA	(a) 1/2 CP + 1/3 AFWS or (b) 1/2 SIP + 1/2 PORV + 1/3 AFWS or (c) 1/4 HPSI + 2/2 PORV or (d) 1/3 AFWS + SSR + 1/2 LPSI	(a) 1/2 HPSI or 1/2 HPSR or (c) 1/3 AFWS + SSR + 1/2 LPSR	Same
SGTR	(a) 1/4 HPSI + 1/3 AFWS or (b) 1/4 HPSI + 2/2 PORV or (c) 1/3 AFWS + SSR or (d) 1/3 AFWS + 1/2 PORV	(a) 1/3 AFWS or (b) 1/2 HPSR or	Same
Incore instrument Tube rupture	(a) 1/4 HPSI + 1/3 AFWS or (b) 1/4 HPSI + 2/2 PORV or (c) 1/3 AFWS + SSR + 1/2 LPSI	(a) 12 QS + 1/2 HPSR or (b) 1/2 QS + 1/3 AFWS + SSR + 1/2 LPSR	Same
Steamline breaks	(a) 1/3 AFWS or (b) 1/4 HPSI + 2/2 PORV	(a) 1/3 AFWS or (b) 1/2 HPSR	Same
Transients	(a) 1/3 AFWS or (b) 1/4 HPSI + 2/2 PORV or (c) PCS	(a) 1/3 AFWS or (b) 1/2 HPSR or (c) PCS	Same

3.4 Systems

This section provides the results of our review of system descriptions and system fault trees in the Millstone 3 PSS. The systems descriptions were reviewed with regard to whether the information provided enabled us to verify the fault tree analysis and system success criteria. The fault trees were reviewed with regard to their accuracy, validity, and completeness in quantifying accident sequences.

There are 16 systems for which fault trees were used in the Millstone 3 PSS. A list of these systems and the system failure probabilities for the total system and redundant trains within the system under support state 1 are provided in Table 3.4-1. the systems were quantified for eight different support states. These support states are defined in Table 3.4-2 and discussed in Section 3.10.2. The fault trees and descriptions of associated systems were provided in Volumes 4 and 5 (Section 2.3) of the PSS. The fault tree for the vital DC system was included in Appendix 1-E of Volume 1.

Our review concentrates on those systems that provided important support functions and those system that were involved in high risk accident sequences. In this regard, the following systems were found to be of particular importance:

- main electrical
- vital AC
- ESF actuation
- emergency generator load sequencer
- auxiliary feedwater
- quench spray
- service water

A system-specific review is provided in each of the 16 subsections below. These subsections are divided into three parts. The first part provides a system description based on the system descriptions in the PSS and the Millstone 3 FSAR. The second part discusses the system fault tree in light of the system description. Particular attention is given to the treatment of test and maintenance, human errors, and common-cause failures.

Our evaluation in this part also considers consistency among the fault tree components, the top event, and the system success criteria. The last part of each subsection provides our conclusions and comments on the system fault tree with regard to accuracy, validity, and completeness.

The system success criteria and the top event definition of each fault tree were generally consistent. The effects of test and maintenance, human error, and common-cause were included in almost all of the fault trees.

A few potentially significant problems and several minor ones were identified during the review of the system fault trees for accuracy, validity, and

Table 3.4-1 Results of the system fault tree analysis.

	System	Unavailability[a]
1.	Main electrical	4.56E-4
2.	120VAC	8.43E-5 (per bus)
3.	ESF actuation	1.17E-3 (per signal per train)
4.	Load sequencer (EGLS)	1.59E-5 (per signal, both trains)
5.	Auxiliary feedwater	6.80E-5
6.	High pressure injection	5.87E-5 (for small and medium LOCAs)
7.	Low pressure injection	1.74E-4
8.	Main steam isolation	8.197E-4[b], 1.5E-5[c]
9.	Quench spray	3.2E-4
10.	Safety injection pump cooling	7.32E-3 (per train)
11.	Charging pump cooling	5.32E-4
12.	Low pressure recirculation	3.0E-3
13.	High pressure recirculation	5.85E-3
14.	Containment recirculation spray	2.0E-3
15.	Service water	7.44E-6[d]
16.	Vital DC	1.4E-8/yr[e]

[a] These values are taken from the PSS. All values are failure on demand (except 16).
[b] For steamline breaks inside containment.
[c] For steamline breaks outside containment.
[d] Loss of system function within 24 hours.
[e] Loss of system function for a continuous 24 hour period.

Table 3.4-2 Support state definitions

System	Unavailability
(1)	All support systems available
(2)	One support train unavailable
(3)	Both support trains Unavailable
(4)	All ESF signals unavailable
(5)	LOSP, all support systems available
(6)	LOSP, one support train unavailable
(7)	LOSP, both support trains unavailable
(8)	LOSP, all ESF signals unavailable

completeness. The minor ones would not contribute more than a few percent error to the overall frequency of core melt, so the reader is referred to individual subsections for a discussion of the minor problems. The potentially significant errors are taken up in the paragraph below.

An important dependence of the vital AC, main electrical system, and emergency generator load sequencer on the vital DC system was not included in the corresponding fault trees. In the event of a loss of offsite power, the vital AC system would initially be dependent upon the batteries in the vital DC system. This is an apparently critical dependence because the emergency diesels cannot transmit power to the emergency bus unless the load sequencer is operating, but the sequencer requires vital AC to function. The real difficulty occurs in the individual fault trees for the vital AC and vital DC system. The unavailability of each system is calculated assuming that AC power is available on the emergency bus. This makes the results invalid for those cases when no power is available on the emergency bus. Thus, the PSS provides no estimate of the unavailability of the vital AC and vital DC systems, on demand, for those cases in which offsite power is unavailable. Yet, such a case is precisely when the unavailability of these systems is extremely important. The significance of this problem increases in light of the fact that loss-of-offsite-power-initiated sequences are dominant contributors to important plant damage states. This issue is taken up in more detail in Subsections 3.4.1, 3.4.2, 3.4.4 and 3.4.16 below.

Quantification of system failure with fault trees depends directly on the use and application of component failure data. The review of the validity of the Millstone 3 PSS failure data is discussed in Section 3.5.

3.4.1 Main Electrical System

3.4.1.1 System Description

The main electrical system is designed to provide a reliable source of power to the normal and emergency AC power systems. The normal AC power system supplies power to non-safety-related equipment that is necessary to support the plant's power operation under normal conditions. During off-normal conditions the emergency power system is designed to provide power to safety systems that are required for plant shutdown and mitigation of postulated accidents.

The PSS and the FSAR indicate that the main generator provides power to the electrical system through the two normal station service transformers (NSSTs) during normal plant operation. The NSSTs are the preferred sources of station service power, and NSST "A" supplies power to the 4160V emergency buses via the normal buses 34A and 34B. If the preferred source of offsite power is lost, the system makes an automatic transfer to the two reserve station service transformers (RSSTs). RSST "A" provides power directly to the emergency buses 34C and 34D from an alternate offsite source.

If both sources of offsite power are unavailable, the emergency AC power system provides power directly to both emergency buses 34C and 34D. This system consists of two diesel generators, each of which is dedicated to one emergency bus and is capable of providing all engineered safety feature equipment and essential shutdown loads on that bus.

A diagram of the main electrical system showing the link between the off-line and on-line portions of the emergency AC system is provided in Fig. 3.4.1-1.

3.4.1.2 System Fault Tree

The fault tree for the main electrical system was used to model the unavailability of power on emergency buses 34C and 34D. The structure of event trees and support states in the Millstone PSS requires that the unavailability of the main electrical system be modeled for three cases. Case 1 models the unavailability of power on both buses (34C and 34D) when loss-of-offsite-power is the initiating event. Case 2 models random failures on a single bus that could lead to bus failure. The case 2 model forms part of the input to the case 1 model. The case 2 model is also used to calculate the unavailability of the emergency bus in other fault trees and in the support state model. Case 3 is used to model unavailability of all AC power for an initiating event other than loss-of-offsite-power. The probability of no power on buses 34C and 34D is calculated using both the probability of bus failures and the probability of losing offsite power within 24 hours of a postulated accident. Figure 3.4.1-2, which is taken directly from the Millstone PSS, was used to calculate the unavailability of offsite power. Figure 3.4.1-3 shows a substantially reduced form of the Millstone PSS fault tree used to calculate the unavailability of AC power on a single AC emergency bus. The circuit breaker referred to in this tree is the large breaker between the emergency generator and the emergency bus. The PSS fault tree for this component is extremely detailed. Figure 3.4.1-4 provides a simplified fault tree for the main electrical system and shows the relative positions of each of the three cases in the system logic.

Table 3.4.1-1 provides a summary of the system unavailability that was obtained in the PSS for each case and the dominant cut sets in each case. For case 1, common-cause failure of both emergency diesel generators is the dominant contributor, contributing 53% to total unavailability. The remainder of the unavailability is contributed by combinations of random failures in the emergency electrical equipment. However, none of these cut sets contributes more than 1% each. The dominant cut set for case 2 is the failure of a diesel generator to start and run, contributing 16% to the total. The next most significant cut set for this case involves mechanical failure of the circuit breaker and contributes about 2.4%; however, the sum of all cut sets involving circuit breaker failures contributes 82% to total unavailability. Remaining cut sets contribute no more than 1% each. The dominant contribution to unavailability for case 3 is loss of offsite power combined with common-cause failure of both diesel generators. This cut set contributes 57% of the total unavailability. No other cut set contributes more than 1%.

According to the Millstone PSS, the only significant common-cause contribution to electrical system failure is that associated with the diesel generators. All other components such as wiring, circuit breakers, protective relays, etc., were determined to have common-cause failure rates that were negligible when compared to their random failure rate. This was determined by examining common-cause failures for components with and without aggregate control circuit failures. Common-cause calculations for diesel generators assume a binomial failure rate model.

Table 3.4.1-1 Dominant cut sets for failure of the main electrical system.

Dominant cut set		Unavailability (per demand)
Case 1: Both emergency buses unavailable[a]		
Common cause		2.6E-4
Random failures		1.96E-4
	Total	4.56E-4
Case 2: One emergency bus unavailable[a]		
Diesel generator failure		2.33E-3
Circuit breaker failures		1.15E-2
	Total	1.4E-2
Case 3: No AC power available on either emergency bus[b]		
Loss of offsite power combined with common-cause failure of both diesel generators		7.80E-8
Other failures		5.90E-8
	Total	1.37E-7

[a] For a mission time of 24 hours, given loss of offsite power as an initiating event (without consideration of recovery of offsite power).

[b] For a mission time of 24 hours, given offsite power initially available.

The Millstone PSS found no credible human errors that could lead to component unavailability in the main electrical system. The stated reason for this was that aside from the emergency generators, the electrical system is in continuous use and thus not subjected to any formal tests. Each diesel generator and its associated control circuitry is tested monthly on a staggered basis. Operational tests are performed during refueling shutdown. No maintenance is scheduled for the electrical system during normal operation. Nonetheless, unscheduled maintenance on the diesel generators as a result of periodic testing is included in the calculation of their unavailability.

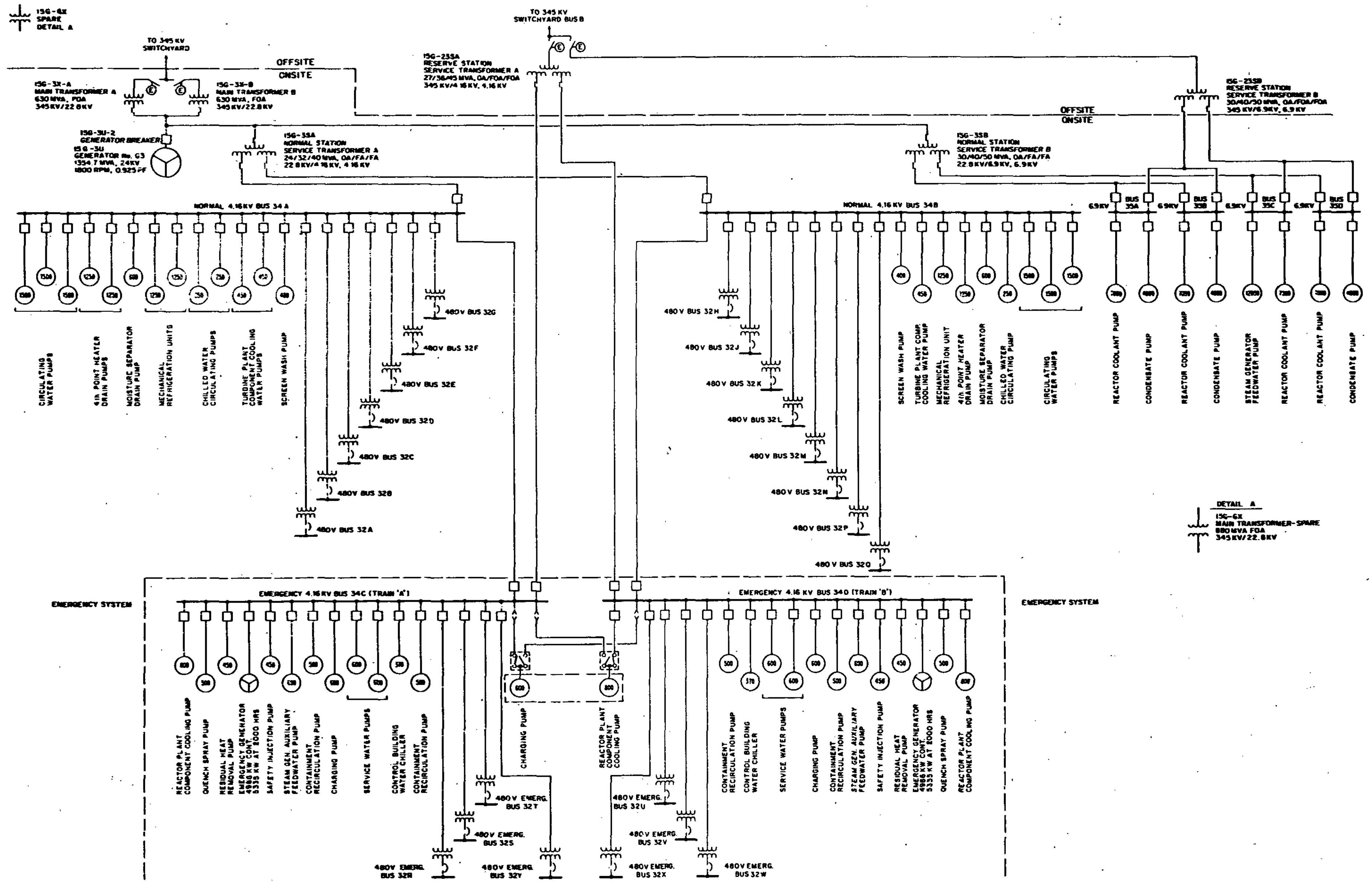

15G-6X SPARE DETAIL A
TO 345 KV SWITCHYARD
OFFSITE
ONSITE
15G-3X-A MAIN TRANSFORMER A 630 MVA, FOA 345KV/22.8KV
15G-3X-B MAIN TRANSFORMER B 630 MVA, FOA 345KV/22.8KV
15G-3U-2 GENERATOR BREAKER
15G-3U GENERATOR No. G3 1354.7 MVA, 24KV 1800 RPM, 0.925 PF
TO 345 KV SWITCHYARD BUS B
15G-23SA RESERVE STATION SERVICE TRANSFORMER A 27/36/45 MVA, OA/FOA/FOA 345 KV/4.16 KV, 4.16 KV
15G-3SA NORMAL STATION SERVICE TRANSFORMER A 24/32/40 MVA, OA/FA/FA 22.8KV/4.16KV, 4.16 KV
15G-3SB NORMAL STATION SERVICE TRANSFORMER B 30/40/50 MVA, OA/FA/FA 22.8KV/6.9KV, 6.9KV
15G-23SB RESERVE STATION SERVICE TRANSFORMER B 30/40/50 MVA, OA/FOA/FOA 345 KV/6.9KV, 6.9 KV
OFFSITE
ONSITE
NORMAL 4.16KV BUS 34 A
NORMAL 4.16 KV BUS 34B
6.9KV BUS 35A
6.9KV BUS 35B
6.9KV BUS 35C
6.9KV BUS 35D
CIRCULATING WATER PUMPS
4th POINT HEATER DRAIN PUMPS
MOISTURE SEPARATOR DRAIN PUMP
MECHANICAL REFRIGERATION UNITS
CHILLED WATER CIRCULATING PUMPS
TURBINE PLANT COMPONENT COOLING WATER PUMPS
SCREEN WASH PUMP
480V BUS 32A
480V BUS 32B
480V BUS 32C
480V BUS 32D
480V BUS 32E
480V BUS 32F
480V BUS 32G
480V BUS 32H
480V BUS 32J
480V BUS 32K
480V BUS 32L
480V BUS 32M
480V BUS 32N
480V BUS 32P
480 V BUS 32Q
SCREEN WASH PUMP
TURBINE PLANT COMP. COOLING WATER PUMP
MECHANICAL REFRIGERATION UNIT
4th POINT HEATER DRAIN PUMP
MOISTURE SEPARATOR DRAIN PUMP
CHILLED WATER CIRCULATING PUMP
CIRCULATING WATER PUMPS
REACTOR COOLANT PUMP
CONDENSATE PUMP
REACTOR COOLANT PUMP
CONDENSATE PUMP
STEAM GENERATOR FEEDWATER PUMP
REACTOR COOLANT PUMP
REACTOR COOLANT PUMP
CONDENSATE PUMP
DETAIL A
15G-6X MAIN TRANSFORMER-SPARE 880 MVA FOA 345KV/22.8KV
EMERGENCY SYSTEM
EMERGENCY 4.16KV BUS 34C (TRAIN 'A')
EMERGENCY 4.16 KV BUS 34D (TRAIN 'B')
EMERGENCY SYSTEM
REACTOR PLANT COMPONENT COOLING PUMP
QUENCH SPRAY PUMP
RESIDUAL HEAT REMOVAL PUMP
EMERGENCY GENERATOR 4986 KW CONT. 5335 KW AT 2000 HRS
SAFETY INJECTION PUMP
STEAM GEN. AUXILIARY FEEDWATER PUMP
CONTAINMENT RECIRCULATION PUMP
CHARGING PUMP
SERVICE WATER PUMPS
CONTROL BUILDING WATER CHILLER
CONTAINMENT RECIRCULATION PUMP
CHARGING PUMP
REACTOR PLANT COMPONENT COOLING PUMP
CONTAINMENT RECIRCULATION PUMP
CONTROL BUILDING WATER CHILLER
SERVICE WATER PUMPS
CHARGING PUMP
CONTAINMENT RECIRCULATION PUMP
STEAM GEN. AUXILIARY FEEDWATER PUMP
SAFETY INJECTION PUMP
RESIDUAL HEAT REMOVAL PUMP
EMERGENCY GENERATOR 4986 KW CONT. 5335 KW AT 2000 HRS
QUENCH SPRAY PUMP
REACTOR PLANT COMPONENT COOLING PUMP
480V EMERG. BUS 32T
480V EMERG. BUS 32S
480V EMERG. BUS 32R
480V EMERG. BUS 32Y
480V EMERG. BUS 32U
480V EMERG. BUS 32V
480V EMERG. BUS 32X
480V EMERG. BUS 32W

Fig. 3.4.1-1 Main electrical system (Source: MP 3 FSAR)

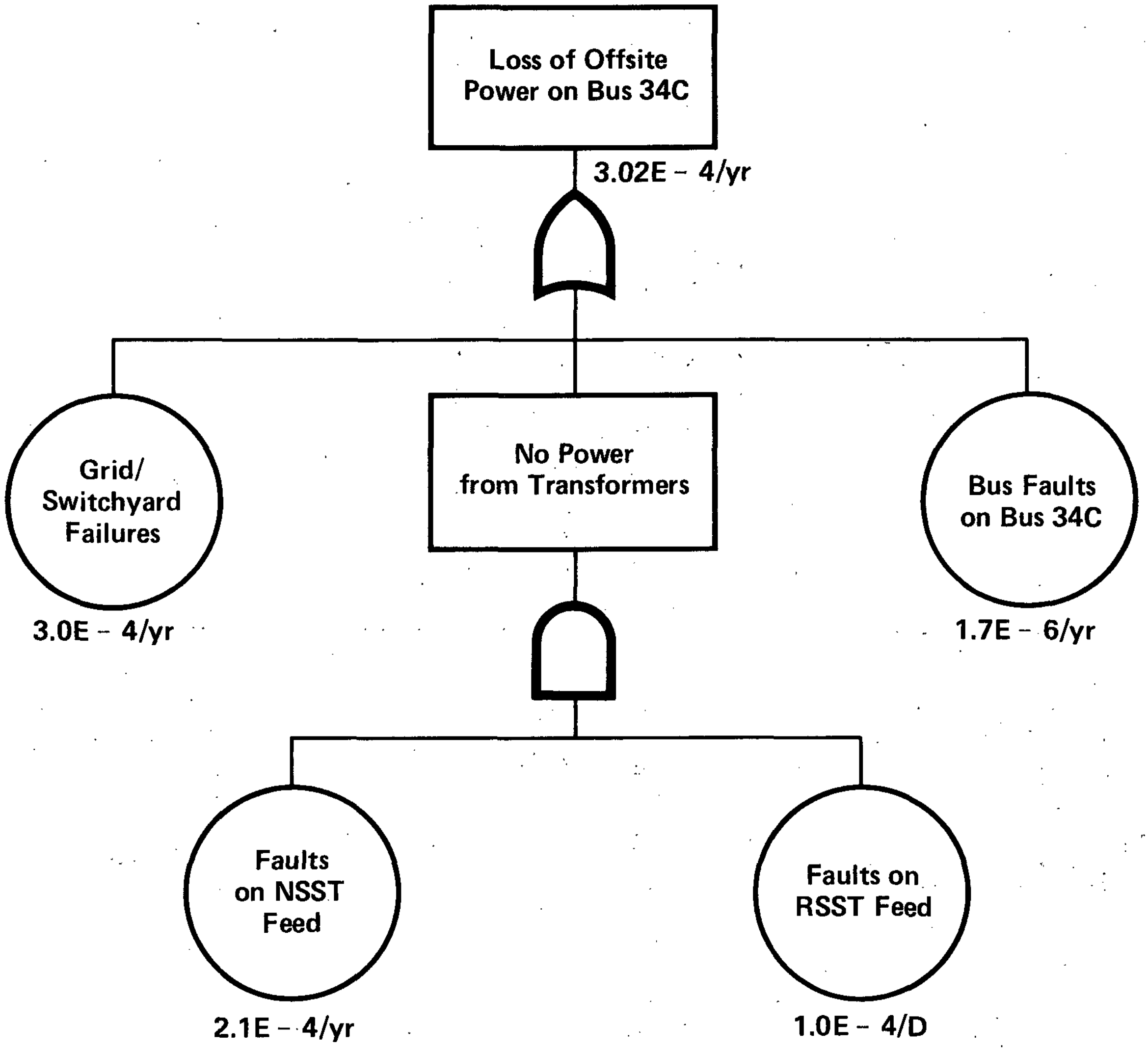
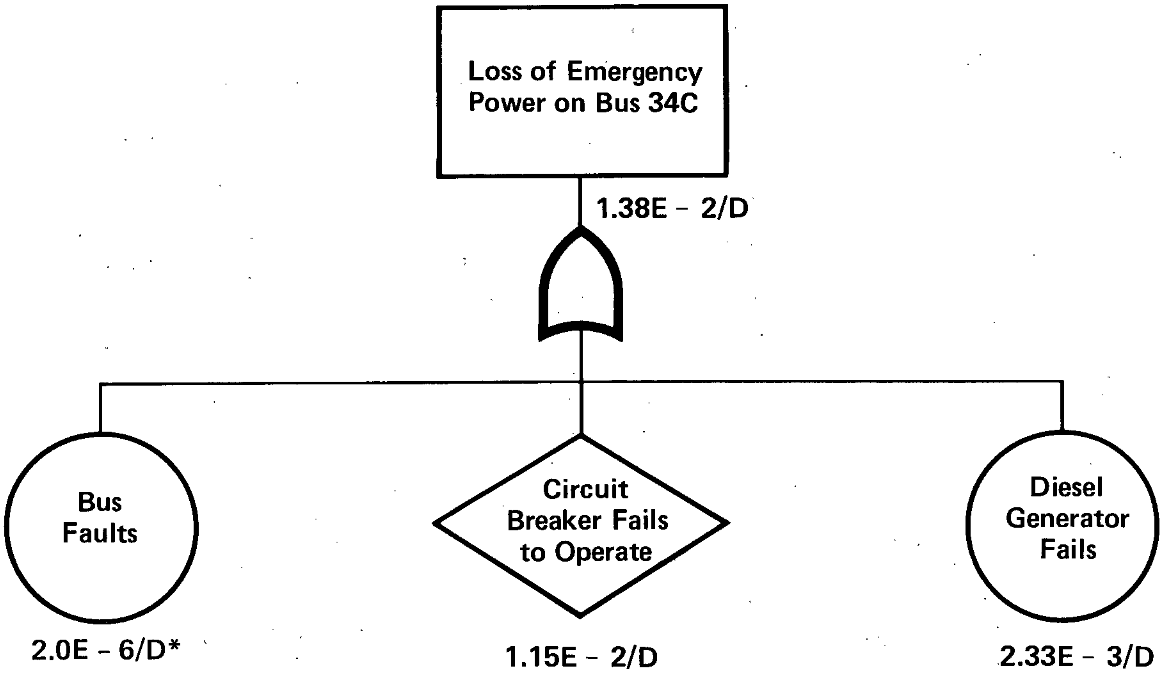


Fig. 3.4.1-2

Fault tree used to calculate the probability of loss of offsite power (Source: MP 3 PSS)



* Failure rates for bus 34C are given as 7.3E - 8/h. The mission time used to calculate failure/D for this fault tree is 28 h. In Figure 3.4.1-2 the mission time used to determine failure/D as a result of bus faults is 24 h giving a value of 1.7E - 6/D.

Fig. 3.4.1-3 Reduced fault tree for the loss of emergency power on one of the two emergency buses.

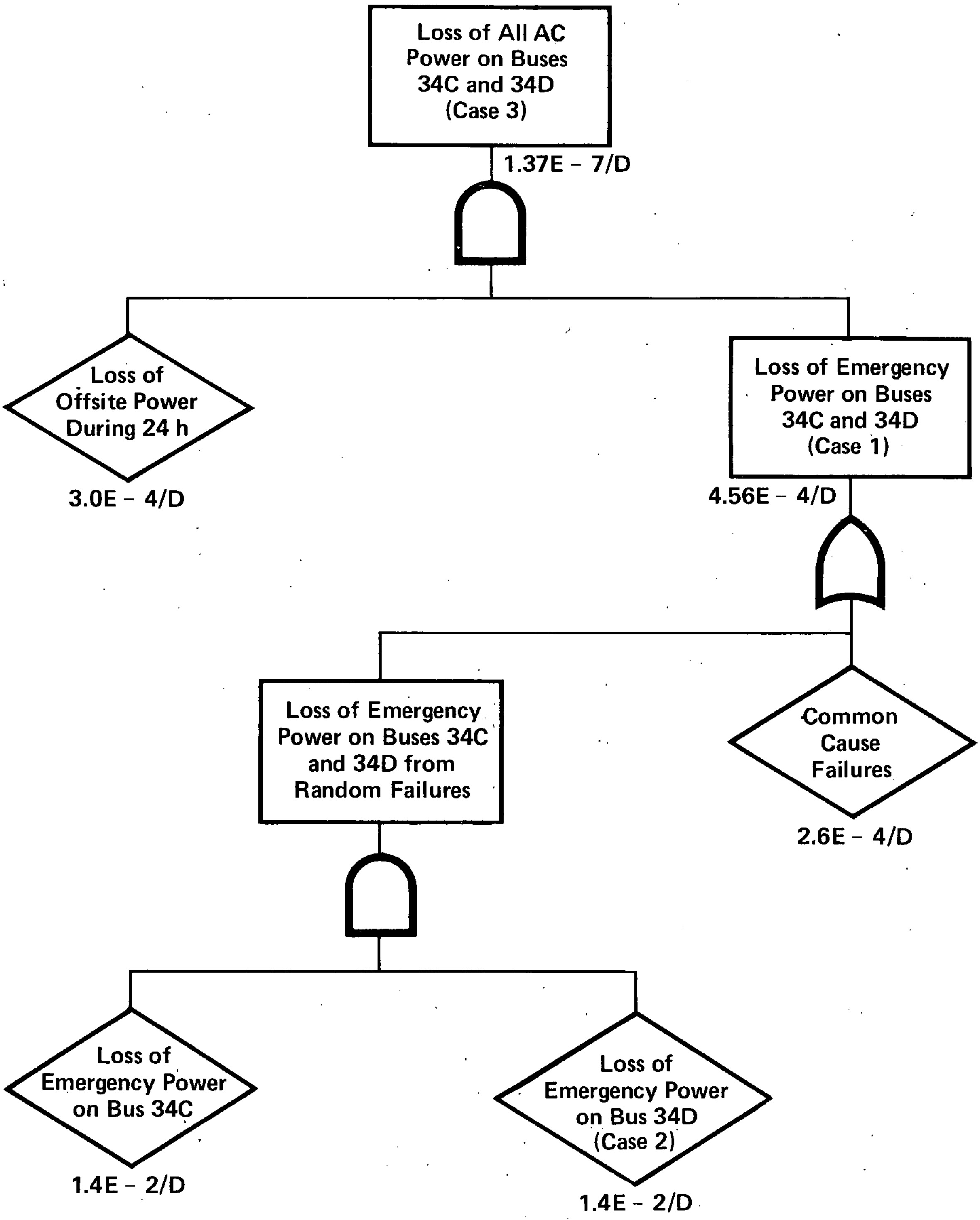

Loss of All AC Power on Buses 34C and 34D (Case 3)
1.37E - 7/D
Loss of Offsite Power During 24 h
3.0E - 4/D
Loss of Emergency Power on Buses 34C and 34D (Case 1)
4.56E - 4/D
Loss of Emergency Power on Buses 34C and 34D from Random Failures
Common Cause Failures
2.6E - 4/D
Loss of Emergency Power on Bus 34C
1.4E - 2/D
Loss of Emergency Power on Bus 34D (Case 2)
1.4E - 2/D

Fig. 3.4.1-4 Simplified fault tree for the main electrical system.

3.4.1.3 Comments on the Main Electrical System Fault Trees

The fault trees for the main electrical system are, for the most part, accurate, complete, and valid. However, several notable exceptions require discussion.

One item of interest involves the circuit breaker between the diesel generator and the corresponding emergency bus. Closure of this breaker requires that a trip coil be energized. This coil is energized by a trip contact that must be closed either manually or automatically. According to the fault tree for this system (Fig. 2.3.2.1-3 of the PSS), failure of this trip contact requires failure of both the automatic and the manual mode. The automatic trip contact requires a signal from the emergency generator load sequencer (EGLS) for operation. But the EGLS requires 120VAC to operate. Nonetheless, the unavailability of EGLS used for this trip coil in the PSS is based on the overall unavailability of vital 120VAC when, in fact, during such an event, the only source of vital 120VAC would be from the 125VDC system.

Another item of concern involves the difference in system resolution for subsystems in the electrical systems fault tree. Diesel generator failure is modeled as a base event, but the circuit breaker between the generator and emergency bus is modeled in significant detail. No explanation is given for the large difference in resolution. If data was available on the overall failure rate for these breakers, it should have been used in preference to the detailed model. Additionally, the fault tree reveals that the circuit breaker relies, in part, on the emergency generator load sequencer which is powered by the vital AC. There appears to be a dependence of the electrical system on itself via the load sequencer that is buried within a rather large fault tree. In contrast to the detailed analysis used for the diesel CB, the absence of CB, transformer, and transfer scheme failures in the LOP analysis indicate that this analysis may be optimistic.

3.4.2 120V AC Vital Bus

3.4.2.1 System Description

The 120VAC vital bus system is a safety-related, voltage-regulated support system. It supplies control and instrument power to the plant protection systems. The 120VAC vital bus is divided into four separate channels. Each vital bus or channel provides a unique source of power to a corresponding ESF or EGLS cabinet. Vital buses VIAC-1 and V1AC-2 supply power to ESF cabinets (Trains A and B), respectively. Similarly, vital buses VIAC-3 and VIAC-4 provide power to EGLS cabinets (Trains A and B). These four vital buses appear as basic events in the ESF actuation system and EGLS system fault trees.

In each channel, the 120VAC vital bus normally receives power from a solid state inverter through a high speed static transfer switch. The primary source of power to the inverter comes through a rectifier from a 480VAC bus (one for each channel). If rectifier output is lost, a secondary DC supply is available from the associated 125VDC battery charger and/or battery. In the event of inverter loss, a third source of 120VAC vital power is provided through a 480V- to 120V-stepdown and regulating transformer from the 480V emergency bus. A simple schematic for the V1AC-1 channel is provided in Fig. 3.4.2-1.

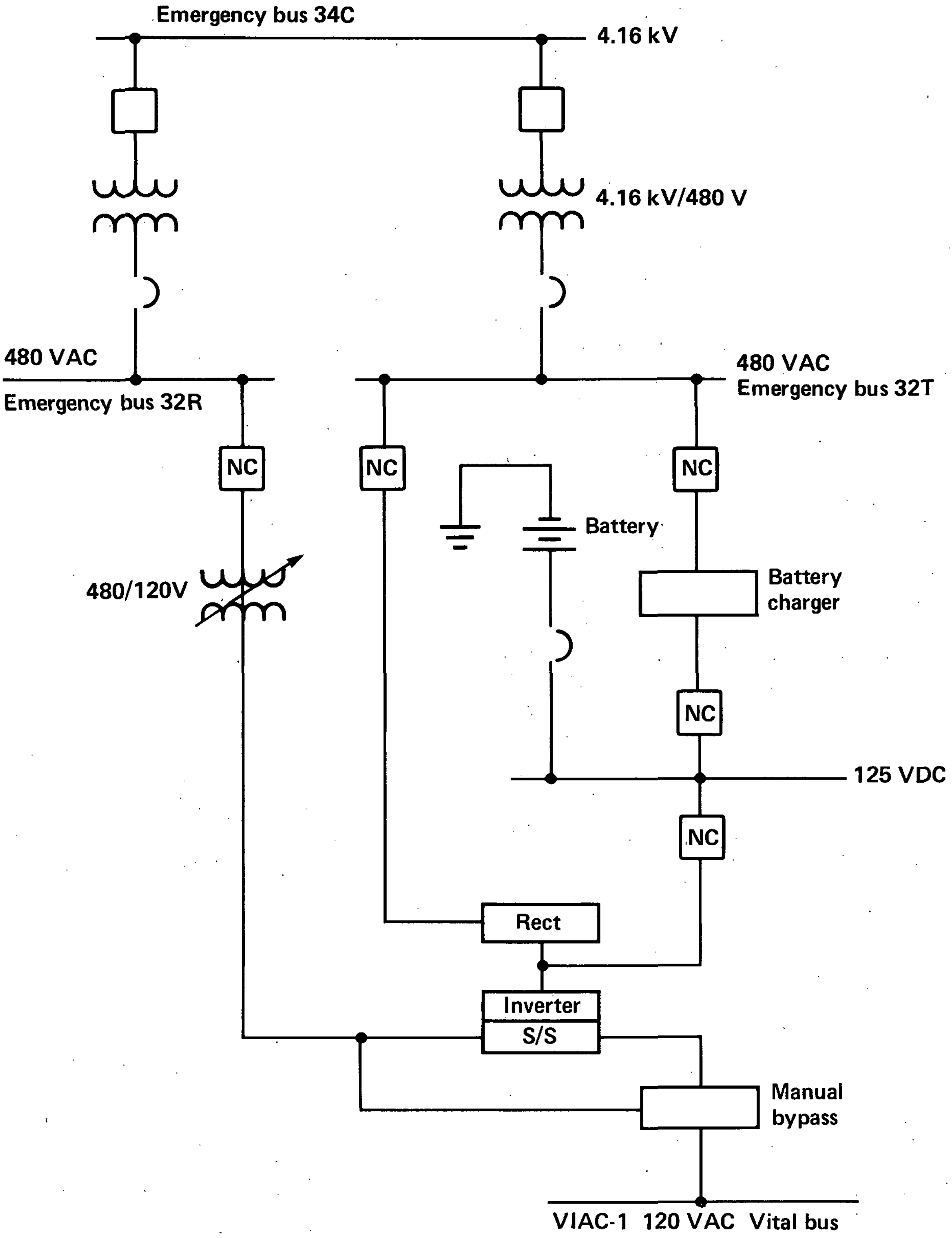


Fig. 3.4.2-1 Schematic of the VIAC-1 channel.

Voltage on each 120VAC vital bus is continuously monitored and displayed in the control room. It is stated that an alarm is sounded in the control room on change of state in the static transfer switch due to loss of inverter output. However, it is not clear exactly what is sensed by this alarm system (i.e., voltage, current).

3.4.2.2. System Fault Tree

The system fault tree for the 120VAC vital bus was used to determine the unavailability of 120VAC power on each channel. Because all four channels are assumed identical, only one fault tree was developed.

The unavailability of the V1AC-1 vital bus was calculated to be 8.4E-5. Almost 99% of the unavailability is contributed by nine cut sets (four singles, four doubles, and one triple). Two singles contribute 66%. These are failures of either the bypass switch or the static transfer switch. The third single cut set (which contributes 14%) comes from a fuse failure, but this fuse was not identified in the schematic provided in the PSS for this system. A fourth single involves bus faults on the 120VAC bus and contributes about 2% unavailability. The four double cut sets involve failure of the regulating transformer and some other component. These contribute about 16%. The final cut set is a triple that includes loss of offsite power, loss of on-site power, and loss of the 480/120V transformer. Because loss of power would not require unavailability of the transformer for system failure, this cut set points up an error in this fault tree's structure. This error is discussed below. Table 3.4.2-1 lists the dominant cut sets that contribute to the unavailability of the vital AC on one channel.

Test and maintenance, common-cause, and human error are not modeled in the vital 120VAC fault tree. The system is in continuous use and there are no tests requiring any of its components to be taken out of service. All maintenance is performed during refueling outage. Unscheduled maintenance is supposed to be performed only with continuous power maintained to the vital bus through an alternate source. The PSS states that no common-cause failures were postulated for the vital AC because they were accounted for by command faults that are included in pump and MOV start logic. It is also stated that no credible human errors could contribute to system unavailability.

3.4.2.3 Comments

Our initial review of the vital 120VAC fault tree revealed several inaccuracies. In particular there was a problem in the representation of the system logic. Nonetheless, we estimated that these errors did not contribute more than a 10% error in the calculation of system unavailability. After discussing these problems with NU personnel, we received a revised fault tree which addressed these concerns. Nevertheless, the revised fault tree contained an error that was not in the original fault tree, in that loss of power on bus 34C is no longer modeled in the system fault tree. Thus, the tree still does not fully model the unavailability of vital AC. However, our analysis of the fault tree reveals that, because system failure is dominated by switch, fuse, and transformer failures, this error does not contribute significantly to the estimate of this systems unavailability.

Failures in the vital AC system were not major contributors to risk in the Millstone PSS. Nonetheless, the problems noted could become significant for

Table 3.4.2-1 Dominant cut sets in the PSS for the unavailability at the 120V vital AC.

Cut set probability	Component failures (failure/demand)
Static transfer switch fails open	2.8E-5
Rotary bypass switch transfers open	2.8E-5
Fuse opens prematurely	1.2E-5
Power transformer and inverter fails	1.13E-5
Bus faults on the vital 120-AC bus	2.0E-6
Power transformer (480/120) and power transformer (4.16kV/480V) fails	1.3E-6
Total	8.43-5

cases in which the probability of basic events may have changed. Thus, the usefulness of this fault tree for uncertainty and sensitivity analyses may be limited until these problems can be corrected.

3.4.3 Engineered Safety Features Actuation System

3.4.3.1 System Description

The engineered safety features (ESF) actuation system examines selected plant parameters and determines whether predetermined protection limits are being exceeded. The ESF actuation system consists of two separate sets of electronic circuitry. The first set is an analog portion consisting of three to four (depending on the system) redundant channels per system parameter. The second set is made up of two redundant logic trains which process the analog inputs and actuate ESF equipment as required.

Each channel of the analog portion is connected to a separate and redundant sensor for the parameter of interest. This channel is made up of four major components: (1) the channel test switch, (2) the loop power supply, (3) the comparator, and (4) the comparator trip switch. With the exception of the containment spray system, the comparator trip switch operates on the "de-energize-to-actuate principle" so that the analog portion of the ESF actuation system cannot be disabled during test.

The output signals from the analog channels are transmitted to two separate and redundant logic trains corresponding to the separate safety system trains (Trains A and B). The logic trains pass the channel output through input relays to the logic cabinet. The logic cabinet uses 2/3 or 2/4 logic to trip a relay driver which actuates the corresponding safety system. Each logic train is independently capable of actuating the required ESF equipment.

3.4.3.2 System Fault Tree

The ESF actuation system was modeled to determine the unavailability of actuation signals on the final outputs. The Millstone team from NU determined that a model for the safety injection (SI) signal would adequately represent all other signals.

The results of the fault tree quantification for the SI signal yield an unavailability of 1.17E-3/per demand per signal per train with a variance of 1.53E-6. The calculated unavailability for both trains (including common-cause failures) is 1.60E-5/ demand/ signal for both trains. Almost 99% of the unavilability for a single train is contributed by five dominant cut sets. These single member cut sets are summarized in Table 3.4.3-1.

The dominant contributor to system unavailability is a bimonthly logic test which temporarily disables the system and makes up 29% of the total. This is followed by failure of two different universal logic cards which respectively make up 14 and 27% of the total. Failure of vital AC power supply and a relay driver comprise a respective 7% and 5% of the remaining contributions.

Even though testing of the digital portion of the system makes a significant contribution to unavailability, testing on the analog portion does not. This is because the channel being tested is energized and thus in "actuate" mode. The exception to this is the quench spray actuation which has a separate model for unavailability that is discussed in Section 3.4.9. System unavailability due to maintenance is included in random hardware faults.

The common-cause failure analysis is limited to command faults within the ESF sensors. According to the PSS, this limitation is due to the diversity within the ESF which makes other common-cause failures noncredible. Failure of the main electrical system and the emergency AC buses is treated as resulting in a dependent failure of both the ESF and ESF actuation system. Common-cause failures of both trains of the ESF actuation system were judged by the PSS to occur at the rate of 1.5E-5 demand.

This value is obtained from the overall reliability of the electrical portion at the reactor protection system as cited in NUREG-0460 (Ref. 3.4-1).

The Millstone PSS considers two sources of human errors that contribute to ESF actuation system unavailability. One source is associated with periodic testing of the analog portion of the system, the other with periodic testing on the digital portion. In the analog portion, the quench spray sensor channels, because they are the only set of channels that do not operate on the "de-energize-to-actuate principle", can contribute to unavailability from failure to restore the channels after testing. This source of human error is unique to the quench spray system and included in its fault tree. For the digital portion of the ESF actuation system, test unavailability due to human error is insignificant compared to that contributed by the test itself.

3.4.3.3 Comments

Our review of the ESF actuation system fault tree raised some concerns regarding its completeness, accuracy, and validity in treating common-cause failures. The calculated unavailability of both trains is dominated by common-cause failure. But common-cause failure is estimated from a value derived from NUREG-0460. There is limited consideration given to the validity of this value. Certainly, there is a great deal of uncertainty associated with a value obtained from a systems analysis of the reactor protection system at another plant.

Unavailability of a single train is dominated by tests on the digital portion of the system. Thus, any errors in estimating the amount of time necessary for the test procedure could be important. In addition, the calculation of variance in system unavailability for the ESF actuation system is not provided.

3.4.4 Emergency Generator Loading Sequencer (EGLS) System

3.4.4.1 System Description

The EGLS is a solid-state digital system that is designed to sequence the reloading of ESF systems to prevent electrical system instability caused by motor starts when power from the diesels transfers to the emergency bus. The system provides actuation signals to shed loads, temporarily block manual equipment starts, and sequentially load ESF equipment on buses 34C and 34D during emergency conditions. The overall sequencing system is comprised of two identical EGLS cabinets, Trains A and B, which are powered from separate 120VAC vital buses, VIAC-3 and VIAC-4.

Table 3.4.3-1 Dominant cut sets in the PSS for the unavailability of an actuation signal on one train of the ESF actuation system.

Component failure		Probability (failure/demand)
Unavailability due to test of the digital circuitry		3.4E-4
Improper operation of universal logic card		3.2E-4
Improper output from the universal logic card		1.6E-4
Relay contacts fail to transfer		1.0E-4
Unavailability of 120V vital AC		8.4E-5
Relay driver receives improper output from one gate		5.3E-5
	Total	1.17E-3

The EGLS receives and processes signals of bus undervoltage due to loss of power (LOP), safety injection (SIS), containment pressure change (CDA), recirculation (RECIRC), reserve breaker (AR BKR), and diesel generator breaker (DG BKR) status. The EGLS automatically performs the functions of load shedding, load blocking, and sequential load application under conditions of LOP, SIS with LOP, and CDA with LOP. Under the conditions of (SIS) without LOP and CDA without LOP, the EGLS does not introduce load shedding, load blocking or sequential load application into any of the control circuits of the engineered safety features (with the exception of the containment recirculation pumps which are actuated by the RECIRC signal after a five minute time delay following CDA). However, the EGLS processes the SIS and CDA signals in these cases, and it is thus required to close breakers on standby equipment, even though simultaneously. An EGLS is provided for each emergency generator.

During the first 40 seconds, the EGLS automatically and sequentially applies loads to the buses which power the safety systems. After the first 40 seconds, the manual start block signal is removed and additional emergency bus loads may be started manually. Typical loads manually started are the pressurizer heaters, fuel pool cooling pumps, and turbine protection equipment.

The EGLS has seven operating modes. Five of these modes are for plant emergency conditions which involve LOP. The other two are for plant emergency conditions which do not involve an LOP. The modes are prioritized such that a CDA mode will always take precedence over an SIS mode when both inputs are present. An LOP mode will always take precedence over a non-LOP mode.

In each of the LOP operating modes, the EGLS first recognizes a loss of power on the plant safety buses and immediately generates LOP and manual start block (MSB) output signals to plant safety equipment. These signals effectively strip the bus and temporarily inhibit the operator from restarting any loads. This allows each diesel generator time to start, achieve proper voltage and frequency, and be connected to its dedicated safety bus without incurring adverse loading conditions. Upon receiving a signal confirming that the DG BKR has closed, the EGLS will begin generating time-sequenced "safeguard sequencer start" (SSS) and manual trip block (MTB) signals to plant equipment. Once initiated, the SSS and MTB signals are maintained until the EGLS is reset. Should an SIS or CDA input occur without an LOP, the appropriate SSS and MTB signals are generated immediately without time sequencing. The MTB signal inhibits the operator from tripping loads once they have been automatically started.

3.4.4.2 System Fault Tree

The sequencer system fault tree was used to determine the unavailability of one or both EGLS systems. This information was employed in the support states model as the unavailability of EGLS trains. It is also used as the unavailability of the EGLS signal for the diesel generator breaker in the main electrical system fault tree. Two fault trees are used to represent the seven sequencer modes. These two are the SIS signal only mode and the SIS with LOP mode. The quantified output of these fault trees is used to represent the operating mode unavailability of the sequencers.

In the "SIS only" operating mode, four dominant cut sets are reported to contribute 80% of the total availability of 8.2E-4. The remaining cut sets contribute less than 1% each. The dominant contributor is stated to be failure of AC power which makes up 30% of the total. Failure of sequencer input relays to energize, reportedly contributes 25%. Failure of the sequencer output relay and failure of an input signal from the diesel generator auxiliary breaker contacts, reportedly contribute 12.5% each.

In the "SIS with LOP" operating mode, approximately 94% of the total unavailability of 9.3E-4 is stated to be due to four cut sets. The remaining sets contribute less than 1% each. For this mode the dominant contributor is input relay failure, which contributes 37.5%. Another 30% is stated to be due to AC power supply failure. Failures of the output relay and diesel generator auxiliary breaker contacts contribute 12.5% each.

There are no test and maintenance procedures that are credited as contributors to system unavailability. The EGLS has two manual test modes and one automatic test mode. One of the manual tests, which is performed monthly, does not prevent the sequencer from responding to accident signals. The other manual test is performed only during refueling outages. The automatic test sequence is performed at 30-second intervals and also does not inhibit accident signals. There is no scheduled maintenance on the sequencer. Unavailability due to unscheduled maintenance is not included in the fault tree.

Two sources of common-cause failure are considered for the sequencer. One source is a dependent failure due to the loss of vital AC. The other is failure within the sequencer hardware. The common-cause failure rate for both trains of ELGS actuation is judged to be 1.5E-5 per demand in the PSS, the same value used for the ESF actuation system. The justication given for this value is that the EGLS has an equal or greater diversity than the reactor protection system (RPS) used in NUREG-0460 (Ref. 3.4-1), so that the same common-cause failure probability may be used.

3.4.4.3 Comments on the EGLS Fault Trees

Our review of the EGLS fault tree reveals that to some extent it is invalid, inaccurate and incomplete. We identified several major problems which make it difficult to assess the final top event unavailability without more information and a restructuring of the fault tree logic. Our concerns are enumerated below.

The major problem involves the failure to accurately model the dependence of a single sequencer on the corresponding vital AC and vital DC systems. A major difficulty comes from the use of the output from the vital 120-AC fault tree as a substitute for the vital DC failure. The fault tree model does not deal with the fact that, following a loss-of-power accident, the EGLS would be the primary initial support system and that for the first 10 to 40 seconds following this event, it would be functioning with AC power unavailable on buses 34C and 34D.

The unavailability of both EGLS cabinets is apparently dominated by common-cause failures. However, the common-cause failure rate in the PSS is based on the rate for the electrical portion of the reactor protection system (RPS) in NUREG-0460. This rate was used for the EGLS because the Millstone EGLS has an equal or greater diversity than the NUREG-0460 RPS.

There are many aspects of the load sequencer operations which are not addressed in the PSS. In particular, the loading sequencer performs functions which raise questions relative to the possibility of exacerbating accident conditions. The sequencer strips loads on plant safety buses when it receives a loss-of-offsite-power signal. During subsequent diesel generator startup, it blocks manual starts of safety equipment. Failure of the EGLS at this point could result in the total inability to load equipment. When the diesel generator breaker closes, the sequencer begins to load the safety buses with safety equipment in a timed sequence and initiates manual trip blocks so that the equipment cannot be tripped. As a final point, we note that the dominant cut sets described in the text do not correspond to those provided in the computer output listing. However, the same total unavailability is reported in both places.

3.4.5 Auxiliary Feedwater System

3.4.5.1 System Description

The auxiliary feedwater system (AFWS) is an engineered safeguards system which is designed to provide a supply of high pressure feedwater to the secondary side of the steam generators, for reactor coolant system (RCS) heat removal following a loss of normal feedwater. The AFWS also provides this cooling function in the event of a main steamline break, feedwater line break, small break loss-of-coolant accident (LOCA), loss of power, or low low steam generator water level conditions. In addition, the AFWS is designed to respond to all of the above conditions whether or not all AC power is available.

The AFWS consists of two motor-driven auxiliary feedwater pumps, one turbine-driven auxiliary feedwater pump, and the associated controls, piping, and valves necessary to perform the RCS heat removal function. Each auxiliary feedwater pump normally takes suction from the demineralized water storage tank (DWST). The DWST, which is sized at 340,000 usable gallons, has sufficient capacity to provide the short-term safety grade source of auxiliary feedwater for the steam generators. An additional source of 200,000 gallons of water is provided to the auxiliary feedwater pumps by the condensate storage tank. This non-safety grade source of water is connected to each pump suction line through normally closed air-operated valves. The long-term safety grade source of auxiliary feedwater is provided by the service water system.

The AFWS is normally lined up to all four steam generators through normally-open, motor-operated control valves. In the event of an AFWS demand, the minimum success criteria stated in the PSS is that one of the three auxiliary feedwater pumps start and run. Redundant piping flow paths from the pumps to the steam generators provide at least two of the steam generators with the required flow even if only one pump is available for service. Each of the two motor-driven pumps is capable of feeding two steam generators while the tubine-driven pump is capable of feeding all four steam generators.

3.4.5.2 System Fault Tree

The auxiliary feedwater system fault tree was used to assess the failure of the system to meet its success criteria for a period of 24 hours following any postulated accident or transient. System success is defined as delivering 235 gpm of auxiliary feedwater to at least three of four steam generators following all transients.

The auxiliary feedwater system fault trees (with and without a faulted steam generator) were quantified for six cases in order to represent the effects of the plant support states:

- Case A: Both trains of AC power available - no faulted steam generator (addresses support states 1 and 5)

- Case B: One train of AC power available or equivalent - no faulted steam generator (addresses support states 2, 3 and 6)

- Case C: No AC power available - no faulted steam generator (addresses suport state 7).

- Case D: Turbine-driven AFWS pump train not available and both trains of AC power recovered - no faulted steam generator (addresses support state 7 for loss of offsite power as the initiating event)

- Case E: Both trains of AC power available or equivalent - one faulted steam generator (addresses support states 2, 3, 6 and 7)

- Case F: No AC power available or equivalent - one faulted steam generator (addresses support states 2, 3, 6, and 7)

Table 3.4.5-1 summarizes the unavailabilities of the auxiliary feedwater system for each support state with/without a faulted steam generator. For support state 8, both ESF actuation Trains A and B are assumed to be unavailable. Thus, AFWS unavailability is 1.0 by definition. Table 3.4.5-2 lists the dominant contributors for each of the six cases A through F.

The common-cause failure analysis for the AFWS used a binomial failure rate model. The analysis treated the turbine-driven auxiliary feedwater pump as a diverse system with respect to the motor-driven auxiliary feedwater pump trains. Analyses were performed for both those accidents and transients that do not require a steam generator to be isolated and those that do require isolation. A total of seven common-cause analyses were performed. They are:

1 No faulted steam generator, both emergency AC buses available
2 No faulted steam generator, one emergency AC bus available
3 No faulted steam generator, no emergency buses available
4 No faulted steam generator, loss of turbine-driven auxiliary pump
5 One faulted steam generator, both emergency AC buses available
6 One faulted steam generator, one emergency AC bus available
7 One faulted steam generator, no emergency bus available

Table 3.4.5-1 Summary of unavailability results for the auxiliary feedwater system.

Support state	Steam generator status	System unavailability (failure/demand)	Case
01	None isolated	6.8E-5	A
01	Steam generator "A" isolated	4.94E-4	E
02	None isolated	5.9E-4	B
02	Steam generator "A" isolated	4.53E-2	F
03	None isolated	5.9E-4	B
03	Steam generator "A" isolated	4.53E-2	F
04	None isolated	1.0	-
04	Steam generator "A" isolated	1.0	-
05	None isolated	6.8E-5	A
05	Steam generator "A" isolated	4.94E-4	E
06	None isolated	5.9E-4	B
06	Steam generator "A" isolated	4.53E-2	F
07	None isolated	4.52E-2	C
07	None isolated	2.77E-4[a]	D
07	Steam generator "A" isolated	4.53E-2	F
08	None isolated	1.0	-
08	Steam generator "A" isolated	1.0	-

[a] For support state 07 with loss of offsite power as the initiating event and recovery of offsite power occurring within one hour.

3.4.5.3 Comments on the AFWS Fault Tree

In general, we found the fault trees for this system to be accurate, complete, and valid. Nonetheless, we noted issues of concern regarding success criteria and the overall unavailability of the system. One issue is that the auxiliary feedwater unavailability probability (6.8E-5/demand) appears optimistic. Other assessments have derived values 5 to 10 times greater for similar systems, and even higher failure rates may be expected early in life. A further discussion of this matter is provided in Section 3.6.

Table 3.4.5-2 Dominant contributors to unavailability for cases A-F in the PSS.

Case	Dominant contributors	Percent
A	Common-cause	96
B	Motor-driven pump "A: and turbine-driven pump both fail	37
	Pump "A" actuation logic and turbine pump failures	16
	Common-cause	10
C	Turbine-driven pump failure	90
D	Common-cause	54
	Random failures in the motor-driven pumps	46
E	Failure of pump "B" and steam pump	64
	Common-cause	13
F	Turbine-driven pump failure	90

3.4.6 High Pressure Safety Injection System

3.4.6.1 System Description

The high pressure safety injection system (HPSI) provides reactor core cooling and shutdown capability by injecting borated water into the reactor vessel following a loss-of-coolant accident (LOCA). The HPSI system, in conjunction with the low pressure safety injection system and the recirculation cooling system, must provide adequate cooling and makeup to the reactor core for sufficient time to mitigate the effects of any postulated LOCAs.

The major components of the HPSI system are three charging and two HPSI pumps, along with the associated piping, valves, and control circuitry. Two of the three charging pumps are normally used for the chemical and volume control system. These two pumps are rotated on a monthly basis so that one pump is always operating. When the safeguards actuation signal ("S" signal) is received, the injection mode of operation is automatically initiated. The non-operating charging pump is started and both it and the running pump are realigned to take suction from the refueling water storage tank (RWST), discharging into the reactor coolant system cold legs (one in each of the four RCS loops). During normal plant operation, the two HPSI pumps are not in operation but are prealigned to the RWST. When the "S" signal is received, both pumps start, taking suction from the RWST, and discharging to the RCS cold legs. The "S" signal comes from the ESF actuation cabinet.

3.4.6.2 System Fault Tree

The fault tree for the HPSI system is used for three classes of accidents - large, medium, and small LOCAs. The success criterion for a large LOCA specified that two of four charging or HPSI pumps be available. The success criterion for a small or medium LOCA specified that one of four charging or HPSI pumps be available. The system fault tree was used to quantify the probability of failing to achieve the success criteria for the three LOCA classes in each of eight support states. The results of these calculations are provided in Table 3.4.6-1. Six fault tree calculations were used to obtain the 16 values shown in Table 3.4.6-1. Table 3.4.6-2 lists the dominant cut sets in each of these six cases and the percentage of the cut set contribution to overall unavailability.

The effects of common-cause failures, test and maintenance unavailability, and human errors were all included in the HPSI fault tree. Common-cause failure was modeled using a binomial failure rate model. The only human error that was included was failure to restore equipment after test and maintenance. These failures were included along with random equipment failures.

3.4.6.3 Comments on the HPSI Fault Tree

Our review of the HPSI fault tree indicates no major problems with regard to validity, accuracy, and completeness. The HPSI fault trees indicate that for small, medium and large LOCA, the unavailability in support states 1 and 5 is dominated by common-cause failures. Unavailability in support states 2 and 6 is dominated by the unavailability of the oil cooling system for the charging and SI pumps. In support states 3, 4, 7, and 8, the HPSI system unavailability is one due to dependent failures.

One item of concern is the vague description of success criteria. It is stated that two of four charging or HPSI pumps are required for a large LOCA and one of four charging or HPSI pumps are required for a medium LOCA. It is not clear, under this criterion, whether two charging pumps or one charging pump and one HPSI pump are the minimum requirement for system success in a large LOCA. Similarly, it is equally unclear whether the success criteria imply that one charging pump is sufficient to mitigate a medium LOCA. Also, there is no consideration given to pump "run-out." Additional discussion of these issues is provided in Section 3.3.

3.4.7 Low Pressure Safety Injection System

3.4.7.1 System Description

The low pressure safety injection (LPSI) system is designed to provide a large volume of water to the cold legs of the reactor coolant system (RCS) in the event of a loss-of-coolant accident (LOCA). In the first phase of emergency

Table 3.4.6-1 High pressure safety injection system unavailability results in the PSS.

	System unavailability (mean values)	
	Large LOCA (HP-1)	Medium and small LOCA (HP-2)
Support states	(per demand)	(per demand)
1	1.12E-4	5.87E-5
2	5.19E-2	7.01E-4
3	1.0	1.0
4	1.0	1.0
5	1.38E-4	5.88E-5
6	5.19E-2	7.01E-4
7	1.0	1.0
8	1.0	1.0

Table 3.4.6-2 High pressure safety injection system dominant contributors.

Hypothetical accident	System unavailability (failure/demand)	Dominant contributor (failure/demand)	Contribution %
Large LOCA (HP-1)			
AC power available	1.12E-4	7.47E-5 common-cause failure	67
loss of one bus	5.19E-2	2.38E-2 SI and chg cooling	46
loss of offsite AC power	1.38E-4	8.27E-5 common-cause failure	60
Medium and Small LOCA (HP-2)			
AC power available	5.87E-5	5.87E-5 common-cause failure	∿100
loss of one bus	7.01E-4	1.42E-4 SI and chg cooling	20
loss of offsite AC power	5.88E-5	5.88E-5 common-cause failure	∿100

core cooling (ECC), borated water from the RWST and the accumulators is delivered to the RCS cold legs. When the water level in the RWST reaches the low low level limit, the LPSI system terminates injection and the second phase of ECC begins. This phase involves the recirculation of borated water from the containment sump to the RCS cold legs by the residual heat removal (RHR) pumps.

The LPSI system consists of the accumulators, the RHR pumps, and the associated valves, orifices, piping, and supporting circuitry. There are four independent accumulator trains, each of which is dedicated to one of the four reactor coolant system loops. The two RHR pumps are included in two redundant and independent trains. Each train delivers water to all four RCS loops.

3.4.7.2 System Fault Tree

The LPSI system fault tree was used to calculate the probability of system failure based on two system success criteria. The first criterion is associated with the large LOCA, vessel rupture, or interfacing systems LOCA initiating events. Water must be delivered from three accumulators and at least one full-capacity RHR pump. System failure occurs when either one accumulator fails to discharge into an unbroken loop or when both RHR pumps fail to deliver water to three intact RCS loops. The second criterion is associated with the medium LOCA initiating event and requires that one out of two full capacity RHR pumps deliver to two intact cold legs.

Compatability with the support states model required that the LPSI system fault tree be quantified for two cases. Case 1 addresses situations in which both trains of AC power are available and corresponds to support states 1 and 5. Case 2 addresses situations in which only one train of AC power is available and corresponds to support states 2 and 6. The LPSI system is unavailable in support states 3, 4, 7, and 8.

The LPSI system unavailability and dominant cut set contributions for cases 1 and 2 are summarized in Table 3.4.7-1. When both trains of AC power are available (case 1), unavailability of the accumulators is the dominant cut set, contributing 92% of the overall system unavailability.

Common-cause failures contribute approximately 7%. When only one train of AC power is available (case 2), 32% of the system failure probability is attributed to the actuation circuits spurious closure of the motor-operated valve in the pump miniflow line. Failure of accumulator check valves contributes approximately 29%. Hardware faults of the RHR pump contribute 21%. Failure of the check valves in the suction and discharge lines of the RHR pump account for 10% of the failure probability.

Test and maintenance unavailability, common-cause failures, and human error are all included in the system fault tree. A test unavailability analysis is not included in the LPSI fault tree because it is stated that tests do not make the system unavailable. Components outside of containment that can be isolated and tested for failure are maintained on an unscheduled basis. Thus, maintenance unavailability calculations have been done for check valves, air-operated valves, motor-operated valves, and the RHR pumps. A common-cause failure analysis was performed for the two RHR pumps and the motor-operated isolation valves in the pumps' miniflow lines. The common-cause failure calculations were based on a binomial failure rate model. Human errors that

Table 3.4.7-1 Dominant contributors to LPSI system unavailability in the PSS.

Components		Failure probability (per demand)
Case 1: Both AC trains available		
Accumulator check valves		1.9E-3 (92%)
Common cause		1.6E-4 (7%)
	Total	2.1E-3 (100%)
Case 2: One AC train available		
Circuit breaker on pump fails to close		2.1E-3 (31%)
Accumulator check valves		1.9E-3 (29%)
Accumulator check valves		1.4E-3 (21%)
Other check valves		6.4E-4 (10%)
	Total	6.7E-3 (100%)

were given credit for system failure involve failures to restore the RHR pumps and vital motor-operated and air-operated valves following test and maintenance.

3.4.7.3 Comments on the LPSI System Fault Tree

In general, the LPSI system fault tree appears to be accurate, complete, and valid. Nonetheless, with regard to the long- and short-term system success criteria there are issues that may require additional analysis.
The LPSI system is defined as including the RHR pumps and the accumulators. The success criterion is stated to be three accumulators and one RHR pump for the large LOCA, a vessel rupture or an interfacing systems LOCA (event V). According to this criterion, the system is modeled as failed when one of three accumulators fails even when two RHR pumps are available. It is not likely that failure of a single accumulator would result in a core melt when one or more RHR pumps is operating. The fact that accumulator failure appears to dominate LPSI failure could make this criterion an important conservatism. However, The LPSI is not a contributor to any risk at Millstone 3. Thus, this conservatism is not likely to be significant. Nonetheless, it should be recognized that for event V, the accumulators are of little use and the operation of the RHR system is not sufficient for success against this sequence. Finally, it is also speculative whether one RHR pump could prevent core melt for a rupture low in the reactor vessel.

The requirement for long-term operation of the RHR is not considered in the fault tree analysis. For long-term decay heat removal, the RHR may have to operate several weeks. However, this would be the case only if the plant were not restarted. Additionally, the active components of the RHR are outside the containment where maintenance and repair could be readily performed. Thus, failure of the RHR in the extended cooling mode is not likely to be a significant risk contributor.

3.4.8 Main Steam Isolation System

3.4.8.1 System Description

The main steam isolation (MSI) system is designed to prevent uncontrolled blowdown of the steam generators in the event of a steamline break. The system consists of one 30-inch, steam-operated "Y" pattern globe valve per loop, for a total of four valves. The valves are located in the main steam piping downstream of the main steam safety and relief valves, in the main steam valve building.

The main steam isolation trip valves are designed to close within 5 seconds of receipt of a steamline isolation signal for all values of pressure differential across the valve. They are designed to fail in the closed position upon loss of electrical power or steam header pressure and are spring loaded in the close direction. Main steamline header pressure acts as the operating medium for both the opening and closing operations of the valves. An external nitrogen supply is used for operation and testing of the valves when steamline header pressure is below approximately 185 psig.

Each main steam isolation trip valve is controlled by redundant pairs of solenoid valves (a set of Train A and B solenoid valves). Opening and closing sets of solenoid valves pressurize and vent the bottom and top of the valve-operating piston compartment.

3.4.8.2 System Fault Tree

The MSI system fault tree was used to determine the probability of failing to achieve the system success criteria following a postulated steamline break. Two types of steamline breaks are considered; a steamline break inside containment, and a steamline break outside of containment. For a steamline break inside containment, the success criterion is closure of the MSI valve on the faulted steam generator/steamline or the closure of three out of three MSI valves on the unfaulted steam generator/steamlines. For a steamline break outside of containment, the success criterion is closure of any three out of four MSI valves. Because the MSI system fails safe upon loss of power and does not depend on service water, the support states that relate to ESF electric power and service water supply are not addressed in the MSI failure analysis.

The calculated unavailability for the MSI system is:

Case	Mean system unavailability (failure/demand)	Variance
Steamline break inside containment	8.2E-4	7.1E-7
Steamline break outside containment	1.5E-3	4.9E-6

The dominant contributor to total unavailability in both cases is common-cause failures. Common cause contributes 92% of the total mean unavailability for steamline breaks inside containment and 91% for steamline break outside containment.

3.4.8.3 Comments on the MSI System Fault Tree

No problems in terms of accuracy, completeness, and validity were found with the MSI system fault tree. System failure is dominated by common-cause contributions. The common-cause failure analysis employs the binomial failure rate model, which is described in Appendix 2-C of the PSS and reviewed in Section 3.10 of this report. A separate common-cause analysis was performed for each success criterion.

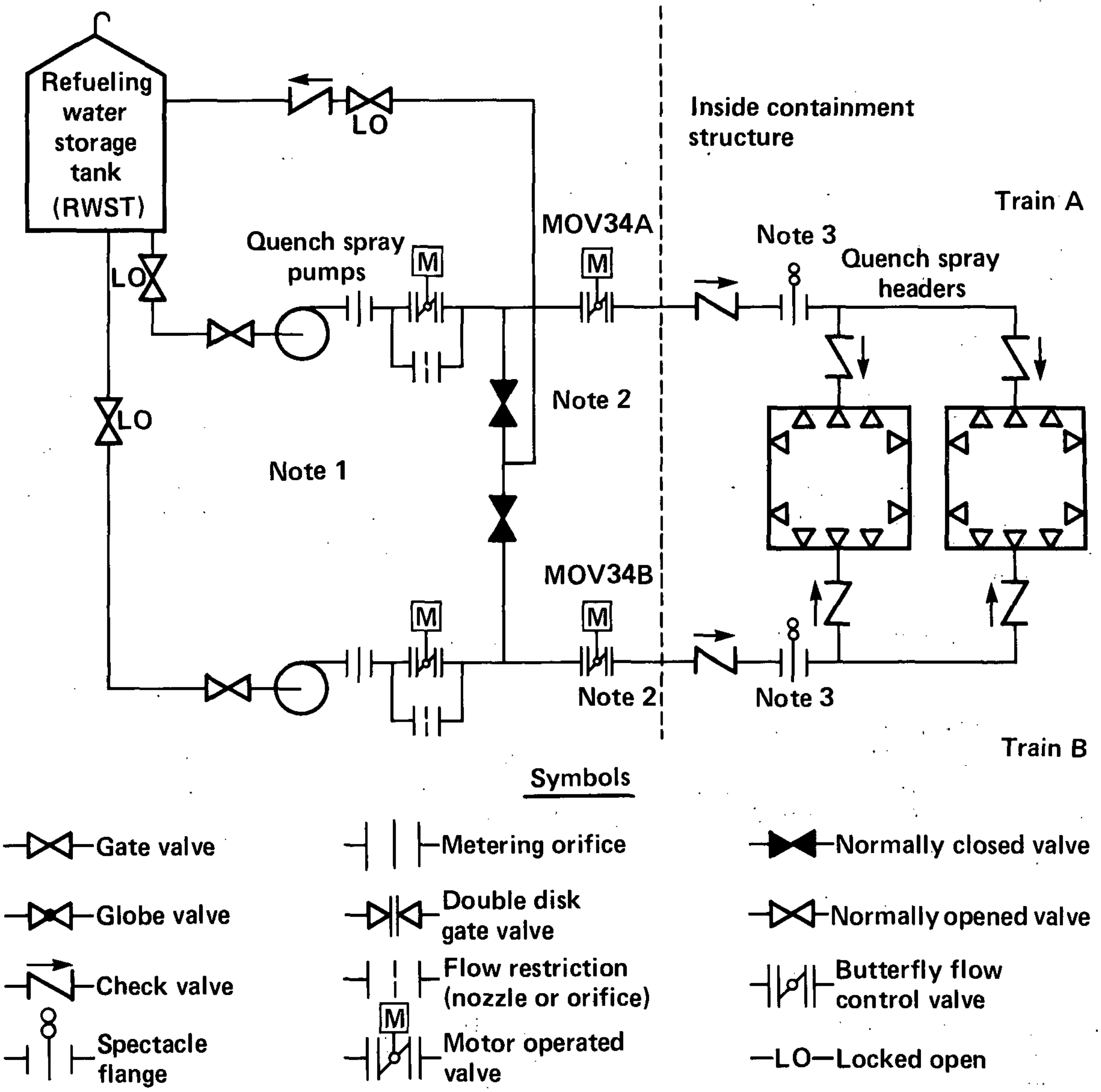
3.4.9 Quench Spray System

3.4.9.1 System Description

The quench spray system is designed to provide rapid, short-term quenching of steam released from pipe breaks within containment. The system consists of two identical trains, each of which contain a quench spray pump. These pumps feed two ring headers near the containment dome. The quench spray pumps take suction from the refueling water storage tank (RWST).

The quench spray system is initiated by a containment depressurization actuation (CDA) signal that results from coincident high containment pressure signals. The quench spray system is automatically terminated by a low level switch in the RWST. NaOH is added to the spray water in order to maintain a minimum pH and thus prevent long-term corrosion of stainless steel inside the containment once quench spray has been actuated.

The quench spray system in conjunction with the containment recirculation system is used to maintain the integrity of the containment structure. Following a major primary or secondary pipe rupture inside containment, the system returns the containment to subatmospheric pressure by removing heat from the containment atmosphere. Figure 3.4.9-1 provides a schematic view of the quench spray system.



Notes:

1. Vent, drain, and leakage monitoring lines not shown.
2. Valve is closed during normal plant operation.
3. Spectacle flange is at open position during normal plant operation.

Fig. 3.4.9-1 Quench spray system.

3.4.9.2 System Fault Tree

The quench spray fault tree models the capability of the two pumps to start and run and the availability of various valves to open on demand. In preparing the system fault tree, the Millstone team gave consideration to the impact of independent component failures, test and maintenance, common-cause failure, and human errors. We have reviewed the fault tree and found it to be accurate, complete, and valid with minor exceptions discussed below.

The quench spray system fault tree was quantified for two cases in order to represent the effects of the eight plant support states. These cases are:

Case A: Two trains of AC power available, corresponding to support states 1 and 5.

Case B: One train of AC power available, corresponding to support states 2 and 6.

For support states 3, 4, 7 and 8 the quench spray system is unavailable (Q=1). For case A, the unavailability of the quench spray is 3.2E-4 with a variance of 1.0E-7 and for case B the calculated unavailability is 8.2E-3 with a variance of 5.6E-5.

When both trains of AC power are available, the dominant contributor to quench spray unavailability is common-cause failures. Common-cause makes up 70% of the system unavailability. Most of this is associated with common mode failures of both pumps to start and includes factors such as common design errors, common actuating logic, and common test and maintenance procedures. Much of the remaining common-cause unavailability comes from the two motor-operated discharge valves (MOV34A and MOV34B). Other contributors to overall unvailability are ESF logic (9%), pump faults (3%), and failures in the motor-operated discharge values (2%). The residual unavailability comes from cross-train component failures.

When only one train of the quench spray system is available, the major contributors to unavailability are pump failure to start (28%), pump hardware faults (17%), motor-operated discharge valve failure to open (26%), motor-operated discharge value failure to remain open (12%), and check valve failures (12.7). Table 3.4.9-1 summarizes the major contributors to quench spray system unavailability for cases A and B.

Four sets of common-cause failure are used to calculate the common-cause unavailability of the quench spray system. These are:

(1) failure of the quench spray pumps in Trains A and B to start

(2) failure of the quench spray pumps in Trains the A and B to run

(3) failure of the motor-operated valves in Trains A and B to open and allow spray discharge through the ring headers

(4) failure of the motor-operated valves in Trains A and B to remain open

Common-cause calculations for the quench spray system assume a binomial failure rate model. This failure rate model is described in Appendix 2-C of

Table 3.4.9-1 Quench spray unavailability.

Dominant contributors		Unavailability (failure/demand)
Case A:		
Common-cause		2.24E-4
ESF actuation logic		3.00E-5
Pump faults		9.60E-6
Faults in one of the motor-operated valves MOV34A MOV34B and in one pump in an opposite train		9.80E-6
Faults in the MOV34A and MOV34B		6.40E-6
Other faults		4.00E-5
	Total	3.20E-4
Case B:		
Pump failure to start		2.30E-3
Failure of motor-operated valve MOV34A to open		3.13E-3
Pump hardware faults		1.40E-3
Failure of motor-operated valve to remain open		9.84E-4
Check valve faults		9.84E-4
Other faults		4.02E-4
	Total	8.20E-3

the Millstone PSS and reviewed in Section 3.10 of this report. Contributions to each failure mode from actuation logic are included in the individual binomial failure rates for the components.

Two additional common-cause failures were considered, but judged by the PSS authors to be insignificant contributors to unavailability: these are (1) freezing of the RWST and quench spray lines and (2) common-cause failures of pairs of check valves.

There are three human errors which are included in the quench system fault tree as contributors to system unavailability: these are (1) failure to properly close the gate valves (valves 36 and 37 on Fig. 3.4.9-1) in the pump test line following test or maintenance, (2) failure to restore the locked open gate valves (28 and 29) following tests of the motor-operated discharge valves (40 and 41), and (3) failure to restore the quench spray actuation of the ESF logic following its test.

3.4.9.3 Comments on the Quench Spray Fault Tree

Our review of the quench spray system fault tree indicates that it is accurate, complete, and valid with only minor reservations. One question is why the effect of test and maintenance on the motor-operated discharge valves MOV34A and MOV34B (valves 40 and 41 on the P and ID) was not modeled in the fault tree. Another concern involves the exclusion of freezing RWST and quench spray lines and common-cause failures of pairs of check valves from the list of categories. There have been licensee event reports that involve freezing of the RWST lines. However, our major concern is not that these could be significant contributors to risk but that the authors judged these modes as insignificant contributors without demonstrating this quantitatively. Finally, it is interesting that failure of RWST cooling water is not modeled. It seems clear that, although this system is not necessary for proper functioning of the RWST, its failure would effect containment performance during LOCA accidents. We feel that some estimate of chilled water system availability would be useful in making an accurate assessment of damage states or accident recovery.

3.4.10 Safety Injection Pump Cooling System

3.4.10.1 System Description

The purpose of the safety injection pump cooling system is to cool the bearing oil of the safety injection pumps. It is a safety-related system and a critical support system for the high pressure safety injection system. The system is made up of two safety injection pump cooling pumps, two safety injection pump oil coolers, two heat exchangers, and a shared cooling surge tank. Each safety injection pump has dedicated cooling pump, heat exchanger, and oil cooler. The heat exchanger interfaces with the service water system. The surge tank is supplied by the reactor plant component cooling water. Normally, the safety injection pump cooling system is not in operation. It is designed to start automatically when the associated safety injection pump starts.

3.4.10.2 System Fault Tree

The system fault tree was used to model the unavailability of safety injection pump cooling in a single train. The calculated unavailability of each train is 7.32E-3 per demand. Pump faults contribute 96% of the overall system unavailability. Furthermore, actuation system faults are associated with 36% of the unavailability, loss of control power to the pump circuit breaker contributes 32%, and hardware faults contribute 20%. Residual unavailability for each train is due to piping faults, heat exchanger faults and check valve faults. Table 3.4.10-1 summarizes the dominant cut sets that contribute to overall unavailability of the safety injection pump cooling system.

Table 3.4.10-1 Dominant cut sets in the PSS for the safety injection pump cooling system.

Component cut set	Probability (failure/demand)
Motor-driven pump actuation circuit fault	2.60E-3
Loss of control power to circuit breaker or pump	2.34E-3
Failure of motor-driven pump to start and run	1.49E-3
Failures of bus circuit breaker	2.43E-4
Check valve failure	3.20E-4
Motor-driven pump trip circuit faults	2.34E-4
Other faults	1.30E-5
Total	7.32E-3

Unavailability of both pump cooling systems is only a consideration when AC power and service water is available to both trains. In this case, common-cause failure dominates the calculated unavailability of both systems. The common-cause unavailability contribution from the safety injection pump cooling system to the high pressure safety injection system is calculated to be 1.43E-4.

The safety injection pump cooling pumps are tested monthly on a staggered basis. However, the system is not unavailable during tests. All components that can be isolated and are outside containment are maintained as necessary on an unscheduled basis. Maintenance unavailability estimates for the high pressure injection system includes contributions from maintenance on the safety injection pump cooling system.

Consideration of human errors resulted in the conclusion that no human errors were judged credible for the safety injection pump cooling system.

3.4.10.3 Comments

Our review of the safety injection pump cooling system revealed no significant omissions or problems. Nonetheless, the fault tree was remiss in some general areas. Pump capacities, water source requirements, and power requirements were not fully described. The system success criteria were not fully described. PSS Table 2.23.2.10.3-1 lists the mission time for the motor-operated pump as three hours. However, the basis for this value is not presented. It should be noted that failure of this system when both trains are available is dominated by common-cause failures.

3.4.11 Charging Pump Cooling

3.4.11.1 System Description

The charging pump cooling system is a safety-related system that cools gear and bearing oil of the charging pumps. This system is essential for the operating of the charging pumps and thus necessary to mitigate the consequences of a loss-of-coolant accident. The system consists of two charging pump cooling pumps, two heat exchangers which transfer heat from the cooling system to the service water, three charging pump oil coolers, and a shared surge tank. One of the cooling pumps is normally running while the other is on standby. In the event of a safety injection signal or loss of power signal, the standby pump automatically starts. In addition, when the standby pump is running, the isolation valves are aligned so that each cooling pump and heat exchanger is dedicated to one charging pump.

3.4.11.2 System Fault Tree

The system fault tree was used to model the effect of charging pump cooling system unavailability on the unavailability of the high pressure safety injection system (HPSI). One fault tree was used for both trains of the charging pump cooling system. However, different calculations were used for component unavailabilities in the train of charging pump cooling in which the cooling pump is operating (Train A) and the standby train (Train B). For loss of offsite power events (support state 5), both systems were modeled in standby.

The calculated unavailability for the operating train was calculated to be 5.3E-4 per demand. The dominant cut sets for this train are listed in Table 3.4.11-1. Check valve faults contribute 60% to unavailability and failures of the motor-driven pump to run contribute 28%. Unavailability of the standby train was determined to be 1.2E-2. The dominant cut sets for this system are also listed in Table 3.4.11-1. Ninety-eight percent of the unavailability is due to faults in the motor-driven pump. These are further composed of 41% contribution from circuit faults, 22% from actuation system faults, 20% from loss of central power to the pump circuit breaker, 13% from pump hardware faults, and 2% from circuit breaker hardware faults.

Common-cause failures are determined for support states 1 and 5 (AC and service water available to both trains). For all other support states, only one train of charging pump coding is available. The common-cause calculations for the charging pump cooling system assume a binomial failure rate model. For support state 1 (all systems available), the calculated unavailability of both cooling trains is 3.6E-6. The unavailability for support state 4 (loss of offsite power) is 5.4E-5.

The charging pump cooling pumps are tested monthly on a staggered basis. All isolable components outside of containment are assumed to be maintained as necessary on an unscheduled basis. The cooling system unavailability as a result of maintenance has been incorporated into the maintenance unavailability of the charging pumps.

Table 3.4.11-1 Dominant cut sets in the PSS for the charging pump cooling system.

Component failure		Probability (failure/demand)
Operating train		
Check valve failure to operate		3.2E-4
Motor-driven pump failure to run		1.46E-4
Trip circuit faults on motor-driven pump		4.01E-5
Loss of control power to circuit breaker on motor-driven pump		1.95E-5
	Total	5.3E-4
Standby train		
Trip circuit faults on motor-driven pump		4.83E-3
Actuation system faults for motor-driven pump		2.6E-3
Loss of control power to circuit breaker on motor-driven pump		2.34E-3
Motor-driven pump failure to start and run		1.49E-3
Bus circuit breaker failure to close		3.38E-4
Check valve failure		3.4E-4
	Total	1.19E-2

No human errors were judged to be credible for the charging pump cooling system.

3.4.11.3 Comments

Our review of the charging pump cooling system fault tree identified some items of note. There is an inconsistency in the failure probability listed in the input table and the value listed for the same component in the list of cut sets. The pump trip circuit for both the operating and standby pumps is calculated to have a component failure probability of 2.34E-4. Nonetheless, the cut sets for this component list its failure probability as 4.01E-5 for the operating train and 4.83E-3 for the standby train. The reason for the difference is not discussed.

It should be noted that for the charging pump cooling system, the unavailability of both trains due to random failures is greater than that due to common-cause. For support state 5 (no offsite power), the unavailability of both trains of the charging pump cooling system due to random failures is 1.42E-4, which is roughly a factor of 2 larger than the common-cause unavailability (5.40E-5). When offsite power is available (support state 1), the unavailability of both trains due to random failures is 6.3E-6 and that due to common-cause is 3.6E-6. These deficiencies are considered relatively minor when compared to the overall failure rate of the charging pump cooling system.

3.4.12 Low Pressure Recirculation System

3.4.12.1 System Description

The low pressure recirculation system is an engineered safeguards system that is designed to provide long-term core coverage and decay heat removal following a medium or large LOCA.

The low pressure recirculation system becomes functional in the latter phase of a LOCA. The system is designed to operate in two modes: spray mode and safety injection mode. The system takes suction from the containment sump and pumps it through coolers (cooled by service water) to the contanment recirculation headers (spray mode) and/or to the reactor coolant system (safety injection mode). The spray mode of operation is actuated automatically on high high containment pressure. The safety injection mode of operation is actuated manually from the main control board. The system then remains in long-term operation after an accident until terminated by administrative control.

3.4.12.2 System Fault Tree

The fault tree was developed in accordance with the system success criteria which require delivery of coolant flow from one containment recirculation pump to at least one intact reactor coolant loop following a large or medium LOCA.

Operator action is required to isolate flow to the spray headers, secure the refueling water storage tank (RWST), and align valves for injection to the reactor coolant system (RCS). These operator actions have been explicitly modeled in the fault tree.

The low pressure recirculation system fault tree was quantified for two cases in order to represent the effects of the eight support states. Case 1 addresses situations in which both trains of AC power are available and corresponds to support states 1 and 5. Case 2 addresses situations wherein only one train of AC power is available and corresponds to support states 2 and 6. For cases corresponding to support states 3, 4, 7, and 8, the low pressure recirculation system is unavailable. Table 3.4.12-1 summarizes the calculated unavailability of this system for each of the eight support states.

The calculated system unavailability for case 1 is 3.0E-3. Common-cause failure is the dominant contributor and accounts for 18% of the total unavailability. The dominant random failure contributor was found to be plugging of the service water motor-operated butterfly valves. Coincident failure of these valves accounts for 6% of the total system unavailability. The remaining unavailability is made up of hundreds of two-element cut sets.

The calculated system unavailability for case 2 is 4.9E-2. Of this, approximately 26% is due to the single failure of a motor-operated service water isolation valve on one of the containment cooling heat exchangers. The unavailability of this valve is the result of flow tests during refueling. Local faults of other valves account for an additional 33% of system unavailability.

Contributions from test and maintenance, common-cause failure, and human error were included in the system fault tree.

3.4.12.3 Comments

No significant problems were found regarding the accuracy, completeness, and validity of the fault tree analysis for the low pressure recirculation system.

3.4.13 High Pressure Recirculation System

3.4.13.1 System Description

High pressure recirculation is an operational mode in which the charging and safety injection pumps are aligned in series, or "piggy-back operation", with the containment recirculation system (CRS) pumps. These engineered safeguards systems act to maintain long-term reactor coolant system inventory while removing decay heat during recovery from a small or medium-sized LOCA.

Table 3.4.12-1 Low pressure recirculation system unavailability results in the PSS.

Support state	System unavailability (failure/demand)
1	3.0E-3
2	4.9E-2
3	1.0
4	1.0
5	3.0E-3
6	4.9E-2
7	1.0
8	1.0

The recirculation pumps take suction from water in the containment sump and pump it through heat exchangers to the suction of the high pressure pumps, which inject to the RCS. Alignment of valves is performed manually at the main control board when indications of low low RWST level and automatic shutoff of the RHR pumps are received.

3.4.13.2 System Fault Tree

The fault tree for the high pressure recirculation system (HPRS) was used to calculate its unavailability in terms of the system success criterion. This criterion specifies that coolant flow be delivered to two of three intact reactor coolant loops from one of four pumps (two charging pumps and two HPSI pumps) by taking suction from one of two recirculation pumps. Component unavailability for system operation was analyzed for the initial phase of coolant recirculation following a LOCA. The analysis assumed a total run time of 24 hours just prior to recirculation switchover to the hot legs of the reactor coolant system. The analysis also assumed successful operation of the HPSI pump during the injection phase of emergency core cooling.

Operator action is required to initiate high pressure injection recirculation flow. The operator must isolate flow to the spray headers from the two recirculation pumps and align the discharge of these pumps to the suction of the charging and safety injection pumps. This is accomplished by opening isolation valves in the cross-connect lines that link the suction lines of the charging pumps with those of the safety injection pumps. At the same time, the operator must close isolation valves that tie the suction of these pumps to the refueling water storage tank (RWST). The closing and opening of the isolation valves by the operator was modeled in the system fault trees.

The HPRS system fault tree was quantified for two cases in order to represent the effects of the eight support states. Case 1 addresses situations in which both trains of ESF AC power and both trains of service water are available and corresponds to support states 1 and 5. Case 2 addresses situations in which only one train of ESF AC power is available and corresponds to support states 2 and 6. The HPRS is unavailable in support states 3, 4, and 8. Table 3.4.13-1 summarizes the calculated unavailability of the HPRS for each of the eight support states.

The calculated system unavailability for case 1 is 5.85E-3 per demand. Common-cause is the dominant contributor, making up approximately 30% of the total. Random failures of motorized valves in the service water system is the next most dominant contributor. At least one of these valves must open to admit service water into its associated containment recirculation cooler. Coincident failure of both valves failing closed accounts for 3% of total system unavailability. Mechanical failure of either valve coincident with failure of some other HPRS component accounts for an additional 10% of total system unavailability. The remaining unavailability is made up of hundreds of two-element cut sets.

The calculated system unavailability for case 2 is 5.84E-2 per demand. Approximately 19% of the total is due to the single failure of a motor-operated service water isolation valve on one of the containment cooling heat exchangers. An additional 32% of system unavailability is due to failure of any one of seven motorized valves in the system to change state to its required accident position. The residual system unavailability is made up of

Table 3.4.13-1 High pressure recirculation system unavailability results in the PSS.

Support state	System unavailability (failure/demand)
1	5.85E-3
2	5.84E-2
3	1.0
4	1.0
5	5.85E-3
6	5.84E-2
7	1.0
8	1.0

other single component random failures, including failure of the containment spray pump to start and run and failure of an operator to open two motorized valves.

3.4.13.3 Comments on the HPRS System Fault Tree

The fault tree for the HPRS system was generally accurate, complete, and valid except for assumptions made in the common-cause calculations. These assumptions require scrutiny since common-cause is a major contributor to system unavailability.

The common-cause failure analysis for the HPRS system required an understanding of which combinations of components (or trains) are common and which are diverse. In order to carry out the analysis, the PSS makes the following asumptions regarding the commonality of components:

(1) The HPSI pump trains are claimed to be diverse from the charging pump trains because the charging pumps are operating-type pumps, whereas the HPSI pumps are standby-type pumps. It is not clear why this makes them diverse.

(2) Motor-operated gate valves (MOGV) are assumed to be alike and subject to common-cause failure.

(3) Motor-operated globe valves (MOGLV) are assumed to be alike and subject to common-cause failure.

(4) Motor-operated butterfly valves (MOBV) are assumed to be alike and subject to common-cause failure.

(5) Motor-operated gate, globe, and butterfly valves are assumed diverse from each other and <u>not</u> subject to common-cause failure.

(6) No common-cause potential is assumed to exist between containment recirculation pumps and either HPSI or charging pumps because of the significant differences in the pump design. However, this assumption does not recognize such things as common environment or common maintenance errors.

(7) No common-cause potential is assumed to exist for redundant pairs of check valves failing to open in high pressure systems. Licensee event reports indicate that this may not be the case.

(8) The contribution to common-cause failure due to plugging of the sump screens was assumed to be negligible when compared to other common-cause contributors.

Although no supportive basis was given for these assumptions, none appear to be particularly significant. Several of these assumptions are questionable, e.g., no common-cause failures in check valves. The most likely cause for such failures would appear to be corrosion effects or design defects, both of which are potentially common-cause effects (Ref. 3.4-2). Furthermore, the analysis of recirculation apparently assumed that all injection trains had succeeded, so that the PSS missed contributions to unavailability from one train failing in injection and the other in recirculation.

3.4.14 Containment Recirculation Spray System

3.4.14.1 System Description

The containment recirculation spray system is designed to provide long-term removal of heat from the containment atmosphere following a LOCA or steamline break inside containment. This system operates in conjunction with the quench spray system to restore the containment to subatmospheric pressure.

The containment recirculation spray system consists of two 100-percent capacity trains which are each connected to both of the ring spray headers inside containment. Each train has one pump and two each of the following items: a normally open containment sump suction isolation valve, recirculation pump, heat exchanger, and a normally open spray header isolation valve. Pump operation and valve opening are automatically actuated on "high 3" containment pressure after a five-minute time delay. This delay is provided to ensure an adequate supply of water in the sump for pump operation.

3.4.14.2 System Fault Tree

The system fault tree was used to calculate the failure to achieve system success criteria which is to deliver sufficient recirculation flow to one of two containment spray headers.

The effects of test and maintenance and common-cause are considered in the fault tree model. The analysis assumes that testing will not contribute to system unavailability of the containment recirculation spray. This is based on the observation that sufficient time will be available, between the onset of an accident and the time when the system is actually needed, for an operator to remove a component from test and place it in the required operating mode. The only maintenance included in the system fault tree is that of the recirculation pumps. Common-cause failures are modeled using the binomial failure rate model.

The system fault tree was quantified for two cases in order to represent the effects of the eight plant support states. Case 1 addresses situations in which both trains of AC power are available and corresponds to support states 1 and 5. Case 2 addresses situations in which only one train of AC power is available and corresponds to support states 2 and 6. The containment recirculation spray system is unavailable in support states 3, 4, 7, and 8. Table 3.4.14-1 summarizes the calculated unavailabilities of the recirculation spray system for each support states.

In case 1, the dominant contributor to system unavailability is common-cause, accounting for 28% of the total. The dominant random failure contributor to system unavailability was found to be local faults resulting in plugging of service water motor-operated valves. Coincident failure of these valves accounts for 8% of the total system unavailability. The residual unavailability is made up of hundreds of two-element cut sets such as failure of a pump in one train while a motor-operated valve in the opposite train fails to open.

In case 2, the dominant contributor to system unavailability is failure of the service water containment cooler isolation valve, accounting for 34% of the total system unavailability. The large unavailability associated with this value results from the length of the interval between flow tests. The valve is tested only during refueling outages.

3.4.14.3 Comments on the System Fault Tree

For the most part, the containment recirculation spray system fault tree was found to be accurate, complete and valid. Failure of this system when both trains are available is dominated by common-cause failures. However, in the discussion of common-cause failures in the PSS, the plugging failure of containment sprays was identified as a noncredible event and thus was not included in the analysis. It is of concern that this exclusion was made without providing a qualititative or quantitative analysis which would indicate why common-cause plugging is not a contributor to system failure.

3.4.15 Service Water System

3.4.15.1 System Description

The service water system (SWS) is a major plant support system. It cools a number of important emergency and normal system heat loads. The systems relying on the service water system for cooling include:

- auxiliary feedwater emergency makeup
- charging pump cooling system
- containment recirculation coolers
- containment recirculation pump vent units
- control building chillwater backup
- control building air conditioning water chillers
- emergency diesel generator coolers

Table 3.4.14-1 Containment recirculation spray system unavailability results in the PSS.

Support state	System unavailability (failure/demand)
1	2.0E-3
2	3.8E-2
3	1.0
4	1.0
5	2.0E-3
6	3.8E-2
7	1.0
8	1.0

- emergency diesel generator coolers
- emergency spent fuel pool makeup
- lube water to circulating water pumps
- MCC and rod control area air conditioning units
- post accident liquid sample cooler
- RHR pump vent units
- RPCCW heat exchangers
- safety injection pump cooling
- service water pumps lubricating water
- TPCCW heat exchangers

The service water system consists of two trains, each of which contains an inservice pump and a standby pump. The standby pumps are blocked on the discharge side by normally closed, motor-operated valves. Each pump is used in the service mode 50% of the time and in the standby mode the remainder of the time. If an inservice pump fails, the drop in pressure downstream of the pump is sensed and the corresponding standby pump is automatically started. The MOV downstream of the standby pump receives an opening signal as well.

3.4.15.2 System Fault Tree

The service water system fault tree was used to calculate the probability that the system fails to feed emergency loads. The fault tree model includes the effects of maintenance and common-cause failures on system unavailability. Test unavailability was not modeled because there are no formal tests on the system. Common-cause failures are modeled using the binomial failure rate model. The study identified no human errors that could significantly compromise system availability.

The service water fault tree was quantified for four cases. These four cases and the calculated unavailability for each case is summarized in Table 3.4.15-1.

For cases 1 and 3, the dominant contributor to system unavailability is strainer plugging due to common-cause. This failure is responsible for essentially 100% of the system unavailability in these two cases.

The dominant contributor to system unavailability for case 2 is also strainer plugging, responsible for 30% of the unavailability. The remainder of the unavailability is attributable to a number of random failure cut sets, none of which contributes more than 8.1% to the total unavailability.

The dominant cut set for case 3 is the random failure loss of DC control power to the pumps circuit breakers which prevents both pumps from starting. This contributes 67% of the total unavailability. The residual unavailability is made up of many cut sets, each of which contributes no more than 4%. Common-cause failure due to strainer plugging is responsible for 4% of the unavailability.

3.4.15.3 Comments on the Service Water System Fault Tree

Our review of the service water system fault tree identified a number of concerns regarding the accuracy, completeness, and validity of the analysis. These concerns are enumerated in the paragraphs below.

PSS page 2.33.15-2 states that the "potential diversion paths" to turbine plant and reactor plant component cooling heat exchangers are not considered the SWS fault tree. They are stated to be included in the "recirculation cooling system fault tree." It is not clear what "diversion flow" means, or its consequence. Further, there is no fault tree analysis provided for any system entitled "recirculation cooling."

It is stated on page 2.3.3.15-2 of the PSS that "significant potential for blockage of the (SWS) strainers exists upstream of the service water pumps." Indeed, strainer plugging was subsequently found to be the major contributor to SWS failure for cases 1, 2, and 3. However, on page 1-D-4 (PSS Appendix 1-D, Volume 2), the common-cause strainer plugging failure was ruled out, apparently based on (1) automatic backwash capability, (2) high pressure differential alarms in the control room, and (3) greatly reduced intake water flow should one train fail. The probability of total loss of the service water system was subsequently determined to be 8.68E-12/hour in Appendix 1-D (page 1-D-5). However, the results in Table 2.4.15-1 indicate that the failure rate is 3.1E-7/hour (assuming a 24-hour mission time).

The SWS failure considered in PSS Section 2.3.3.15 was only for the case where SWS is required after an accident has been initiated by other means. A 24-hour mission time was assumed, yielding a failure rate of (3.1E-7/hour) (24 hours) = 7.44E-6. Actually, the mission time required could be much longer, since core cooling is needed for several weeks if the plant remains in a shutdown condition following sustained power operation.

Another concern regards the neglect to treat SWS failure as an initiating event in light of the fault tree results. If SWS fails, the plant would trip, and it appears the only available core heat removal system is auxiliary

Table 3.4.15-1 System unavailabilities in the PSS for service water system.

Description	Unavailability (failure/demand)
Case 1: AC power available to both buses Offsite power available to both buses	7.44E-6
Case 2: AC power available to both buses Offsite power available to both buses One train of service water available	2.47E-5
Case 3: AC power available to both buses No offsite power available	7.44E-6
Case 4: AC power available to one bus No offsite power available One train of service water available	1.80E-4

feedwater if there are no dependencies between SWS and AFWS (also see PSS page 1-D-5). While there appear to be no direct dependencies, this should be clearly demonstrated. For example, the SWS provides cooling for the component cooling system (PSS Fig. 2.3.3.15.2-1), which in some plants provides cooling to AFS pumps, lubricating oil, or pump rooms. We did not identify dependencies of this type in MP 3.

In any event, the possibility of SWS failure was considered in PSS Appendix 1-D and dismissed due to the extremely low probability (based on the 9.68E-12/hr failure rate) and independence from the AFWS. If the PSS Section 2.3.3.15 failure rate of 3.1E-7/hr is used, the annual failure probability is 2.72E-2/yr. If the AFWS is assumed to be independent of the SWS, the core melt probability would be:

$$(2.71E-2)(6.8E-5) = 1.8E-6/\text{year} \qquad (3-4)$$

This result would not be a dominant contributor to the core melt probability (total = 4.5E-5). This assumes, of course, that there are no SWS-AFWS dependencies and that the AFWS failure probability is correctly assessed in PSS Section 2.3.3.5. As indicated previously, the AFWS failure probability appears optimistic, especially early in the plant operating life.

Also at issue in this asssessment is the choice of a realistic value for service water failure given the substantial difference between the results in PSS Appendix 1-D and the results in Section 2.3.15. In attempting to resolve this issue we reviewed a recent ORNL report on service water system events (Ref. 3.4-4). In the ORNL report, 16 events involving service water systems were found, including two events involving strainer plugging during the January 1979 through June 1981 time period. In one case, total loss of service water did occur but the function was eventually restored by use of other systems. The ORNL report concludes that screens and filters in SWS are susceptible to clogging whether or not self-cleaning mechanisms are used. These results would tend to indicate a failure rate closer to the PSS Section 2.3.3.15 value than Appendix 1-D. Thus, since the service water system cools a large number of normally operating and emergency equipment, sustained SWS failure could initiate a core melt if either, (1) auxiliary feedwater fails independently, or (2) a reactor coolant pump seal LOCA occurs as a result of the SWS failure (see Section 3.6.2 for additional discussion).

3.4.16 Vital DC System

The fault tree was not formally included in the main text of the Millstone PSS. However, a fault tree for this system was developed in Appendix 1-E for input to the initiating events analysis. We are reviewing this system here because it is an important support system for the loss of offsite power and because the results of the vital DC fault tree are used in other fault trees as a basic event.

3.4.16.1 System Description

The vital DC buses provide essential DC loads to normal and safety-related equipment. The DC power system has six separate systems - two normal DC power systems serving non-safety-related loads and four Class IE DC power systems serving safety-related loads.

The Class IE DC power is divided into four separate channels. Two channels are devoted exclusively to supplying power to an associated 120 AC vital bus, VIAC-3 and VIAC-4, in the event of a loss of power on these buses. The other two channels, in addition to being able to supply vital 120 AC buses VIAC-1 and VIAC-2, also supply other safety-related DC loads. The redundancy of the system is such that modeling the failure of the two DC buses supplying VIAC-1 and VIAC-2 essentially corresponds to a model of the failure of all DC power.

The class IE 125V DC power system equipment for each channel consists of one operating battery charger, one spare battery charger shared by two channels of the same train, one 125V DC battery, and one distribution switchboard. On each of the two channels that also supply other safety-related DC loads, additional distribution panels are included. Figure 3.4.16-1 provides a simplified line drawing of the vital DC bus 125-VDC-1 that was used for the system fault tree.

The source of power to each of the four Class IE 125V DC bus channels is supplied from either its associated battery charger or battery. The battery charger is powered by the emergency 480V bus corresponding to that train. Each set of two 125V DC buses has one spare battery charger to serve as a backup for the two operating battery chargers. This spare battery charger is connected to both buses of the set through normally opened circuit breakers which are key-interlocked to prevent inadvertent interconnection of both emergency 125V DC buses. The spare battery charger is powered from the associated train emergency 480VAC bus.

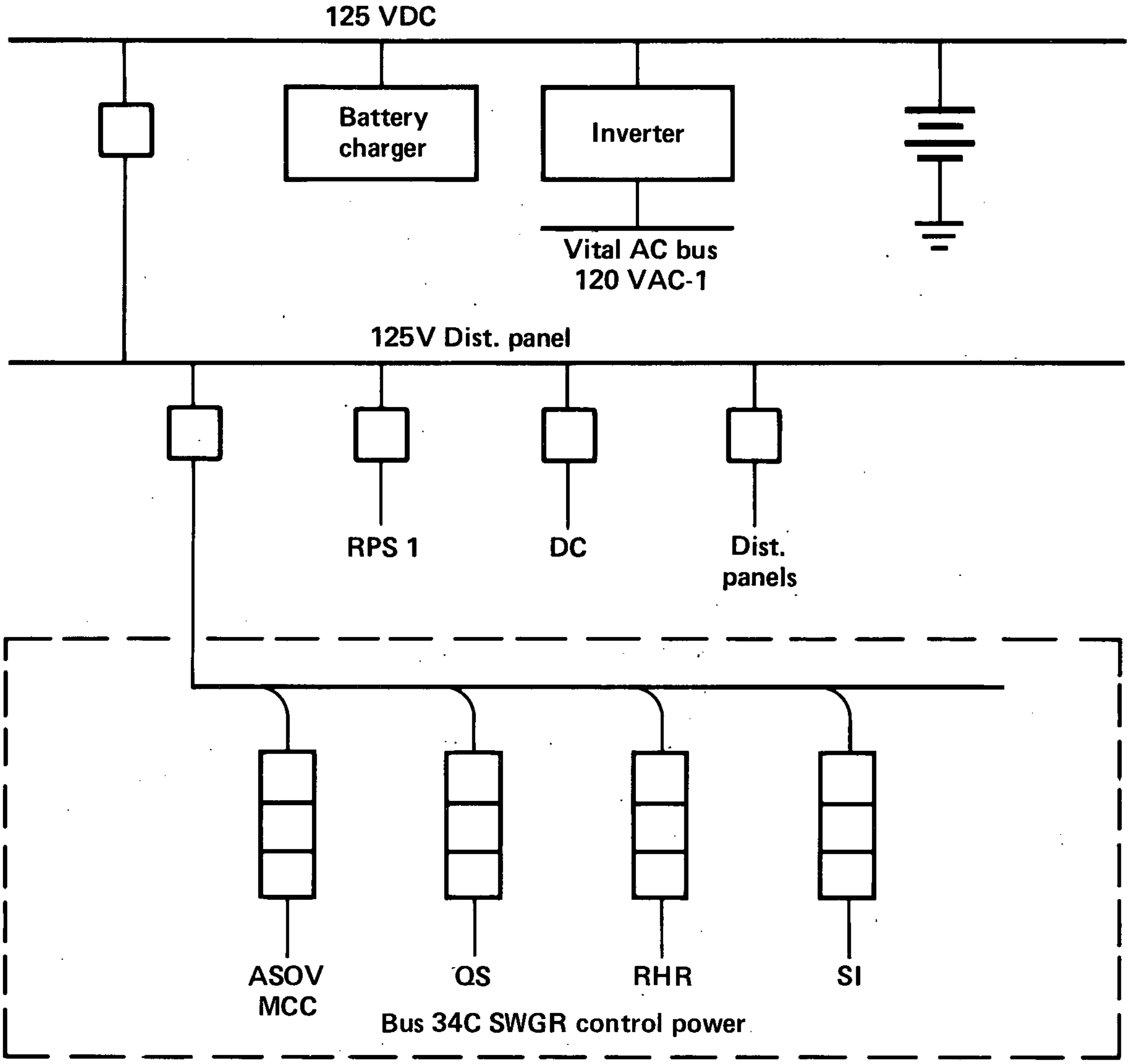


Fig. 3.4.16-1 Simplified diagram of vital DC bus 125-VDC-1.

3.4.16.2 System Fault Tree

The system fault tree model was used to quantify the frequency of failure of a single DC bus and the frequency of total DC power failure. The fault tree model including the 24-hour mission failure rates is shown in Fig. 3.4.16-2. The fault tree calculation provided a failure probability of 5.36E-6/day for losing a single bus. The frequency of losing any one of the two most critical DC buses (125-VDC-1 and 125-VDC-2) was quantified by doubling the failure probability of a single bus. This gives a failure frequency of 3.91E-3/year for losing one of the two critical buses.

The frequency of losing the entire vital DC power system was defined in the Millstone PSS as the frequency of losing a second vital DC source given that the other vital DC source is already in an unavailable state. This failure rate is calculated using a time-dependent reliability model which includes a time-dependent recovery model. The recovery model assumes there is a 0.34 probability that a single channel will be recovered within 20 minutes and a probability of 1.0 that a single channel will be recovered within 24 hours. The calculated frequency for losing all DC power is 1.4E-8/year. This model treated the two channels as completely independent. No allowance was made for common-cause failures. In addition, the system fault tree for vital DC does not account for unavailability due to human error. The exclusion of these factors limits the utility of the fault tree for estimating the frequency of damage states initiated by vital DC failures. Because of the modeling uncertainty involved in the vital DC fault tree, it is possible that vital DC failures could be a significant but unquantified contributor to core melt.

3.4.16.3 Comments on the Vital DC Fault Tree

Our review of the DC fault tree revealed problems regarding the accuracy, completeness, and validity of the system fault tree. These concerns are enumerated in the paragraphs below.

One concern involves the failure of the fault tree to model the unavailability on demand, given that there has been a loss of offsite power. The fault tree (Fig. 3.4.16-2) models the availability of DC power given that AC power is available in the vital AC. The structure of the tree does not allow the determination of DC unavailability given loss of offsite power. During the first few seconds of this event, the portion of the vital DC system which includes the batteries and the components that transmit power from the DC bus to the vital AC bus and the EGLS is a crucial subsystem whose failure could rapidly lead to potentially serious damage states (see Section 3.4.4).

Another issue concerns two questionable assumptions used in the determination of the failure rate for both DC channels. One is that there is no potential for common-cause failures in the DC system. The second involves allowing credit for the recovery of a single channel once it has failed. These assumptions result in much lower failure rates than would otherwise have been calculated. Although these issues could have required a requantification of the entire system, a comparison of the PSS value with the value in the ANO-1 IREP (Ref. 3.4-4) found it to be consistent, so that no requantification was necessary.

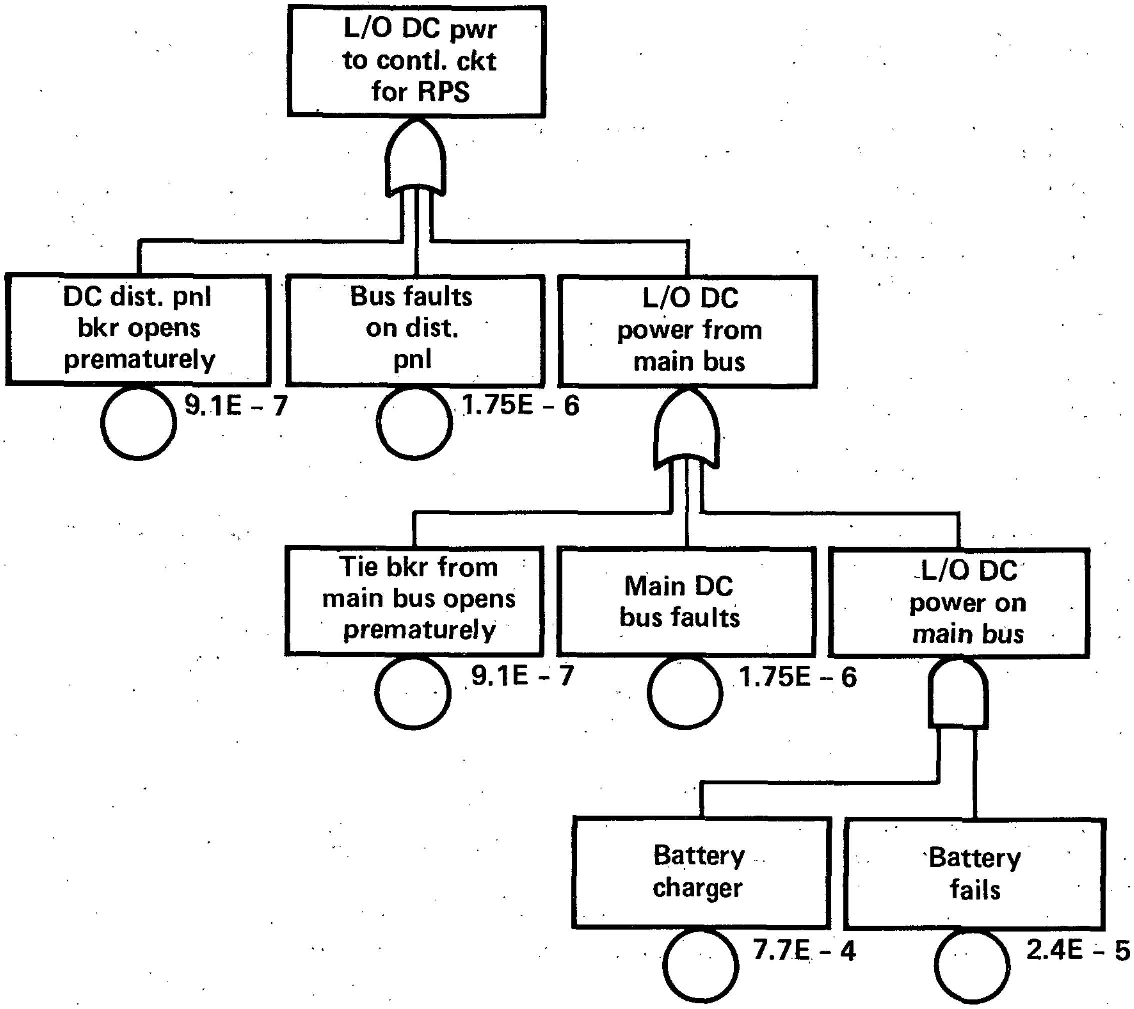


Fig. 3.4.16-2 Fault tree model of loss of vital DC bus.

3.4.17 General Comments Regarding the Millstone 3 System Fault Trees

In the preceeding subsections, we have provided a review of the systems descriptions and system fault trees from the Millstone 3 PSS. In general, we have found the fault trees to be accurate, complete and valid. Nevertheless, as was stated at the outset, notable system-specific exceptions have been identified and discussed in the preceding sections. We have also developed a number of general comments that apply to the systems analysis in general. These comments are taken up in the paragraphs below.

In general, we found system hardware and operational mode descriptions to be inadequate. Pump capacities, water source capacities, and power requirements are generally not provided. System success criteria are not always complete and nomenclature is sometimes inconsistent.

The report gives almost no consideration to time-dependent failures. The problem of higher system failure rates that are experienced early in the plant life ("wear-in" failures) is not addressed in the report. An example of particular relevance in this regard is the auxiliary feedwater (AF) system. The NRC has determined that well-designed, mature AF systems may have failure rates as low as 1.0E-5/year, while newer systems may have failure rates as high as 1.0E-3/year.

A mission time of 24 hours was assumed in the determination of system success. This value appears to be adequate for many systems. Nevertheless, it should be recognized that forced-convection cooling may be required for several weeks after shutdown to remove decay heat. This means that some systems, such as the RHR system and the service water system, may be needed for extended periods. PSS Appendix 1-A briefly considers accidents initiated from shutdown, but failure of heat removal systems is not included. The neglect of this issue deserves note as potentially limiting the completeness of the analysis.

Finally, many conservative assumptions were included in the systems analysis. Several of these are described on pages 2.3-3 and 2.3-4 of the Millstone PSS. We have not focused on these assumptions in our review nor have we attempted to quantify their impact on the results. Nevertheless, it is important that we acknowledge their existence.

3.4.18 References for Section 3.4

3.4-1 U.S. Nuclear Regulatory Commission, "Anticipated Transients Without Scram for Light Water Reactors", USNRC Report NUREG-0460, April 1978.

3.4-2 U. S. Nuclear Regulatory Commission, "Wear in Swing Check Valves," in USNRC Periodical Report "Power Reactor Events," Vol. 4, No. 1, May 1982.

3.4-3 J. A. Haried, Oak Ridge National Laboratory, "Evaluation of Events Involving Service Water Systems in Nuclear Power Plants," USNRC Report NUREG/CR-2797, November 1982.

3.4-4 G. J. Kolb et al., Sandia National Laboratories, "Interim Reliability Evaluation Program: Analysis of the Arkansas Nuclear One - Unit 1 Nuclear Power Plant," USNRC Report NUREG/CR-2787, June 1982.

3.5 Human Factors

The PSS considered a number of human actions in the analysis of Millstone Unit 3. These can be generally categorized into two types: actions in response to accident conditions and actions related to the unavailability of an individual component. Actions of the first type were included in the event trees. There are several different kinds. The major actions were direct operator response in accordance with procedures to diagnose plant conditions and perform the necessary actions to assure the performance of each safety function. Such included manual backup actuation of systems as required, included in the quantification of the top event to which it applied, and recovery of failed systems where possible, which was added to the event sequence analysis in a special additional step following the initial quantification.

Human actions of the second type are actions related to the unavailability of an individual component, due either to a failure to restore a component to service following test or maintenance, or to an error of omission or commission in the operation of a component in response to an accident. These actions were modeled directly in each system fault tree and were thus part of the system unavailability. We have reviewed the human factors analysis and have concluded that it was generally performed in a reasonable and consistent manner in keeping with the methods suggested in the NREP Procedures Guide, NUREG/CR-2815 (Ref. 3.5-1). A few things which should have been analyzed differently are discussed later in this section. In addition, it was necessary to add three operator actions to the analysis. The need for these actions is discussed in Sections 3.2.1.1 and 3.2.2.2 and their quantification, when not obvious, is discussed in this section. A summary description of all the operator actions analyzed is provided in Table 3.2-1. The review results are shown in Tables 3.5-1 and 3.5-2. Where there is a number in the "Review assessment" column of the tables, that number was used in any sequence requantification subsequently performed.

3.5.1 Operator Actions Modeled on the Event Trees

The PSS assumed that essentially all of these actions are dominated by cognitive error as opposed to procedural error. That is, the failure of the operator to make the correct diagnosis of the plant conditions and determine correctly given that the diagnosis is made. In general, this appears to be a sound assumption. Although there are no specific procedures for this plant, the Westinghouse Emergency Procedure Guidelines which pertain to these actions were reviewed, and run-throughs of selected operator actions were performed with plant operators in the control room. Almost without exception, the manipulative actions which the operator is required to make are simple, few in number (usually from one to four), and are performed on no more than two control panels using indicators which are also on those panels. These observations support the assumption that cognitive errors are dominant. The PSS generally utilized the cognitive error model in the NREP procedures guide for quantifying these errors, although there are some exceptions. The following sections discuss these differences. The time frames allocated to perform the various operator actions were also reviewed, since these form the basis for obtaining the quantitative values from the cognitive error model. These time frames are in keeping with those used in previous PRAs, which have shown that most operator responses are required in the 20- to 30-minute time

Table 3.5-1 Human Error Probabilities for operator actions in event trees.

Operator action[c]	Applicable event trees or analysis[d]	Time avail.[a]	Dominant fail.[b]	Human error probability	Review assessment
OA-1	ET03, ET15	30	C	1E-2	Ok
OA-1	ET02	20	C	2E-1	1E-1 (see Sec. 3.5.1.1)
OA-2	ET03, ET15	30	C	1E-2	OK
OA-3	ET03, ET06, ET15	30	C	1E-2	OK
OA-4	ET04	30	C	1E-2	OK
OA-5	ET04	10	C	5E-1	OK
OA-6	ET05				
	Support states 1, 5	30	C	1E-2	OK
	Support states 2, 3, 4, 6	60	C	1E-3	OK
OA-6'	ET06, ET13				
	Support states 1, 5	20	C	1E-1	OK
	Support states 2, 3, 4, 6	30	C	1E-2	OK
OA-7	ET07 - ET21 (ET14A)	30	C	1E-2	OK
OA-7'	ET14B	30	C	1E-2	OK
OA-8	ET22	60	C	1E-2	1E-3 (see Sec. 3.5.1.2)
OA-8'	ET22	10	C	1E-1	NA (see Sec. 3.5.1.2)
OA-8R	ET22	20	C	NA	1E-1 (see Sec. 3.5.1.2)
OA-9	ET15'	10	C	1E-1	5E-1 (see Sec. 3.5.1.3)
OA-10		∿19 hrs	C	NA	1E-4 (see Sec. 3.5.1.6)
OA-2-E		NA	P	NA	1E-3 (see Sec. 3.5.1.4)
OA-6-E		30	C	NA	1E-4 (see Sec. 3.5.1.5)
RT-3	ET22	1	C	1E-2	OK (see Sec. 3.5.1.7)
RT-4	ET22	1	C	1E-2	OK (see Sec. 3.5.1.7)
R-1	ET01 - ET04	60	C	1E-3	OK
R-2	ET02 - ET14, ET22	60	C	1E-3	OK
QS'	ET14B	60	C	1E-3	OK
ESF	ESF recovery, Sec. 2.2.6	30	C	1E-2	OK
SI	SI recovery, Sec. 2.2.3.4	NA	C	1E-1	OK
SBI	Consequential SBI, Sec. 2.2.3.5	30	C	1E-2	OK
SBO	Consequential SBO, Sec. 2.2.3.5	30	C	1E-2	OK
S2	Consequential S2, Sec. 2.2.3.5	10	C	5E-1	OK
SEQ	Fire analysis, Sec. 2.5	NA	P	1E-3	----
HP-2	Recovery analysis, Sec. 3.0	NA	C	1E-2	OK
OA-3	Recovery analysis, Sec. 3.0	NA	C	1E-2	OK
AFR	Recovery analysis, Sec. 3.0	60	C	1E-3	OK

[a] Time available in minutes unless otherwise noted.
[b] C = Cognitive error; P=procedural error
[c] These events are defined in Table 3.2.1.
[d] References in this column are to sections in the PSS.

Table 3.5-2. Human error probabilities for fault tree analysis human error rate.

Type of error	Operator error[c]	HEP per demand	Review assessment[a]
1. Omission	Failure to restore a manual valve to normal position after test or maintenance act.	1E-4	0.1 x $\frac{\text{Time between checks}}{\text{Time between manipulations}}$
2. Omission	Failure to restore a motor-driven pump or an air- or motor-operated valve to normal position after test or maintenance act.	1E-4	1E-4 (monthly) 3E-5 (quarterly)
3. Omission	Failure to restore an alarmed motor-driven pump or an air- or motor-operated valve to normal position after test or maintenance act.	1E-4	1E-4(monthly) 3E-5 (quarterly)
4. Procedural error/with recovery	Error of omission/ commission in operation of air- or motor-operated valve required for accident mitigation.	1E-4[b]	OK (see Sec. 3.5.2.2)
5. Procedural error/with recovery	Error of omission/ commission in operation of motor- or turbine-driven pump required for accident mitigation	1E-4[b]	OK (see Sec. 3.5.2.2)

[a] See Section 3.5.2.1.

[b] Data source: I. A. Papazoglou et al., Brookhaven National Laboratory, "National Reliability Evaluation Program (NREP) Procedures Guide," USNRC Report NUREG/CR-2815, Brookhaven Report BNL-NUREG-51559, Review Draft, June 21, 1982.

[c] Applicable to all ESF systems.

frame. Those events in the PSS with shorter or longer time frames appear to be reasonable. The PSS and review values for these events are shown in Table 3.5.1. The events are defined on Table 3.2.1.

3.5.1.1 Operator Action OA-1

The correct value for this event from the NREP guide is 1E-1. The PSS value used appears to be simply a data transposition error.

3.5.1.2 Operator Action OA-8

The PSS value of 1E-2 for OA-8 is not consistent with the value from the NREP guide. The NREP value of 1E-3 should be used instead, because this event is independent of other events on the tree and there is ample time (>60 minutes) to perform the action. No review is required for associated action OA-8' because it was rejected in the event tree review in Section 3.2.2.5. For the newly added action OA-8R, which is needed for ATWS in combination with a LOCA (see Section 3.2.2.5), the time frame is only 20 minutes. The NREP value for the action is therefore 0.1.

3.5.1.3 Operator Action OA-9

The PSS modified the NREP value because even though the operator has 30 minutes to diagnose the location of the LOCA, there are only 10 minutes from the time quench spray fails until he the recirculation signal must be overidden. This modification is considered to be unjustified since the cognitive error model is not based on the time from the start of the event. It is based on the amount of time the operator has to diagnose a situation from the onset of conditions which would tend to lead to the diagnosis. In this case, review of the emergency procedure guideline shows that the diagnosis of, and response to, this situation begins with the occurrence of the CDA signal followed by the continued increase in pressure resulting from the failure of quench spray. The unmodified NREP value of 5E-1 should be used for this event.

3.5.1.4 Operator Action OA-2-E

This new action (see Section 3.2.1.1) is assumed to be procedural in nature as opposed to cognitive, because it results not from misdiagnosing the situation but rather from the improper performance of the procedure. This procedure is the exception to the rule that operator actions are simple. Review of the guideline for this procedure indicated that it could be quite complex. This error is considered recoverable, however, based on feedback provided to the operator through the procedures. The NREP screening value of 1E-3 for procedural errors with recovery possible has been assigned to this error.

3.5.1.5 Operator Action OA-6-E

This new action (see Section 3.2.1.1) is somewhat unique in that it actually consists of two separate but related cognitive errors. The first error consists of the operator misdiagnosing the initial plant condition and initiating operator action OA-6. The second cognitive error consists of the operator failing to diagnose the first error and reversing the action. This action has been evaluated using the NREP model for cognitive errors as applied to <u>both</u> of the errors involved in OA-6-E. The first error is evaluated to be equal to the probability of failing to perform OA-6 in 30 minutes. That is, the error of failing to perform OA-6 is nominally equivalent to the error of performing OA-6 when not required. The 30-minute time frame is chosen because it represents the best estimate of operator response time for the OA-6 actions, which gives a failure probability of 1E-2. The actual time frame the operator will have will depend on exactly what he misdiagnoses the plant conditions to be. Once this action has been performed, the cognitive error "clock" starts again, and the operator has a certain amount of time to interpret the information feedback from the control room instruments. The review estimate of this time is on the order of 30 minutes. This was chosen because 30 minutes was used for other similar actions, that is, actions which represent the actuation of systems to restore the core cooling function, e.g., OA-1, OA-3, OA-4, and OA-7. The NREP cognitive error value for failure to act within 30 minutes is 1E-2. Thus, the total probability of error becomes the probability of misdiagnosing the situation and performing OA-6 times the probability of failing to recognize the error, or:

$$P(\text{OA-6-E}) = P(\text{OA-6}) \times P(\text{FTR} \mid \text{OA-6}) = .01 \text{ X } .01 = 1\text{E-}4 \qquad (3\text{-}5)$$

3.5.1.6 Operator Action OA-10

This new action is assumed to be cognitive in nature (see Section 3.2.2.2) because it results from the operator failing to recognize the need to take action. The NREP time-dependent HEP for the available time frame (19 hours) is 1E-4.

3.5.1.7 Operator Actions in RT-3 and RT-4

The PSS used a value of 1E-2 for the failure of the operator to act to manually scram the reactor within the first minute of an initiator. This value is substantially lower than the NREP value, which assumes no action is possible within the first minute. However, the use of this value for this particular action is judged to be reasonable. As stated in the PSS, the operator is highly sensitized to the need to hit the manual scram button following a trip signal. Additionally, we note that the cognitive error model is a tool for estimating the probability of proper diagnosis of a situation in a given time frame. In this case, no diagnosis takes place. The operator merely automatically responds to an annunciation of a trip condition without any attempt to determine the reason for the annunication. The action is instinctive as opposed to cognitive. Thus, the estimate of 1 failure in 100 demands is judged to be a reasonable, if not conservative, estimate of failure to perform this action.

3.5.2 Operator Actions Modeled on the Fault Trees

The PSS included two generic types of operator errors in the fault tree analysis; errors in response to accidents, and errors in failing to restore components after test or maintenance acts. These errors are shown in Table 3.5.2 with the human error probabilities used in the PSS and the results of our review of these values.

3.5.2.1 Failure to Restore Following Test or Maintenance

The PSS evaluated these errors using the THERP methodology from NUREG/CR-1278 (Ref. 3.5-2). The use of this methodology is considered inappropriate for this analysis. The THERP system quantifies procedural errors by a detailed analysis of the procedural and decision-making steps the operator must follow in the course of performing a specific act. It was not possible to this for the PSS since there are no actual procedures available for Millstone. Therefore, the PSS designed its trees based on their perception of what the procedures would be like. In doing so, they did not rigorously model all of the steps the operator has to deal with. Even if it had been possible to do this, a simpler screening calculation is more easily justified. A re-evaluation of these errors was performed using the IREP methodology described in the Millstone 1 IREP study (NUREG/CR-3085) (Ref. 3.5-3). A full discussion is not necessary here, but the expression for unavailability reduces to:

$$P(\text{Error}) = P(\text{error per act}) \times \frac{\text{time between status checks}}{\text{time between manipulations}} \quad (3\text{-}6)$$

The calculation for errors numbered 2 and 3 in Table 3.5.2, which pertain to monitored components checked each shift (every eight hours), is straightforward and is performed for components manipulated monthly and quarterly, which should suffice for most ESF components. Using an error rate per manipulation of 0.01 from Ref.3.5-1, the results are:

$$P(\text{monthly}) = (0.01) \times (8\text{hours} / 720\text{hours}) = 1\text{E-}4 \quad (3\text{-}7)$$
$$P(\text{quarterly}) = (0.01) \times (8\text{hours} / 2160\text{hours}) = 3\text{E-}5$$

The calculation for error number 1, which is for unmonitored components, must be made on a per-component basis using reasonable assumptions regarding the ratio of checks to manipulations. The conservative screening value of 0.01 could be used as a scoping value.

3.5.2.2 Errors in Response to Accident Conditions

The PSS used the screening value for procedural errors with recovery potential from the NREP guide (1E-3). This value is reasonable, but it is noted that there may be errors which fall into this class for which there is no recovery potential. For example, failing to open a pump suction valve prior to starting a pump may result in irrepairable damage to the pump in a very short time period, resulting in no chance for recovery. Each error so modeled in the fault trees must be evaluated individually to determine if recovery is possible. If it is not, the NREP screening value of 1E-2 should be used.

3.5.3 References for Section 3.5

3.5-1 I. A. Papazoglou et al., Brookhaven National Laboratory, "Probabilistics Safety Analysis Procedures Guide," USNRC Report NUREG/CR-2815, January 1984.

3.5-2 A. D. Swain and H. E. Guttman, Sandia National Laboratories, "Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Application," USNRC Report NUREG/CR-1278, September 1980.

3.5-3 P. J. Amico et al., Science Applications, Inc., "Interim Reliability Evaluation Program: Analysis of the Millstone Point Unit 1 Nuclear Power Plant," USNRC Report NUREG/CR-3085, February 1983.

3.6 Failure Data

This section presents the results of a review of the failure (and unavailability) rates used in the MP 3 PSS. The review consisted of: (1) a comparison of the individual random component failure rates with similar rates from other sources, (2) a review of the system failure probabilities and unavailabilities, and (3) a review of the common-cause failure assessment. These subjects are considered in separate subsections, following.

3.6.1 Random Component Failure Rates

It should be noted that most of the MP 3 PSS component failure rates were, according to the MP 3 report, derived from a data base for Millstone 3 which was developed by Westinghouse Nuclear Technology Division (WNTD). This data base is described as proprietary, was not provided as part of the MP 3 PSS documentation, and was not included in this review. The data are stated in PSS page 2-A-2 to be based extensively on Westinghouse nuclear plant experience which covers the time period of 1972 through 1981 and contains over "200 years" (we assume this should be 200 reactor-years) of plant operation.

The use of a data base derived extensively from Westinghouse operating plants can provide valid component failure rates for the Millstone 3 plant. However, use of such data does not necessarily assure that the derived rates are applicable to MP 3, nor can it be concluded that this data base is the most applicable of the available data. Most safety system components are procured by the architect-engineer and are not the direct responsibility of the vendor. Thus, Westinghouse plants can have a variety of components supplied by different manufacturers with different procurement specifications and different failure rates. One of the most significant parameters influencing component failure rates is the manufacturer of the component.

The MP 3 PSS random component failure rates are given in PSS Appendix 2-A, Section 2, Volume 6. This appendix also provides the assumptions which were used in deriving the rates. These assumptions were reviewed and the following comments were developed. Each comment includes an assessment of the influence of the discrepancy, when appropriate.

(1) Page 2-A-6: Under subsection A.2.1, it is stated that, for the purpose of deriving a failure rate for motor-driven auxiliary feedwater pumps, "It was assumed that the 'fails-to-operate' failure rate would be similar to that for pumps classified as alternating pumps; i.e., component cooling and service water pumps. These alternating pumps are assumed to operate 50% of the plant operation time." This statement implies that one of the motor-driven auxiliary feedwater pumps was assumed to be operating at all times that the plant was in operation. However, auxiliary feedwater pumps are actually used only during plant startup and shutdown, and on those relatively rare occasions when main feedwater is lost, and when tested. Thus, this assumption is invalid and would produce an optimistic failure rate when used in conjunction with Eq. 2-A-3, Page 2-A-3.

The influence of this assumption is not expected to be great, since auxiliary feedwater failures are typically dominated by failure to start of multiple pumps. A further discussion of auxiliary feedwater failure is provided in Section 3.6.2 following.

(2) Page 2-A-6: The turbine-driven auxiliary feedwater pump, according to item 3.1, was assumed to operate 10% of the total plant operating time. This seems excessively long (876 hours/year) for reasons stated in (1) above (and also since the turbine-driven pump cannot be used for startup) and would produce an optimistic failure rate.

For reasons stated in (1) preceding, this assumption is not expected to have a significant influence on the overall results of the PSS.

(3) Page 2-A-6: The containment spray pump failure rate (item 4.1) "...is derived from the 'fails during operation' mode of the service water and component cooling water pumps." The meaning of this statement is not clear.

The remainder of the review of random component failures consisted of comparing the rates provided in Tables 2-A-2 (fluid system components) and 2-A-3 (electrical/electronic system components) contained in Appendix 2-A, Volume 6, with other rates. The MP 3 PSS values in these tables were compared with the NRC-developed values as contained in the NREP (Ref. 3.6-1) and IREP (Ref. 3.6-2) procedure guides, and with values contained in the Zion PRA (Ref. 3.6-3), a recent industry-sponsored PRA for a Westinghouse plant similar to MP 3.

Table 3.6-1 provides the quantitative comparison for fluid systems and Table 3.6-2 for electrical/electronic systems. The first column lists all the component types which were included in Table 2-A-2 of the MP 3 PSS, in the same order. The second column gives the system(s) for which the corresponding component failure rates were used, and the third column is the failure mode(s) for the component. The next three columns provide the values used for the MP 3 PSS, NREP/IREP, and Zion PRA. The NREP and IREP values were combined since they are essentially identical. In a few cases, only IREP values [taken from Appendix C of the Millstone Unit 1 IREP study (Ref. 3.6-4)] were available. These cases are identified in the comments (last) column.

All values in Tables 3.6-1 and 3.6-2 are mean values. The IREP data, which are given as median values in Reference 3.6-4, were converted to mean values by using the conversion relationship in Appendix C of the NREP guide (Ref. 3.6-1) for loguniform distributions. The NREP/IREP values are also essentially identical to corresponding values used in WASH-1400. The NREP values are all given as hourly rates, while many MP 3 PSS values are on a demand basis. The NREP hourly rates were converted to demand rates assuming a monthly test interval.

Table 3.6-3 provides a listing of the MP 3 PSS values which were significantly different from the NREP/IREP values. The measure of significance was somewhat arbitrarily selected as a factor of 5. In other words, any MP 3 PSS value which was a factor of 5 greater or less than the NREP/IREP value appears in Table 3.6-3. It is considered that differences of less than a factor of 5 are probably not significant in most, if not all cases. The first column in Table 3.6-3 lists the component and failure mode, and the second column provides the factor of difference in terms of the ratio $\frac{\text{(NREP/IREP)}}{\text{(MP 3 PSS value)}}$.

Table 3.6-1 Fluid system components - comparison of component failure rate data.

Component type	System	Failure mode	Failures/hour or demand[a]			Comments
			MP 3 PSS	NREP/IREP	Zion PRA[b]	
1. Manual valve	All ESF systems	a. Transfers closed	2.15E-6/hr	2E-7/hr	5.28E-8/hr	
		b. Transfers open	4.92E-7/hr	1E-7/hr	NG[c]	
2. Check valve	All ESF systems	a. Failure to operate on demand	3.20E-4/D	7E-5/D(M)	4.32E-5/D	
		b. Failure to seat	1.56E-5/hr	2E-6/hr	8.38E-7/hr	
3. Spring-loaded safety valve	All ESF systems	a. Premature opening	1.90E-6/hr	NG[c]	1.65E-6/hr	Zion value includes leakage
		b. Failure to reclose	2.98E-3/D	NG	NG	
4. Motor-operated valve	All ESF systems except cont. spray and CVCS	a. Failure to operate on demand	2.63E-3/D	4E-3/D(M)	1.55E-3/D	
		b. Transfers open	4.57E-6/hr	1E-7/hr	3.14E-8/hr	Zion value includes excessive leakage
		c. Transfers closed	2.15E-6/hr	2E-7/hr	NG	
5. Motor-operated valve	Containment spray	a. Failure to operate on demand	9.54E-4/D	4E-3/D(M)	2.26E-5	Zion value for all motor-operated valves.
		b. Transfers open	4.57E-6/hr	1E-7/hr	NG	MP 3 values assumed the same as item 4
		c. Transfers closed	2.15E-6/hr	2E-7/hr	NG	Same as above
6. Air-operated valve	All ESF systems	a. Failure to operate on demand	4.63E-3/D	4E-3/D(M)	1.44E-3	
		b. Transfers open	4.30E-6/hr	1E-7/hr	NG	
		c. Transfers closed	1.37E-6/hr	2E-7/hr	1.12E-7/hr	

Table 3.6-1 (Continued).

Component type	System	Failure mode	Failures/hour or demand[a] MP 3 PSS	NREP/IREP	Zion PRA[b]	Comments
7. Motor-driven pump	Auxiliary feedwater	a. Failure to start on demand	5.00E-3/D	4E-3/D(M)	NG	
		b. Fails during run operation	1.69E-5/hr	1E-4/hr	9.87E-5/hr	
8. Motor-driven pump	Safety injection	a. Failure to start on demand	1.34E-3/D	4E-3/D(M)	7.21E-4/D	
		b. Fails during run operation	4.86E-5/hr	1E-4/hr	1.55E-5/hr	
9. Motor-driven pump	Residual heat removal	a. Failure start on demand	1.34E-3/D	4E-3/D(M)	7.21E-4/D	
		b. Fails during run operation	6.90E-5/hr	1E-4/hr	2.53E-6/hr	
10. Motor-driven pump	Service water	a. Failure to start on demand	1.34E-3/D	4E-3/D(M)	7.21E-4/D	
		b. Fails during run operation	2.47E-5/hr	1E-4/hr	1/32E-6/hr	
11. Motor-driven pump	Containment spray	a. Failure to start on demand	1.34E-3/D	4E-3/D(M)	7.21E-4/D	
		b. Fails during run operation	1.69E-5/hr	1E-4/hr	1.5E-5/hr	
12. Turbine-driven pump	Auxiliary feedwater	a. Failure to start on demand	2.58E-2/D	4E-2/D(M)	2.29E-2/D	
		b. Fails during run operation	6.15E-4/hr	2E-5/hr	7.63E-6/hr	
13. Isolation valve	Main steam	a. Failure to operate on demand	4.63E-3/D	4E-3/D(M)	NG	MP 3 PSS value assumed the same as item 6
		b. Transfer closed	1.37E-6/hr	1E-7/hr	NG	Same as above

Table 3.6-1 (Continued).

Component type	System	Failure mode	Failures/hour or demand[a]			Comments
			MP 3 PSS	NREP/IREP	Zion PRA[b]	
14. Heat exchanger	All ESF systems	a. External leakage	1.00E-6/hr	3E-6/hr	7.13E-7/hr	MP 3 PSS value stated to be from NREP
		b. Tube side plugged	8.50E-9/hr	4E-9/hr (IREP)	ε[d]	
		c. Shell side plugged	8.00E-10/hr	4E-10/hr (IREP)	ε	MP 3 PSS value stated to be from WASH-1400
15. Motor-operated valve	Chemical and volume control system	a. Failure to operate on demand	5.74E-4/D	4E-3/D(M)	3.72E-3/D	
		b. Transfers open	1.58E-5/hr	1E-7/hr	3.14E-8/hr	Zion PRA value includes excessive leakage
		c. Transfers closed	2.15E-6/hr	2E-7/hr	NG	MP 3 PSS value assumed to be the same as item 4
16. Pipe section <3" in diam.	All ESF systems	a. Ruptures/ plugged	8.50E-9/hr	4E-9/hr	8.6E-9/hr	MP 3 PSS value stated to be from WASH-1400
17. Pipe section >3" in diam.	All ESF systems	a. Ruptures/ plugged	8.00E-10/hr	4E-10/hr	8.6E-10/hr	Same as above
18. Storage tank	All ESF systems	a. Ruptures	8.00E-10/hr	4E-10/hr	NG	MP 3 PSS value assumed the same as item 17
19. Flow/metering orifice	All ESF systems	a. Ruptures	2.70E-8/hr	3E-8/hr	NG	
		b. Plugged	3.70E-4/D	2E-4/D(M)	NG	
20. Strainer	All ESF systems	a. Plugged	1.00E-5/hr	3E-5/hr	NG	MP 3 PSS value stated to be from NREP

Table 3.6-1 (Continued).

Component type	System	Failure mode	Failures/hour or demand[a]			Comments
			MP 3 PSS	NREP/IREP	Zion PRA[b]	
21. Air-operated check valve	All ESF systems	a. Failure to operate on demand	4.63E-3/D	4E-3/D(M)	NG	MP 3 PSS value assumed the same as item 6
		b. Failure to seat	1.55E-5/hr	2E-6/hr	NG	Same as above
22. Air-operated three-way bypass valve	All ESF systems	a. Failure to bypass on demand	4.63E-3/hr	4E-3/D(M)	NG	Same as above
		b. Transfers closed	1.37E-6/hr	2E-7/hr	NG	Same as above
		c. Transfers open	4.30E-6/hr	1E-7/hr	NG	Same as above
23. Butterfly valve	All ESF systems	a. Failure to operate on demand	2.64E-3/D	4E-3/D(M)	NG	MP 3 PSS value assumed to be the same as item 6
		b. Transfers closed	2.15E-6/hr	2E-7/hr	NG	Same as above
		c. Transfers open	1.52E-5/hr	1E-7/hr	NG	
24. Valve limit switch	All ESF systems	a. Failure to operate properly	1.00E-4/D	2E-3/D(M)	NG	MP 3 PSS value stated to be from NREP
		b. Contacts short	2.70E-8/hr	2E-8/hr (IREP)	NG	MP 3 PSS value stated to be from WASH-1400
25. Valve torque switch	All ESF systems	a. Failure to operate properly	1.00E-4/D	7E-5/D(M)	NG	MP 3 PSS value stated to be from NREP
		b. Contacts short	2.70E-8/hr	2E-8/hr (IREP)	NG	MP 3 PSS value stated to be from WASH-1400

[a] /D(M) = per demand value computed from hourly rates assuming monthly testing.

[b] Zion PRA values are from updated, plant specific values given in Table 1.5.1-5 (Vol. 3).

[c] NG = not given

[d] ε = negligible

Table 3.6-2. Electrical/electronic system components - comparison of component failure rate data.

Component type		System	Failure mode		Failures/hour or demand[a]			Comments
					MP-3 PSS	NREP/IREP	Zion PRA[b]	
1.	Diesel generators	Ac emergency electrical power		Failure to start on demand	2.33E-3/D	2E-2/D(M)	1.82E-2/D	
				Fails during run operation	NG[c]	3E-3/hr	5.97E-3/hr	
2.	Bus feed	AC electrical power		Failure to close on demand	3.38E-4/D	4E-3/D(M)	1.63E-3/D	
				Failure to open on demand	1.58E-4/D	4E-3/D(M)	5.31E-4/D	
				Transfers open	1.52E-6/hr	3E-5/hr	2.32E-7/hr	
3.	Main and auxiliary transformer	AC electrical power		Fails during operation	2.80E-6/hr	6E-7/hr	1.73E-6/hr	
4.	ESF aux. power transformer	AC electrical power		Fails during operation	2.80E-6/hr	6E-7/hr	1.73E-6/hr	
5.	DC/AC power inverters	AC electrical power		Fails during operation	2.39E-5/hr	1.09E-5/hr	NG[c]	
6.	Storage battery (wet cell)	DC electrical power		Fails during operation	1.00E-6/hr	2E-6/hr	7.61E-8/hr	MP 3 PSS values stated to be from NREP
7.	Battery chargers	DC electrical power		Fails during operation	3.16E-5/hr	6E-7/hr	5.54E-7/hr	
8.	Metal-enclosed bus	Dc electrical power	a.	Open circuit	1.68E-8/hr	3E-8/hr	NG	
			b.	Bus-to-ground short	5.60E-8/hr	3E-8/hr	NG	
9.	Metal-enclosed bus	Ac electrical power	a.	Open circuit	1.68E-8/hr	3E-8/hr	1.91E-8/hr	MP 3 PSS value assumed the same as item 8
			b.	Bus-to-ground short	5.60E-8/hr	3E-8/hr	NG	MP 3 PSS value assumed the same as item 8

Table 3.6-2 (Continued).

Component type	System	Failure mode	Failures/hour or demand[a]			Comments
			MP-3 PSS	NREP/IREP	Zion PRA[b]	
10. Undervoltage relay	Ac electrical power	a. Fails to trip on demand	4.03E-6/D	1E-3/D(M)	6.28E-6/D	NREP/IREP value based on solid state devices
11. Overcurrent relay	Ac electrical power	a. Fails to trip on demand	4.03E-6/D	1E-3/D(M)	6.28E-6/D	Same as above
12. Underfrequency relay	Ac electrical power	a. Fails to trip on demand	4.03E-6/D	1E-3/D(M)	6.29E-6/D	Same as above
13. Trip/bypass breaker	Reactor protection system	a. Fails to open on demand	3.38E-4/D	4E-3/D(M)	9.79E-3/D	
14. Dc master relay	Reactor protection and ESF actuation	a. Failure to operate on demand	1.00E-4/D	1E-3/D(M)	NG	MP 3 PSS value stated to be from NREP
		b. Contacts transfer open	1.20E-7/hr	1E-7/hr (IREP)	2.43E-7/hr	MP 3 PSS value stated to be from WASH-1400
		c. Contacts transfer closed	2.70E-8/hr	2E-8/hr	NG	Same as above
15. Dc slave relay	ESF actuation	a. Failure to operate on demand	1.00E-4/D	1E-3/D(M)	NG	MP 3 PSS value assumed the same as item 14
		b. Contacts transfer open	1.20E-7/hr	1E-7/hr (IREP)	NG	
		c. Contacts transfer closed	2.70E-8/hr	2E-8/hr (IREP)	NG	
16. Control cable/ wiring	Reactor protection and ESF actuation	a. Line-to-line short	2.70E-8/hr	3E-8/hr	3.22E-6/hr	MP 3 PSS value stated to be from WASH-1400
		b. Line-to-ground short	8.00E-7/hr	1E-6/hr	7.52-6/hr	Same as above
		c. Open circuit	3.70E-6/hr	1E-5/hr	NG	Same as above

Table 3.6-2 (Continued).

Component type	System	Failure mode	Failures/hour or demand[a]			Comments
			MP-3 PSS	NREP/IREP	Zion PRA[b]	
17. Ac output relay	ESF actuation	a. Failure to operate on demand	1.00E-5/D	1E-3/D(M)	NG	MP 3 PSS value assumed the same as item 14
		b. Contacts transfer open	1.20E-7/hr	1E-7/hr (IREP)	2.43E-7/hr	Same as above
		c. Contacts transfer closed	2.70E-8/hr	2E-8/hr (IREP)	NG	Same as above
18. Ac output latching relay	ESF actuation	a. Failure to operate on demand	1.00E-4/D	1E-3/D(M)	NG	Same as above
		b. Contacts transfer open	1.20E-7/hr	1E-7/hr (IREP)	2.43-7/hr	MP 3 PSS value assumed the same as item 14
		c. Contacts transfer closed	2.70E-8/hr	2E-8/hr (IREP)	NG	Same as above
19. Control transformer	ESF actuation	a. All modes	1.00E-6/hr	6E-7/hr	NG	MP 3 PSS value stated to be from NREP
20. Pressure transmitter	Reactor protection and ESF actuation	a. Fails to provide proper outout	6.52E-5/hr	6E-5/hr (IREP)	NG	
21. Water level transmitter	Reactor protection and ESF actuation	a. Fails to provide proper output	4.29E-5/hr	6E-5/hr (IREP)	1.66E-6/hr	
22. Temperature transmitter	Reactor protection and ESF actuation	a. Fails to provide proper output	4.83E-6/hr	6E-5/hr (IREP)	NG	
23. Flow transmitter	Reactor protection and ESF actuation	a. Fails to Ppovide proper output	3.86E-5/hr	6E-5/hr (IREP)	NG	
24. Temperature element (RTD)	Reactor protection and ESF actuation	a. Fails to provide proper output	8.33E-6/hr	6E-5/hr (IREP)	NG	

Table 3.6-2 (Continued).

Component		Failure	Failures/hour or demand[a]			
type	System	mode	MP-3 PSS	NREP/IREP	Zion PRA[b]	Comments
25. Differential pressure transmitter	Reactor protection and ESF actuation	a. Fails to provide proper Output	6.52E-5/hr	6E-5/hr (IREP)	NG	
26. Analog processing module	Reactor protection and ESF actuation	a. Fails to provide proper Output	7.75E-7/hr	3E-6/hr	NG	
27. Comparator (bistable)	Reactor protection and ESF actuation	a. Fails high output	2.40E-6/hr	NG	NG	
		b. Fails low output	1.65E-6/hr	NG	NG	
28. Manual switch (pushbutton)	Reactor protection and ESF actuation	a. Short across contacts	4.04E-7/hr	2E-8/hr (IREP)	ε[d]	Zion PRA value (negligible) based on engineering judgment
29. Manual switch (rotary)	Reactor protection and ESF actuation	a. Short across contacts	1.70E-6/hr	2E-8/hr (IREP)	ε	Same as above
		b. Contacts fail Open	1.70E-6/hr	1E-7/hr (IREP)	NG	
30. Fuse	All electrical systems	a. Open prematurely	4.37E-7/hr	3E-6/hr	8.32E-7/hr	Zion PRA value stated to be for ESF dc power fuse
31. Loop power supply	Reactor protection and ESF actuation	a. Fails to provide proper Output	2.97E-6/hr	6E-7/hr	NG	NREP/IREP value for transformers
32. Radiation monitor	Reactor protection and ESF actuation	a. Fails to provide proper Output	1.06E-5/hr	6E-5/hr (IREP)	NG	

[a] /D(M) = per demand value computed from hourly rates assuming monthly testing.

[b] Zion PRA values are from updated, plant specific values given in Table 1.5.1-5 (Vol. 3).

[c] NG = not given

[d] ε = negligible

In other words, a column 2 value of 5 means that the failure rate used in NREP/IREP is 5 times greater than the corresponding rate in the MP 3 PSS. A total of 23 component failure modes in the PSS were found to vary by more than a factor of 5 from the NREP/IREP values. This represents 23% of the total component failure modes in Table 3.6-1. Numbers in the second column less than 0.2 (or 1/5) indicate that the MP 3 PSS values are greater than (or conservative with respect to) the NREP/IREP values. Numbers greater than 5 indicate that the MP 3 values are less than (or optimistic with respect to) the NREP/IREP values.

As Table 3.6-3 indicates for fluid system components, four MP 3 PSS values were more than a factor of 5 greater than the NREP/IREP values, while four rates were smaller than 1/5 of the NREP/IREP values. For electrical/electronic system components, the majority (12 of 16) of the MP 3 PSS values are lower than the NREP/IREP values, indicating an optimistic bias with respect to the NREP/IREP values.

Table 3.6-4 provides a similar comparison between the MP-3 PSS values and values used in the Zion PRA. (It should be noted that the Zion PRA did not provide values for a number of the MP 3 PSS entries in the Tables 3.6-1 and 3.6-2.) The majority of the MP 3 PSS values, as shown in Table 3.6-4 are conservative (larger) than the equivalent values used in Zion. Of the 20 entries, Zion failure rates are smaller than the PSS values on 13 cases.

It is difficult to draw conclusions regarding the validity of the MP 3 PSS failure rates based on these comparisons. Since the data base used for the MP 3 was not available for review, the validity and robustness of the data could not be ascertained. It was considered significant that so many of the MP 3 rates varied by large amounts from the NREP/IREP values. These variations did show a trend for the MP 3 values to be on the optimistic side, but the trend was not strong.

A further extension of the comparisons was undertaken to determine which MP 3 variations were significantly different in the same direction with respect to both the Zion PRA and NREP/IREP data. Table 3.6-5 provides the results of this comparison. As shown in the table, a total of eight component failure rates were found. One-half of the MP 3 rates are optimistic with respect to the other failure rates, and one-half are conservative.

Generally, system failures are dominated by active components which are required to change state when the system receives a command to operate. Passive component failures (check valves, etc), active components which fail by incorrect transfer (MO valves, etc), and active components which start (pumps, motors, etc.) but fail to sustain operation, usually are not dominant contributors. In Table 3.6-5 the only components which meet these general criteria as potentially significant component failures are CVCS MOV fails to operate, diesel generators (fail to start), and trip/bypass breaker (RPS) fails to open. The battery chargers are normally operating and no change of state is required. Furthermore, battery chargers do not appear as dominant components (see Section 3.4.16). Thus, lowering their failure rate to be consistent with NREP/IREP and Zion PRA values would make their already negligible contribution to risk even lower. The CVCS MOV failures are not expected to be dominant contributors since the high pressure SI pumps are functionally redundant to the CVCS. As shown in Section 5.3, the CVCS does

Table 3.6-3 Comparison of MP 3 PSS and NREP/IREP component failure rates.[a]

Component and failure mode	$\frac{\text{NREP/IREP value}}{\text{MP 3 PSS value}}$ [b]
Fluid system components	
1. Manual valve transfers closed	0.1
2. Check valve fails to seat	0.1
3. MOV transfers open	0.02
4. Motor driven AF pump fails to run	5.92
5. Motor driven CS pump fails to run	5.92
6. Turbine driven AF pump fails to run	0.03
7. MOV (CVCS) fails to operate	7.
8. Valve limit switch fails to operate	20.
Electrical/electronic system components	
9. Diesel generator fails to start	8.5
10. Bus feed breaker fails to close	11.8
11. Bus feed breaker fails to open	25.
12. Bus feed breaker transfers open	20.
13. Battery charger fails to operate	0.02
14. Undervoltage relay fails to trip	250.
15. Overcurrent relay fails to trip	250.
16. Underfrequency relay fails to trip	250.
17. Trip breaker fails to open	10.
18. Relay fails to operate	10.
19. Temperature transmitter fails	12.
20. Temperature element fails	7.
21. Manual pushbutton short	0.05
22. Manual rotary switch short	0.012
23. Manual rotary switch contacts fail open	0.067
24. Fuse opens prematurely	7.
25. Radiation monitor fails	6.

[a] Millstone 3 PSS value is conservative if ratio is less than 1.

[b] NREP values are essentially identical to IREP values. Where only the NREP value was available, or both values were available, the NREP value was used. Where only the IREP value was available, it was used.

Table 3.6-4 Comparison of MP 3 PSS and Zion PRA component failure rates.[a]

Component and failure mode	$\frac{\text{Zion value}}{\text{MP 3 PSS value}}$
Fluid system components	
1. Manual valve transfers closed	0.03
2. Check valve fails to operate	0.14
3. Check valve fails to seat	5.34
4. MOV transfers open	0.007
5. MOV (containment spray) fails to operate	0.023
6. Air-operated valve transfers closed	0.083
7. Motor-driven AF pump fails to run	5.84
8. Motor-driven RHR pump fails to run	0.037
9. Motor-driven SWS pump fails to run	0.053
10. Turbine-driven AF pump fails to run	0.012
11. MOV (CVCS) fails to operate	6.5
12. MOV (CVCS) transfers operate	0.002
Electrical/electronic system components	
13. Diesel generator fails to start	7.8
14. Bus feed breaker transfers open	0.153
15. Storage battery fails to operate	0.076
16. Battery charger fails to operate	0.018
17. Trip/bypass breaker (RPS) fails to open	28.9
18. Control cable/wiring short (line-to-line)	119.
19. Control cable/wiring short (line-to-ground)	9.4
20. Water level transmitter output failure	0.039

[a] Millstone 3 PSS value is conservative if ratio is less than 1.

Table 3.6-5 MP 3 component failure rates significantly different from both NREP/IREP and Zion PRA values.[a]

Component and failure mode	NREP/IREP value[b] / MP 3 PSS value	Zion value / MP 3 PSS value
Fluid system components		
1. Manual valve transfers closed	0.1	0.03
2. MOV transfers open	0.02	0.007
3. Motor-driven AF pump fails to run	5.92	5.84
4. Turbine-driven AF pump fails to run	0.03	0.012
5. MOV (CVCS) fails to operate	7.	6.5
Electrical/electronic system components		
6. Diesel generator fails to start	8.5	7.8
7. Battery charger fails to operate	0.02	0.018
8. Trip/bypass breaker (RPS) fails to open	10.	28.9

[a] Millstone 3 PSS value is conservative if ratio is less than 1.

[b] NREP values are essentially identical to IREP values. Where only the NREP value was available, or both values were available, the NREP value was used. Where only the IREP value was available it was used.

not appear in any of the dominant sequences. The RPS relay failure would appear to be significant only in terms of influencing the probability of failure to scram. The RPS system (scram) failure probability was not considered in the MP 3 fault tree assessments (Section 2.3), rather it appears that a scram failure value of 3.0E-5 was adopted based on NUREG-0460 recommendations (Section 2). Thus, the RPS relay failure rate does not appear to be a significant issue.

This leaves only the diesel generators as both "outliers" with respect to the NREP/IREP and Zion data and potentially significant contributors to the core melt frequency. Diesel generator failures were found to have a not negligible influence on core melt frequency (Section 5.3). Because of this significance and the optimistic failure rate (compared to other sources) given to diesels in the MP 3 PSS, the issue of diesel generator failure rates (to start and assume load) was given rather comprehensive consideration, as described in the following subsection.

3.6.2 System Failures

This subsection provides the results of a review of the MP 3 PSS system failure rates. The first part of the review consisted of screening the MP 3 values against independent assessments for similar systems to determine if large discrepancies existed. This was followed by an evaluation to determine if the system failure rate discrepancies found had the potential for influencing the core melt frequency computed for the MP 3 plant. If such a potential was found, an attempt was made to requantify the core melt frequency to assess the potential impact of the apparent discrepancies.

It should be emphasized that the use of alternate failure rate assessments for the MP 3 systems does not imply that they are more applicable. The basis for and validity of these assessments need to be considered and judgment used in reaching conclusions regarding realistic failure rates. Such rates are, of course, unknown and must be estimated. Frequently it is difficult to judge which value is a better estimate.

A second evaluation of the validity of the MP 3 system failure rates was also performed by reviewing the fault trees used for system failure quantification. The results of this review is presented in Section 3.4 and will not be considered further here.

The alternate sources of system failure rates were selected to provide a diverse spectrum from available literature. Accordingly, the following sources were used:

- Zion PRA (Ref. 3.6-3). An industry-sponsored PRA for a Westinghouse plant similar to MP 3.

- Sequoyah RSSMAP PRA(Ref. 3.6-10). An NRC-sponsored PRA for a Westinghouse plant similar in many respects to MP 3.

- ORNL: Accident Precursor Study (Ref. 3.6-6). A study which used generic PWR LER data to estimate system failure rates for PWRs.

- Reactor Safety Study (Ref. 3.6-7). An NRC-sponsored PRA which is frequently used as the baseline to compare with other studies.

- Various other sources for individual systems.

Table 3.6-6 lists the systems which were determined to be important to safety in the MP 3 PSS. These systems represent all of those which were analyzed by fault trees in Section 2.3 of the MP 3 PSS. The first column lists the 15 systems considered, and the remaining columns provide failure rates from the various sources as identified at the top of each column. The first column of failure rates is from the MP 3 PSS. Comparable failure rates for a few systems could not be readily found in the literature, but some comparison values were found for all 11 of the systems.

In reviewing the Table 3.6-6 comparisons, it is apparent that some of the MP 3 values are outside of the range provided by other sources and others are questionable. For all of these cases, the MP 3 values are smaller (optimistic) than the comparable values. Each of the systems will be considered separately, with substantially more discussion provided for MP 3 failure rates which seem to be inconsistent with other rates. In all cases, the rates quoted are for no degradation of support equipment. Other qualifications on the values are provided in the notes at the bottom of Table 3.6-6 and are discussed further, as appropriate, in the discussion of each system.

Table 3.6-6 Comparison of system failure rates.

System	Failure rate MP 3 PSS	RSS (Ref.3.6-7)	Zion PRA (Ref.3.6-3)	Sequoyah(i) (Ref.3.6-10)	Other
1. Main electrical a. On-site emergency power	4.56E-4	1E-2[l]	7.5E-4[m]	≤1E-3[k]	1.8E-3[i], 1.1E-3 to 6.8E-3[n]
2. 120VAC	8.43E-5[b]				
3. ESF actuation	1.6E-5	6.7E-5		≤6.7E-5	
4. Loading sequencer	1.59E-5[c]				
5. Auxiliary feedwater	6.8E-5	3.7E-5	4.2E-6	≤1E-5	1.1E-3[g], 3.4E-4[h]
6. High pressure injection	5.87E-5[p]	6.3E-3	1.4E-6[i] 7.4E-9[j]	3.5E-3	1.3E-3[g]
7. Low pressure injection	1.84E-4	4.2E-3	4.7E-4	1.9E-3	
8. Main steam isolation	8.2E-4[d] 1.5E-4[e]				1.2E-3[g]
9. Quench spray		3.2E-4	2.4E-3	5.5E-5	1.7E-3
10. Safety injection pump cooling	7.32E-3[b]				
11. Charging pump cooling	5.3E-4				
12. Low pressure recirculation	3.0E-3	8.8E-3	5.2E-3	4.6E-3	
13. High pressure recirculation		5.85E-3	8.E-3	3.8E-4	8E-3
14. Containment recirculation spray	2E-3		1.6E-3		
15. Service water	7.44E-6(f)		2.2E-8[f]		2.7E-5/yr[o]

Table 3.6-6 (Continued).

Notes:

a. Per bus
b. Per train
c. Both trains
d. Steamline break inside containment
e. Steamline break outside containment
f. During a 24-hr period
g. ORNL precursor study (Ref. 3.6-6)
h. Ebasco study (Ref. 3.6-8)
i. Medium LOCA (2 of 4 pumps)
j. Small LOCA (1 of 4 pumps)
k. Has inter-unit bus ties, one of two diesels
l. No load sequencer, one of two diesels with swing unit
m. One of three diesels
n. Battle paper (Ref. 3.6-9)
o. From Oconee RSSMAP PRA (Ref. 3.6-5), 1 of 2 pumps
p. Medium and small LOCAs

(1) Main electrical system, on-site emergency power. The MP 3 value for this system is lower than any other in Table 3.6-6, from a factor of about 2 for the Zion PRA value, to about 20 for the RSS value. The most comprehensive assessment of on-site emergency power reliability was performed by Battle, et al., (Ref. 3.6-9), and the range of values found (for one of two diesels, the MP 3 configuration) was 2 to 15 times higher than MP 3. Because of these differences, a review of the basis for the MP 3 value was performed, and the results are summarized herein.

The MP 3 value for loss of on-site emergency power (4.56E-4) is dominated (as would be expected) by the common-cause failure of both diesel generators. This contribution was assessed at 2.59E-4 (Table 2.3.3.1-3, Page 2.3.3.1-48) which represents about 60% of the total. The common-cause failure assessment was performed using the binomial failure rate model. The single diesel failure rate used in the MP-3 BFR model was 2.33E-3. Thus, the MP 3 common-cause quantification corresponds to a β-factor of about 0.1, a reasonable value. The β-factor model is equivalent to the binominal failure rate model for two redundant trains or components (Ref. 3.6-11). However, the value of 2.33E-3 for a single diesel generator failure is not consistent with other results. Single diesel generator failure rates have consistently been found to be in the range of 1 to 10E-2 (Refs. 3.6-7, -9, -12).

The basis for the MP 3 diesel generator failure rate is given in Appendix 2-E of the MP 3 PSS (Volume 6, Section 2). This appendix derives the single diesel generator failure rate based on a large number of tests on the MP 3 diesel units and similar tests. A total of 300 tests were said to have been performed on the MP 3 diesel generators, and additional tests (totaling 1,839) were used to establish the failure rate. The test details in Appendix 2-E are very sketchy. It is merely stated that the 300 MP 3 tests "were performed under conditions which rigorously stressed the diesels under numerous load conditions." It is not stated whether, and to what extent, "prepping" (pre-lubing, pre-warming, pre-checking) of the diesels was performed prior to testing, whether the tests were under "fast start" conditions which would exist under actual demands, time interval between tests, whether the other tests (other than the 300 MP 3) were under the same "rigorous" conditions, and what other measures and considerations were employed to assure that the test data represents "field" conditions. In view of this lack of information regarding the tests, it was not possible to evaluate the validity of the MP 3 diesel generator failure rate based on the tests. However, the derivation of the failure rate given that the test data are applicable does appear valid. Other investigators (Refs. 3.6-9, -13) have concluded that reliability improvements below about 1E-2 are probably not readily achievable for diesel generators. Further, Ref. 3.6-12 indicates that Fairbanks-Morse diesels (the manufacturer of the MP 3 units) have a somewhat worse-than-average failure rate, and larger units (the MP 3 units, at 5000 kW, are among the largest used at nuclear plants) tend to be less reliable.

In view of these considerations, it seems highly unlikely that a failure rate of less than about 2E-2/demand can be achieved for diesel generators at the MP 3 site unless extraordinary measures have been taken to improve reliability.

If a value of 2E-2/demand were substituted for the MP 3 rate of 2.33E-3, the probability of on-site emergency power failure would be about 2.2E-3 assuming the same relative common-cause contribution and that the other contributors to the failure probability remain the same. This represents about a factor of 5 increase in the MP 3 value. The significance of this increase is assessed later in this section.

(2) 120V AC System. No comparable failure rates for this system could be readily found in the open literature. A review of the fault tree quantification for the derivation of this value is given in Section 3.4. It should be noted that failure of the 120VAC system does not appear as a dominant contributor to the core melt frequency (Section 5.3).

(3) ESF Actuation. The MP 3 result for the probability of ESF actuation failure (1.6E-5) is about a factor of 4 less than the equivalent value from the RSS and less than a factor of 4 smaller than the Sequoyah value. This is considered reasonable agreement. Further, since ESF actuation failures do not appear in any of the dominant accident sequences (Section 5.3), a factor of 4 (or even larger) increase would have an insignificant effect on the results.

(4) Load Sequencer. No values in the open literature could be readily found to compare with the MP 3 failure rate for the emergency diesel generator loading sequencer. However, the value appears reasonable, and loading sequencer failures are not among dominant systems (Section 5.3).

Further, since the loading sequencers are a part of the emergency on-site power system, the MP 3 failure rate for the sequencers would have to be raised by over an order of magnitude to become a contributor to emergency power failure.

(5) Auxiliary Feedwater. The MP 3 auxiliary feedwater system failure rate was assessed to be 6.8E-5/demand. This value is, as shown in Table 3.6-6, somewhat higher than the RSS, Zion, and Sequoyah assessments (all have similar systems, consisting of two 50% capacity motor-driven pumps and a 100% steam turbine-driven pump). However, more recent assessments (shown in the "Other" column of Table 3.6-6) indicate significantly higher failure rates, being 5 (for the Ebasco study) to 16 (for the ORNL precursor study) times higher than the MP 3 rate. It should be noted, however, that the ORNL assessment is for all auxiliary feedwater systems (including designs other than MP 3) based entirely on LER data. It appears, based on the comparison, that the MP 3 value is not unreasonable for a mature system. However, for the first year or two of operation, the NRC has estimated, based on LER data, that the auxiliary feedwater failure rate may be in the range of 1E-4 to 1E-3/demand, corresponding to the Ebasco (Ref. 3.6-8) and ORNL precursor study (Ref. 3.6-6) values. It therefore seems appropriate to examine the impact on the core melt frequency of assuming a factor of 10 increase in the MP 3 auxiliary feedwater system value to determine the potential significance during the first years of operation. This impact is evaluated later in this section.

(6) High Pressure Safety Injection System. MP 3 PSS failure rate assessed for the HPSI is lower than all Table 3.6-6 values except for Zion. However, there are significant differences for the success criteria and the system designs assumed for the RSS and Sequoyah PRAs. In the RSS, the Surry plant HPSI consists of (Appendix II, Ref. 3.6-14) three charging pumps, one of which is required to operate for success during small and medium LOCAs. In the Sequoyah study (Section B.9, Ref. 3.6-5), the HPSI consists of two charging pumps plus two safety injection pumps. For success, at least one pump from each system is assumed to be required. In the MP 3 PSS, the HPSI is described as including three charging pumps (one of which is in a standby condition) and two safety injection pumps. According to the PSS (Table 2.3.3.6.2-1), only one pump of the four available (the standby pump is not considered available under LOCA conditions) is required for success. In view of these differences, the MP 3 HPSI failure rate does not seem unreasonable. Further, the Zion HPSI design is similar to MP 3 (two independent systems of two pumps each) and success for small LOCAs is one of any four pumps (Section II-4.5.2.3.1). In this instance, the Zion PRA assesses the failure rate (Table 3.6-6) at 7.4E-9, well below the MP 3 value.

(7) Low Pressure Safety Injection System. The MP 3 LPSI failure rate is lower than all other values, ranging from a factor of 2.6 lower than Zion to a factor of 23 less than the RSS.

The LPSI system is needed as a safety injection system only for large-break LOCAs. In this case, the accumulators are also required, such that the success criteria becomes operation of both systems. It is thus important to consider both systems in combination. Table 3.6-7 provides a comparison between Zion, the RSS, and the MP 3 failure rates for these systems (Sequoyah does not have the same accumulator system design).

As shown in Table 3.6-7, the failure rates for the systems considered in combination are quite similar, with the MP 3 PSS value being between Zion and RSS. It should also be noted that neither the LPSI nor the accumulator system is a dominant contributor to core melt frequency (see Section 5.3).

It is concluded that the MP 3 assessment of LPSI failure is acceptable within the context of the system influence on overall core melt frequency results.

(8) Main Steam Isolation. The main steam isolation system (MSIV) failure rate assessed in the PSS is somewhat lower (for inside containment steamline breaks) than the only other value found (ORNL precursor study). This difference is less than a factor of 2, however, which is not considered significant.

For breaks outside containment, the difference is somewhat more significant, with the MP 3 value a factor of 8 less than the precursor assessment, which does not distinguish as a function of steamline break location. These differences are not considered significant since a factor of 10 increase in MSIV failure rate would only raise the CMF by 30% (Section 5.3).

(9) Quench Spray. The MP 3 quench spray design is very similar to the containment spray injection designs for the RSS and Sequoyah plants. The MP 3 quench spray failure rate is between the Zion value and the RSS and ORNL precursor values (which are roughly equivalent). The largest disparity is between the RSS and MP 3 values, with the MP 3 rate being about a factor of 8 less than the RSS. However, the RSS failure rate included a large contribution (over 40%) from failure of the consequence limiting control system which monitors plant parameters and actuates the containment spray injection system. The equivalent MP 3 system (designated ESF actuation system) is considered in the event trees as a separate failure. In view of these differences, the MP 3 value seems reasonable.

Table 3.6-7 Comparison of low pressure safety injection system failure rates.

System	Failure Rate		
	MP 3 PSS	Zion PRA	RSS
LPSI	1.7E-4	4.7E-4	4.2E-3
Accumulator	1.9E-3	7.2E-4	9.5E-4
Total	2.1E-3	1.2E-3	5.2E-3

(10) Safety Injection Pump Cooling System. No independent failure rate values for this system were found in documents reviewed for the comparison.

(1I) Charging Pump Cooling System. No independent failure rate values for this system were found in documents reviewed for the comparison.

(12) Low Pressure Recirculation System. The MP 3 PSS assessment of the LPRS failure rate corresponds very closely to all other values in Table 3.6-6 and is therefore considered reasonable.

(13) High Pressure Recirculation System. The MP 3 PSS value for the HPRS is very nearly the same as the RSS and Sequoyah results and is therefore considered reasonable.

(14) Containment Recirculation Spray System. The MP 3 PSS value is comparable to the Zion rate. No other equivalent rates were found. The MP 3 rate is also comparable to those of other recirculation systems considered previously. It is therefore concluded that the MP 3 CRSS failure rate is reasonable.

(15) Service Water System. The MP 3 service water failure was assessed for the 24-hour period following the initiation of an accident during which service water is assumed to be required to maintain cooling of essential safety equipment. The MP 3 SWS failure rate is much higher than Zion (a factor of 338) and also higher than the equivalent Oconee RSSMAP (Ref. 3.6-5) rate by a factor of 100 (obtained by converting the Oconee yearly rate to a 24-hour rate). However, for the 24-hour period assumed as the mission time, the failure probability is so low that SWS failure does not contribute to any dominant accident sequence. Therefore, assuming a lower rate would have no effect on the probability of any dominant sequence.

It is of interest to note that a second independent assessment of SWS failure is included in the MP 3 PSS in Appendix 1-D. This failure rate was assessed in the context of SWS failure as an initiating event. Since the service water system cools a large number of both normally operating and emergency equipment (see Section 9.2 of Ref. 3.6.15 for details), sustained SWS failure would appear to lead to core melt if either auxiliary feedwater fails independently or a reactor coolant pump seal LOCA occurs as a result of the SWS failure.

The PSS Appendix 2-F assessment of SWS concludes that the failure rate of the SWS is 8.68E-12/hour, much lower than the Table 3.6-6 rate (taken from Section 2.3 of the PSS) which would be 3.1E-7/hour. Further, the Appendix 2-F assessment concludes that simultaneous plugging of the SWS inlet screens is not a credible event, while Section 2.3 assumes that this failure mode is the only credible failure mode. If the Section 2.3 rate is used to compute an annual frequency of SWS failure as an initiating event, a value of 2.7E-3/year is obtained, compared to 7.6E-8/year based on Appendix 1-D. This is a very large discrepancy of potentially significant proportions especially if reactor pump seal LOCAs are likely as a result of SWS failure. It should be noted that the Section 2.3 rate of 2.7E-3/year is considerably higher than the Oconee assessment from Table 3.6-6. A recent assessment of events in service water systems (Ref. 3.6-16) indicates that a number of problems have occurred, including a complete failure (which was recovered in time to preclude serious consequences) in approximately 200 reactor-years of experience surveyed.

In discussing this issue with NU in December 1983, it was pointed out by NU that the Section 2.3 assessment in the PSS includes no credit for recovery of the SWS in the event of screen plugging, while PSS Appendix 1-D discusses the basis for and quantifies credit for screen plugging recovery. Furthermore, NU contended that SWS failure would not result in reactor pump seal failure since the component cooling water system could be drained for an extended length of time providing sustained cooling to the reactor pump seals by maintaining flow through the heat exchanger which provides cooling to the seal cooling system. This means that core melt from SWS failure would not likely occur unless auxiliary feedwater failure also occurs.

On balance, it appears that SWS failure is not a significant contributor to core melt frequency either as an initiating event or as a support system failure following other initiating events.

3.6.3 Requantification of Accident Sequences Based on System Failure Rate Revisions

This section provides an estimate of the change in core melt frequency as a result of revisions to the MP 3 PSS system failure rates which appear justified based on the preceding discussion. Two such changes are considered: (1) an increase of a factor of 5 in the emergency power system failure rate based on a revised failure rate for the diesel generators, and (2) an increase of a factor of 10 in the auxiliary feedwater system failure rate which is judged to apply only to the first year or two of operation.

Table 3.6-8 provides the results of the requantification. The results indicate that the core melt frequency would be increased about a factor of 3 over the MP 3 PSS value for the first year or two of operation and would be only slightly higher thereafter.

It should be emphasized that these changes are valid only if the revisions are considered separately; that is, no other changes suggested elsewhere in this review are considered.

3.6.4 References for Section 3.6

3.6-1 I. A. Papazoglou et al., Brookhaven National Laboratory, "National Reliability Evaluation Program (NREP) Procedures Guide," USNRC Report NUREG/CR-2815 (Final Draft), September 9, 1982.

3.6-2 D. D. Carlson et al., Sandia National Laboratories, "Interim Reliability Evaluation Program Procedures Guide," USNRC Report NUREG/CR-2728, January 1982.

3.6-3 Commonwealth Edison Company, "Zion Probabilistic Safety Study," 1981.

Table 3.6-8 Requantification of core melt frequency based on revisions to system failure rates.

	System failure rates		Core melt frequency
	Emergency power	Auxiliary feedwater	
1. Current MP 3 PSS	4.56E-4	6.8E-5	4.5E-5
2. Revised diesel generator failure rate	2E-3	6.8E-5	5.1E-5
3. Same as 2 above with revised AFS failure rate[a]	2E-3	6.8E-4	1.3E-4

[a] Noted to apply only to the first year or two of operation.

3.6-4 P. J. Amico et al., Science Application, Inc., "Interim Reliability Evaluation Program: Analysis of the Millstone Point Unit 1 Nuclear Power Plant," USNRC Report NUREG/CR-3085, February 1983.

3.6-5 D. D. Carlson et al., Sandia National Laboratories, "Reactor Safety Study Methodology Applications Program: Sequoyah #1 PWR Power Plant," USNRC Report NUREG/CR-1659, February 1981.

3.6-6 J. W. Minarick and C. A. Kukielka, Science Applications, Inc., "Precursors to Potential Severe Core Damage Accidents: 1969-1979, A Status Report," USNRC Report NUREG/CR-2497, June 1982.

3.6-7 U.S. Nuclear Regulatory Commission, "Reactor Safety Study - An Assessment of Accident Risks in U.S. Commerical Nuclear Power Plants," USNRC Report WASH-1400 (NUREG-75/014), October 1975.

3.6-8 J. J. Raney, Ebasco Services, Inc., "Auxiliary Feedwater Systems Reliability," presented at International Meeting on Thermal Nuclear Reactor Safety, August 29-September 2, 1982, Chicago, IL, USNRC Conference Proceeding NUREG/CP-0027.

3.6-9 R. E. Battle et al., "Reliability of the Emergency AC Power System at Nuclear Power Plants," presented at International Meeting on Thermal Nuclear Reactor Safety, August 29-September 2, 1982, Chicago, IL, USNRC Conference Proceeding NUREG/CP-0027.

3.6-10 G. J. Kolb et al., Sandia National Laboratories, "Reactor Safety Study Methodology Applications Program: Oconee #3 PWR Power Plant," USNRC Report NUREG/CR-1659, May 1981.

3.6-11 C. L. Atwood, EG&G Idaho, Inc., "Data Analysis Using the Binomial Failure Rate Common Cause Model," USNRC Report NUREG/CR-3437, September 1983.

3.6-12 J. P. Poloski and W. H. Sullivan, EG&G Idaho, Inc., "Data Summaries of Licensee Event Report of Diesel Generators at U.S. Commercial Nuclear Power Plants,: USNRC Report NUREG/CR-1362, March 1980.

3.6-13 G. L. Boner and H. W. Hanners, University of Dayton, "Enhancement of On-Site Emergency Diesel Generator Reliability," USNRC Report NUREG/CR-0660, February 1979.

3.6-14 J. A. Haried, Oak Ridge National Laboratory, "Evaluation of Events Involving Service Water Systems in Nuclear Power Plants," USNRC Report NUREG/CR-2797, November 1982.

3.6-15 Northeast Utilities, "Final Safety Analysis Report, Millstone Unit 3," 1982.

3.7 Operating Experience Analysis

The use of failure data derived from operating experience is vital to the validity of any PRA analysis. In the Millstone PSS operating experience provided an important source of input for determining the frequency of initiating events, random failure rates, and operator errors. This section provides a review of the use of operating experience in the PSS in each of these areas.

The Millstone 3 plant is still in the final stages of construction, so we have no data on failures at Millstone 3. Thus, failure data must generally come from industry-wide sources. But operating experience indicates that some failure and unavailability rates can vary widely from plant to plant, and we do not know whether Millstone will be above or below average. Nevertheless, recent advances have been made by the industry in identifying below-average design, maintenance, test and operation procedures. This has come about through study of LERs and more attention to the plant specific causes of system and component failures. To the extent that these activities represent improvements, a new plant such as Millstone 3 can and would be expected to take advantage of this experience to improve its performance over the average performance of plants already running.

3.7.1 Initiating Events

Twenty-two initiating events (in 21 classes) are identified in the Millstone PSS as events that could lead to core damage. Since Millstone 3 is not an operating plant, no plant-specific operating experience is available for incorporation into the data analysis for initiating events. However, site-specific information was used for the loss of offsite power event. Estimates of initiating event frequency distributions were based largely on PWR experience. Sources used in this analysis include an Electric Power Research Institute (EPRI) compilation of transient data, (Ref. 3.7-1) an Oak Ridge National Laboratory (ORNL) report on loss of offsite power experience, (Ref. 3.7-2) and WASH-1400 (Ref. 3.7-3).

A Bayesian analysis was performed in order to estimate the loss of offsite power frequency for Millstone 3. We reviewed this calculation and conclude that it could be optimistic. The analysis uses data on the loss of offsite power at all U.S. reactors. The method used matches the moments of this population data to the moments of an assumed lognormal prior distribution. The Millstone site-specific data used in the PSS (one loss-of-offsite power in seven years) is then incorporated to form a posterior distribution that is used as the event frequency. The difficulty with this analysis is that the use of all U.S. reactors as a prior distribution could be optimistic. The loss of power occurrence for plants on the Northeast Inter-tie, which is exposed to a higher incidence of hurricanes and other severe weather, might be a more appropriate choice for the prior distribution or at least for the Bayesian update. We estimate that, if performed in this manner, the calculated frequency of loss of offsite power would increase by as much as a factor of two.

For those initiating events in which the PWR population provided data points, a classical statistics treatment was used to estimate the frequency of the particular initiating event. In these cases, the initiating event frequency was treated as a random variable whose distribution reflects inherent plant-to-plant variability. The distributions are assumed lognormal. The initiating events for which this classical treatment was used are listed in Table 3.7-1.

For those initiating events in which available data were limited (those events which have not occurred) a Bayesian appproach was used to estimate the distribution for the frequency of an initiating event. A prior distribution was developed based on WASH-1400 distributions. These distributions were then updated, based on the observation of zero occurrences in 213 years of U.S. PWR operating experience. The resulting distribution was used to estimate the frequency of a particular initiating event. This approach was used in both the Indian Point (Ref. 3.7-4) and Zion (Ref. 3.7-5) PRA studies. The initiating events that were given a Baysian treatment are listed in Table 3.7-1. The remaining initiating events were considered unique to the Millstone 3 plant, thus no data exist. The estimate of the initiating event frequency in each case was based on a specific analysis for that system.

Aside from our concern that the loss of offsite power may be underestimated by a factor of two, we found no major concerns regarding the operational data analysis for initiating events. However, one item of minor concern is the use of classical estimation for events which have had a small and perhaps statistically insignificant number of occurrences, such as small LOCAs and steam tube rupture. For these cases the use of classical estimation for event frequency could lead to optimistic results relative to the Bayesian estimate.

3.7.2 Component Failures

The component failure rate data used in the Millstone 3 PSS was obtained from three sources: WASH-1400 (Ref. 3.7-3), NREP (Ref. 3.7-6), and the Westinghouse Nuclear Technology Division (WNTD) data base. Most of the component failure rates were derived from WNTD. This data base is described as proprietary and is not provided as part of the Millstone 3 PSS documentation. This data base is described as being based extensively on Westinghouse nuclear plant experience and contains over 200 reactor years of plant operating experience. Additional discussion of component failure rate data is provided in Section 3.6 (Failure Data).

3.7.3 Human Errors

Human error is another area in which the use of operating experience is both a necessity and a source of potentially large uncertainties. In treating human error, the PSS used NUREG/CR-1278 (Ref. 3.7-7) for most of its human factors failure data. Although this document has industry-wide acceptance in general, the data in it contains a great deal of uncertainty. In particular, the failure data are lumped into broad categories whose applicability to specific situations at Millstone 3 is only approximate. In addition, it is of course not known how Millstone's operators will respond compared to industry averages.

Table 3.7-1 Dependence of Millstone initiating events on operating experience.

Initiating events that use site-specific operating experience:

Loss of offsite power

Initiating events that use a classical treatment of operating experience data:

Small LOCA
Steam generator tube rupture
Steamline break outside containment
Loss of reactor coolant system flow
Loss of main feedwater flow
Primary to secondary power mismatch
Turbine trip
Reactor trip
Core power excursion
Spurious safety injection

Initiating events that use a Bayesian treatment of operating experience data:

Large LOCA
Medium LOCA
Steamline break inside containment
Incore instrument tube rupture

Unique initiating events:

Special large LOCA initiators
Loss of a single service water train
Loss of a single vital DC Bus
Total loss of vital DC power
Loss of vital AC bus 120-VAC-1 or 120-VAC-2
Loss of vital AC bus 120-VAC-3 or 120-VAC-4
ATWS

Additional discussion of human error failure data and its use in Millstone accident sequences is provided in Section 3.5.

3.7.4 Concluding Remarks on Operating Data Analysis

Despite the limitations discussed above it is our conclusion that the Millstone 3 PSS under review has used state-of-the-art data bases generally. There are cases where we have reservations about specific numerical values. It appears that the value used for loss-of-offsite power based on operating experience may underestimate this occurrence by as much as a factor of two. The use of classical statistics for estimating the frequency of events such as steam generator tube rupture, for which there have only been a handful of occurrences, is likely to provide results that are at best highly speculative. These events could have received a better analysis. Nonetheless, we conclude that the operating experience analysis provides a generally acceptable basis for estimating accident probabilities at Millstone 3.

3.7.5 References for Section 3.7.

3.7-1 Electric Power Research Institute, "ATWS: A Reappraisal, Part 3: Frequency of Anticipated Transients," EPRI Report NP-2230, January 1982.

3.7-2 F. H. Clark, "Loss of Offsite Power Experience,: unpublished report, 1981.

3.7-2 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.

3.7-4 Pickard, Lowe and Garrick, Inc., "Indian Point Probabilistic Safety Study," prepared for Power Authority of the State of New York, and Consolidated Edison Company of New York, Inc., 1982.

3.7-5 Commonwealth Edison Company, "Zion Probabilistic Safety Study," 1981.

3.7-6 I. A. Papazoglou et al., Brookhaven National Laboratory, "National Reliability Evaluation Program (NREP) Procedures Guide," USNRC Report NUREG/CR-2815 (Final Draft), September 9, 1982.

3.7-8 A. D. Swain and H. E. Guttman, Sandia National Laboratories, "Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Application," USNRC Report NUREG/CR-1278, September 1980.

3.8 Analysis Codes

3.8.1 Introduction

This section discusses the computer codes that were used to quantify fault trees for the Millstone 3 PSS, since these were the only accident sequence probability codes described in the study. The PSS does not describe any computer codes that were used to quantify the overall damage state probabilities even though it is likely that some computer analysis was used for this process (see Section 3.11). This section does not include a discussion of codes used for accident analysis -- i.e. COCO-class 9, CORCON-MOD1, and MODMESH.

The WAM series codes, WAMBAM (Ref. 3.8-1), and WAMCUT (Ref. 3.8-2), were used in the Millstone PSS for fault tree quantification. These codes were used to determine minimal cut sets for each fault free. Minimal cut sets give all the unique combinations of primary events that cause system failure, and are used to calculate the system unavailability for all support states. WAMBAM was used for preliminary point estimate calculations of system unavailability and failure probability. WAMCUT was used to derive cutsets and to develop the appropriate uncertainty values.

In general, fault tree analysis codes provide two approaches for calculating minimal cut sets (Ref. 3.8-3). One is deterministic; the other is a Monte Carlo approach. The deterministic method uses Boolean-algebra principles to sort through the fault tree structure, which is first encoded in a suitable format. This method is rigorous and accurate, but can consume a great deal of computer storage and processing time. The Monte Carlo approach randomly selects the events in the fault-tree and combines them to test whether the fault tree logic is satisfied. When an event combination has been selected that satisfies the logic, a cut set has been established. This method is less accurate but often faster in terms of computer time. Both WAMBAM and WAMCUT use a deterministic approach for calculating cut sets.

3.8.2 WAMBAM

WAMBAM is designed to calculate the point probabilities for top events in a fault tree. It actually consists of three codes: WAM, WAMTAP, and BAM. The cut set evaluation is carried out in BAM (Boolean Arithmetic Model). WAM and WAMTAP serve as input preprocessors for BAM. The WAM preprocessor is designed to ease the input description of the fault tree and the event probabilities. If requested, the input to BAM can be saved and subsequently modified by WAMTAP. WAMTAP allows the probability of single or grouped primary events to be changed for sensitivity studies.

The evaluation code BAM calculates the probabilities of all operating and nonoperating states for a system. Operations within a system are modeled as gates on a fault tree. The probability of the top event is computed by forming a truth table, each line of which represents a product term (P-term) event disjoint from all other P-terms. The product of the probabilities of the events in each P-term gives the probability of the P-term, and the union of the applicable P-terms gives the probability of the top event. BAM reduces storage requirements by eliminating low-probability paths at an intermediate stage of the processing and at the same time keeps track of the total of the discarded paths.

3.8.3 WAMCUT

WAMCUT was used in the Millstone PSS to derive cut sets and to develop appropriate uncertainty values. WAMCUT is designed to obtain minimal cut sets and to quantify the top events of fault trees. It consists of two parts: WAM and CUT. WAM is a preprocessor that reads the fault tree description and checks for logic and syntax errors. CUT is the cut set finder routine that takes the restructured input fault tree from WAM and finds the cut sets of each gate, working from the bottom to the top of the tree. the output of this code includes a list of cut sets and the probability of each. Also included is the variance of each cut set. The deterministic approach for finding cut sets is similar to WAMBAM.

WAMCUT also eliminates low probability paths at an intermediate stage of processing. The system fault trees for Millstone were quantified with WAMCUT using a specified cut-off value (typically 1E-7). Only cut sets whose probabilities are greater than or equal to the cut-off value were analyzed.

3.8.4 Comments

There are some minor limitations to the use of WAMCUT in the Millstone PSS. Some codes offer the ability to move replicated events up as far as possible toward the top of the fault tree without violating Boolean-algebra rules. The use of such an option in applying WAMCUT to Millstone fault trees might have eliminated some of the inaccuracies that have been noted above. Also, WAMCUT does not provide failure probabilities for intermediate gates in the fault tree. This information would have been useful for auditing these trees. Finally, one can question whether eliminating cut sets on the basis of probability without considering variance would limit the ability of an uncertainty analysis to incorporate those events which have a low probability but large variance.

3.8.5 References for Section 3.8

3.8-1 F. L. Leverenz and H. R. Kirch, Science Applications, Inc., "User's Guide for the WAM-BAM Computer Code," Electric Power Research Institute Report EPRI-217-2-5, 1976.

3.8-2 F. L. Leverenz and H. R. Kirch, Science Applications, Inc., "WAMCUT- A Computer Code for Fault Tree Evaluation," Electric Power Research Institute Report EPRI NP-803, 1978.

3.8-3 U.S. Nuclear Regulatory Commission, "PRA Procedures Guide - A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants," USNRC Report NUREG/CR-2300, January 1983.

3.9 Accident Sequences

This section provides the results of a review of the MP 3 PSS assessment of the progression of accident sequences. The review encompassed an examination of assumptions, analysis, and predicted phenomena associated with the progression of severe accidents as considered in the PSS. The review is limited to considerations of accident progression within the primary system and reactor vessel cavity. It does not consider other phenomena in the containment such as H_2 combustion, overpressure failure, and basemat penetration.

A discussion of accident sequence analysis occurs in Section 4, Volume 8 of the MP 3 PSS and related appendices in Volumes 8 and 9 (Appendices 4-A through 4-N). In addition, as part of the accident sequences review, Section 3 ("Analysis of Recoverable Degraded Core Cooling Sequences") and the related Appendix 3-A ("In-Vessel Debris Coolability") was reviewed.

It should be noted that much of the phenomena associated with the progression of severe accidents is not well understood. Thus, considerable engineering judgment is required in estimating the realistic progression of such accidents, and disagreement exists among investigators. (On-going research is expected to help resolve much of the uncertainty.) In the discussion which follows, an attempt has been made to clearly delineate those issues which are subject to differences in judgement and those for which some data base exists.

The format of this section consists of: (1) a listing of significant comments generated as the result of the review, (2) a listing of conservative assumptions and analysis as described in the PSS, and (3) a summary evaluation which attempts to develop an overall conclusion regarding the significance and implications of individual elements in (1) and (2). The conservative assumptions are listed and evaluated in order to provide additional perspective.

3.9.1 Comments on MP 3 PSS Assessment of Accident Sequences

This subsection provides comments on Section 4 of the MP-3 PSS, as follows:

(1) Page 4.2-3. Failure of containment isolation is considered as a containment failure mode. The probability of such a failure is quantified in Section 4.7.1 where a value of 1E-4/demand is assigned. While the PSS argues that operation of a sub-atmospheric containment precludes the possibility of significant pre-existing undetected penetration openings, very little justification is given for the 1E-4 value. No fault tree is provided, and very little description is given of the isolation system. While such a low failure rate may be justified, it cannot be evaluated from information provided. In view of the very important role long-term containment integrity assumes in the MP 3 PSS and considering the rather poor experience which has been observed with penetration/isolation systems (Refs. 3.9-1, 3.9-2), it appears that further analysis to justify the low failure rate is required (Ref. 3.9-2 suggests a general failure rate for PWRs of 0.1 for leakage being beyond technical specification limits).

(2) Section 4.3.1.5. This section covers the failure scenarios postulated for the reactor vessel during core melt progression. However, there is no consideration here (and none could be found elsewhere in the PSS) of the potential for primary system failures preceding reactor vessel melt-through. Such failures could have a significant impact on containment response and source terms. The most likely conditions for such failures are during accidents wherein the primary system pressure remains at or near the pressurizer relief valve setpoint. (Many important sequences result in these conditions.) Under these conditions, the entire primary system will be heated due to natural convection of steam through the core. Additional heating would occur from release of hot hydrogen gas after metal-water reaction commences. Eventually, some parts of the primary system may become hot enough to fail under the elevated pressure conditions. Steam generator tubes may be susceptible to such failure, particularly if some are in a degraded condition. Such failures would be particularly onerous since a fission product pathway directly to the atmosphere (through the steam generator relief valves) could result.

In a recent analysis (Ref. 3.9-3), the possibility of such primary system failures was suggested. Steam generator tube failures as well as primary piping and reactor vessel ruptures were examined. It was concluded that failure of the main coolant pipes would occur when the maximum cladding temperature reached a rather modest 1300°K for the station blackout accident scenario. (This calculation presumably assumed no prior degradation of steam generator tubes.) It was further concluded that the steam generator tubes would be the likely failure point if the secondary side were in a depressurized condition (which could occur from a stuck open relief valve or from operator action in efforts to cool the primary system).

The Ref. 3.9-3 calculations have not been reviewed as part of this effort. However, the results suggest a potentially significant failure mode which should receive further consideration. Overpressure spikes when molten core material drops into residual water in the reactor vessel lower plenum could also contribute to these failures.

(3) Section 4.3. The MP 3 PSS analysis used Westinghouse codes for assessing the containment thermal-hydraulic conditions. In particular, "COCO-Class 9" (Pg. 4.3-49), "CORCON-MOD1, Westinghouse Version", and "MODMESH" were used for various phases of the accident. These codes are not described in detail in the MP-3 PSS, and very little information was provided to verify their capability. They do not appear to have been subjected to extensive peer review or to have been assessed against experimental data. As a result, the results have not been, and probably cannot be, fully evaluated as part of this review. While no obvious problems appear to exist, it is not possible to conclude that the analyses are valid.

(4) General. There appears to be an inconsistent and somewhat confusing discussion at various locations in Section 4 with respect to the operability of the recirculation spray system without previous operation of the quench spray. On Page 2.2.7-1 it states, unequivocally, that recirculation spray failure was assumed if quench spray failed. However, on Page 4.4-15 recirculation spray is considered operable for "T" sequences, and on Page 4.4-27 recirculation spray only cases are considered for sequences AEC", ALC", SEC", SLC", and TEC". Furthermore, it is stated that for these sequences, the accumulator water would be available for these sequences when recirculation spray is actuated, but this water would not be available until after RV failure (and subsequent depressurization) and then only if accumulator water is vaporized and condensed on the containment walls. The question of sufficient NPSH for these sequences appears not to be addressed.

(5) General - Analysis of Recoverable Degraded Core Cooling Sequences Section 3, Vol, 7). This section, in general, appears to be reasonable. While several questionable and insufficiently justified assumptions appear to have been made, none of these seem overly significant. Further, the PSS consideration of recoverable core cooling sequences has very little significance to the results.

(6) General. There is no consideration in Section 3 of a recoverable degraded core condition in conjunction with the V-sequence accident scenario. In view of the PSS estimate of the fact that the V-sequence accident is an important contributor to risk, this omission seems significant. Further, there appear to be opportunities to interrupt the progression of the V-sequence accident and restore adequate core cooling. It should be noted that no PRA to date has considered this type of recovery.

A comprehensive review of this accident and the corresponding PSS analysis identified several deficiencies in the PSS assessment. One of the most significant is a misleading portrayal of the results and an unrealistic assessment of the accident probability distribution. These problems are considered at length in Section 3.1 and are not repeated here. Additional apparent deficiencies in the PSS relative to the assessment of the V-sequence accident are described below:

a. There appear to be discrepancies in the pipe and valve configuration assumed in the PSS for the RHR suction. This portion of the RHR system was found to dominate the probability of a V-sequence accident. The assessment of the V-sequence probability for this case is provided in PSS Section 1.1.2.1.7. The configuration used in the assessment is reproduced here as Fig. 3.9-1.

According to the PSS Section 1.1.2.1.7 description, the accident would occur upon failure of both valves in either pump suction line. The transition from high pressure to low pressure pipe is shown on Fig. 3.9-1. Thus, rupture could occur inside the containment, but this is conservatively assumed not to occur in the PSS. (Rupture inside containment would not lead to severe offsite consequences since the containment barrier is not breeched.

Figure 3.9-2, which is based on P&ID drawing S&W #12179-EM-112A-1, indicates that a third valve (MV8702A and B) exists in both RHR suction lines. Based on other plant designs, it seems likely that the transition from high to low pressure pipe would occur at the location of these valves rather than inside the containment. If this is the case, the probability of the V-sequence accident would be reduced dramatically since a third valve, normally locked closed, would have to fail. (The S&W drawing does not indicate the design pressure transition point.) If low pressure pipe is located between the inside and outside valves (as implied by the PSS assessment), then there is a possibility of a rupture outside containment. However, depending on relative pipe segment lengths inside and outside the containment, the probability of an outside rupture would be reduced over the PSS value.

b. The PSS description of the progression of the V-sequence accident is very sketchy, and some of the results seem unusual. If the accident were to occur, it appears that the pipe would rupture in the RHR pump cubicle. Following rupture, a high energy blowdown process would ensue. This would likely cause pipe whipping and the generation of high velocity debris in the pump cubicle. It seems

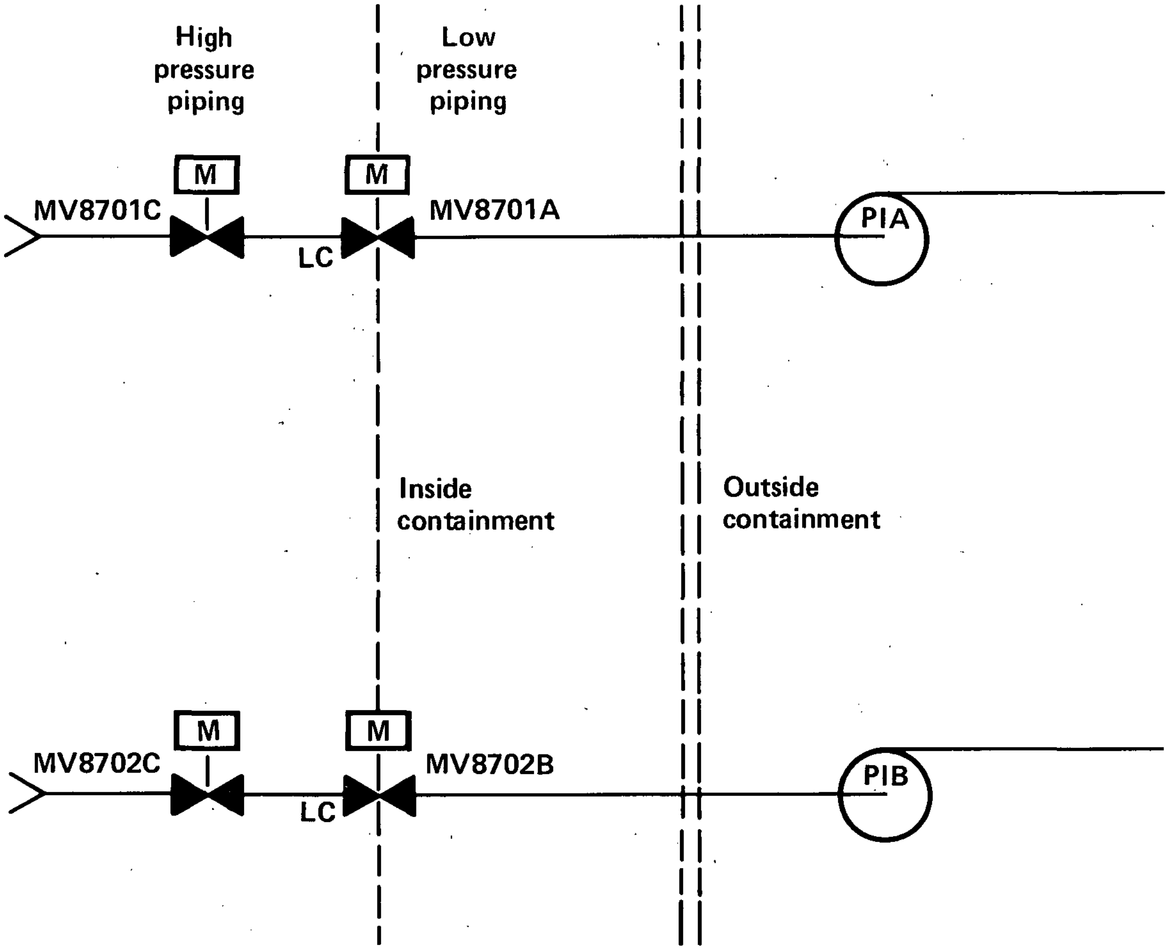


Fig. 3.9-1 MP 3 PSS diagram of RHR suction (reproduced from Fig. 1.1-5 in PSS).

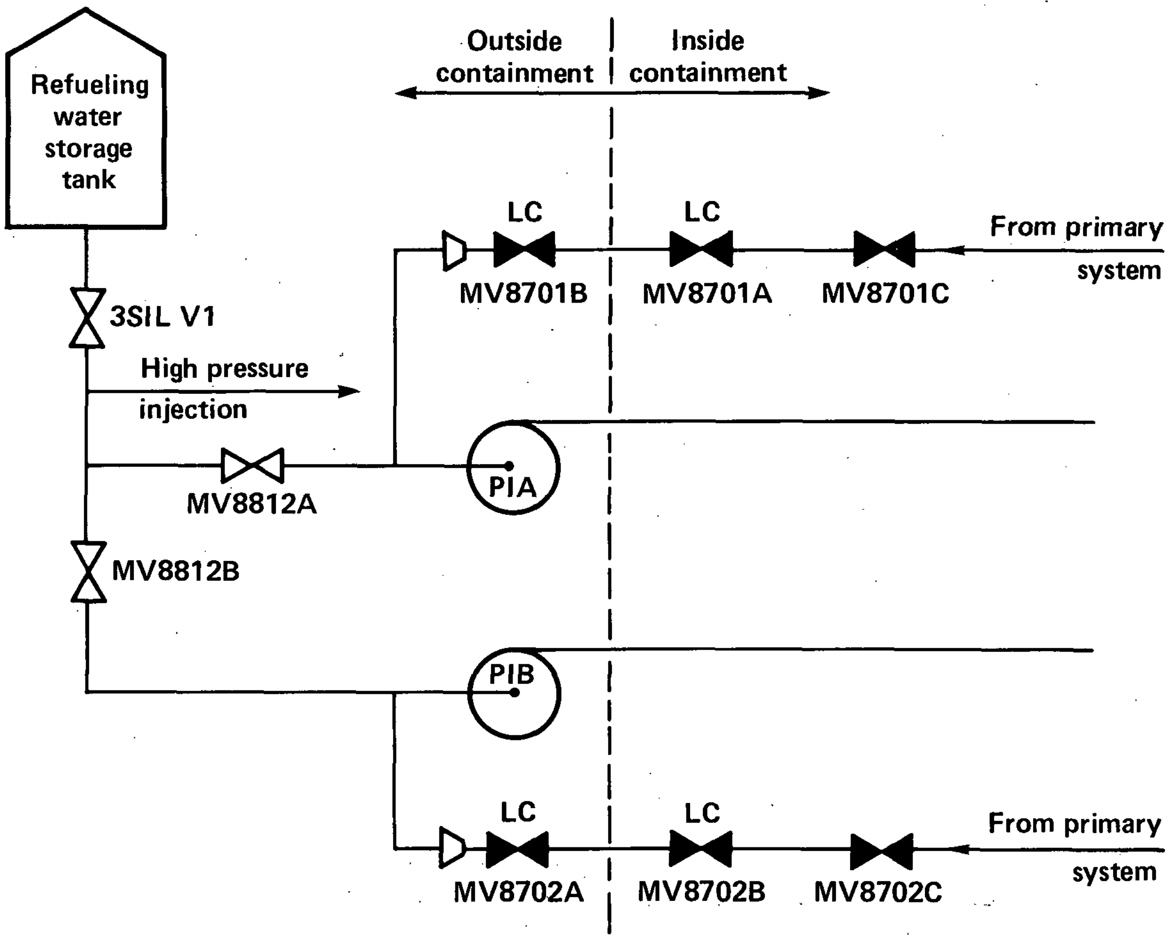


Fig. 3.9-2 MP 3 simplified RHR system from S&W drawing no. 12179-EM-112A-1 (4/14/82).

these events could disable the operation of the RHR pumps even though they would be commanded to start following the rupture. Further, the high temperature steam environment would likely cause the pumps to fail. If they were to operate under these conditions, they would very likely become flooded from the large amounts of water discharged to the area (from blowdown, accumulator discharge, HPIS, drain from the RWST to the break, and LPIS flow).

If the LPIS pumps were to fail, the core would very likely remain cooled from operation of the HPIS. The HPIS run-out flow, assuming operation of both charging and safety injection pumps, is 1700 gpm PSS (Table 4.1-1, Pg. 4.1-4). This is more than adequate to maintain core cooling. (In fact, the PSS states on Pg. 2.2-25 that one high pressure safety injection pump is sufficient to recover from a 6" LOCA.) Assuming a refueling water storage tank volume of 1.2E+6 gallons (Table 4.1-1, Pg. 4.1-13), the core would remain cool for 11.8 hours if the drain from the RWST to the break location is either negligible or terminated by operator closure of valves MV8812A and MV8812B (see Fig. 3.9-2). If the operator throttles down the HPIS flow to conserve RWST water, an even longer time for sustained core cooling could be realized for this scenario. PSS Table IV-5, Pg. IV-31, indicates a radionuclide release time of 2.5 hours for the V-sequence. This value was apparently derived based on full capacity operation of the LPIS which would empty the RWST in about 2 hours.

c. The scenarios described previously for the V-sequence suggest that the accident could be terminated or mitigated. (None of these possibilities were explored in the PSS.) Since about 12 hours may exist before core uncovery occurs, it seems reasonable that an alternate source of water supply to the RWST could be obtained. If so, the HPIS could provide core cooling indefinitely, provided that these pumps do not become flooded from water injected into the LPIS pump cubicle.

It also seems likely that the LPIS rupture may become submerged early in the scenario due to the large amounts of water delivered to the LPIS pump cubicle (see b. above). If core melt occurs while the pipe is submerged, a large fraction of the radionuclides released from the core would be expected to be secured in the water, greatly reducing the source term assumed in the PSS (Table IV-5, Page IV-31) for this accident. Since only small floor drains were found in the LPIS pump cubicle during the plant tour in December 1983, it seems likely that the pipe rupture location would be submerged unless large openings exist in the pump cubicle below the rupture sensitive piping, allowing spillover into adjacent areas.

The preceding discussion suggests that the V-sequence accident is a complex event with many possible outcomes depending on assumptions made and operator actions taken. Figure 3.9-3 qualitatively depicts these alternatives in event tree format. As indicated by the figure, some 20 different outcomes appear feasible. Of these 20, some 17 would appear to result in lower offsite consequences

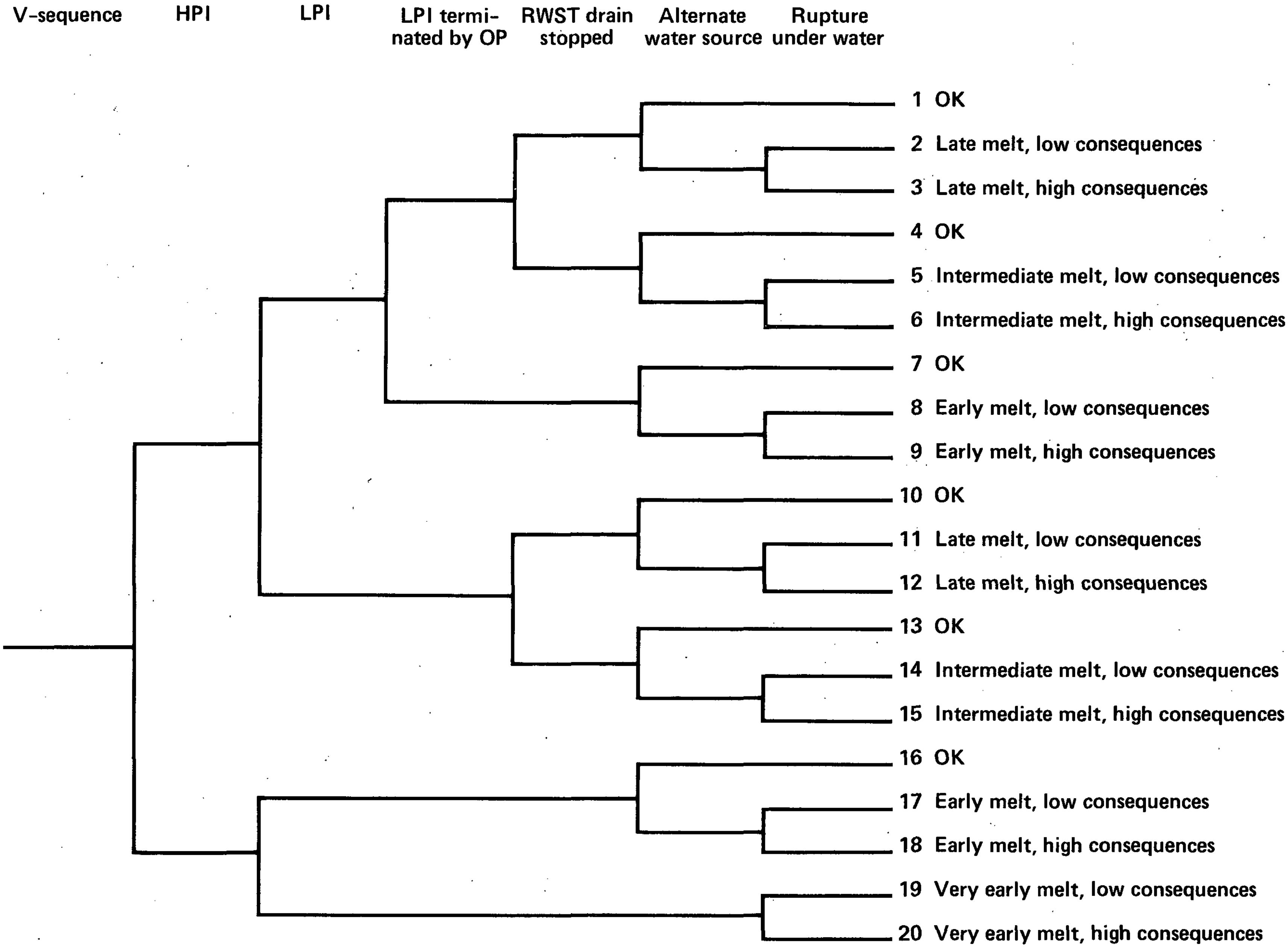

V-sequence
HPI
LPI
LPI terminated by OP
RWST drain stopped
Alternate water source
Rupture under water
1 OK
2 Late melt, low consequences
3 Late melt, high consequences
4 OK
5 Intermediate melt, low consequences
6 Intermediate melt, high consequences
7 OK
8 Early melt, low consequences
9 Early melt, high consequences
10 OK
11 Late melt, low consequences
12 Late melt, high consequences
13 OK
14 Intermediate melt, low consequences
15 Intermediate melt, high consequences
16 OK
17 Early melt, low consequences
18 Early melt, high consequences
19 Very early melt, low consequences
20 Very early melt, high consequences

Fig. 3.9-3 Example event tree for V-sequence

(and therefore lower risk) than assumed in the PSS due to either sustained core cooling, delayed melt, or removal of radionuclides from a submerged rupture. The only scenario apparently considered in the PSS is No. 9 in Fig. 3.9-3. Quantification of the event tree in Fig. 3.9-3 would require additional effort and detailed knowledge of plant design features.

3.9.2 Conclusions

The major findings from review of the PSS assessment of accident sequences are as follows:

(1) No consideration is included of primary system failure prior to vessel melt-through.

(2) The analysis of the V-sequence accident is more conservative than it needs to be, in that opportunities for terminating and mitigating the accident were not credited.

(3) The remaining deficiencies, listed below, do not appear significant:

- Inadequate support for containment isolation failure probability
- Lack of assessment for codes used in core melt progression calculations
- Inconsistent assessment of operability of containment recirculation sprays
- Lack of justification for some degraded core cooling recovery assumptions,

3.9.3 References for Section 3.9

3.9-1 D. W. Sams and M. Trojovsky, EG&G Idaho, Inc., "Data Summaries of Licensee Event Reports of Primary Containment Penetrations at U.S. Commercial Nuclear Power Plants," NUREG/CR-1730, September 1980.

3.9-2 M. B. Weinstein, "Primary Containment Leakage Integrity: Availability and Review of Failure Experience", Nuclear Safety, Vol. 21-5, September-October 1980.

3.9-3 L. Winters, "RELAP 5 Station Black-Out Transient Analysis in a PWR," Energieonderzoek Centrum Nederland, July 1982.

3.10 Dependencies

This section presents the results of a review of the consideration and treatment of dependencies in the MP 3 PSS. The actual meaning of "dependencies" is somewhat vague and occasionally inconsistent within the risk assessment community. Generally, dependencies can be defined as initiating events or system and component failures which are related to or have a detrimental influence on the probability of successive failures. Failures involving dependencies have been found to be very important to nuclear reactor risks, both in PRA studies and in actual accidents. The TMI-2 and Brown's Ferry accidents are examples of actual occurrences which have involved dependencies.

The MP 3 PSS used the large event tree-small fault tree methodology, where support states are defined for various conditions of initiating event occurence and system or train availability, i.e., specific definitions of certain combinations of dependencies. The eight support states used in the PSS are defined in Table 3.10-1, where it can be seen that the initiators are split between loss of offsite power events and all other initiatiors.

It is usually convenient and useful to subdivide the general area of dependencies into more explicit sub-issues. The subdivision chosen for the purposes of the MP-3 review was that recently proposed by Fleming, et al. (Ref. 3.10-6). In this case, three subdivisions are used, defined as follows:

(1) Common Cause Initiating Event. In this case, an initiating event occurs which simultaneously causes multiple system failures and/or degrades systems, increasing their unavailability. The most dramatic examples of this type of dependency are external events, such as earthquakes, which can cause multiple system degradations. However, some important internal initiating events, such as loss of offsite power, can represent important internal initiating events with dependencies.

(2) Intersystem Dependency. In this case, a system failure occurs which causes the simultaneous degradation (either failure or an increase in unavailability) of other systems. An example of such a failure would be the service water system (see Sect. 3.6) which causes the eventual loss of numerous components which depend on SWS for cooling.

(3) Intercomponent Dependency (Common-Cause Failure). This dependency involves the simultaneous (or near simultaneous) failure of components from the same cause. This type of dependency is often referred to as common-cause failure, a term which will be used in the remainder of this section. An example of common-cause failure would be the simultaneous failure to start of pumps in a multi-train system due to seized pump shafts from excessive corrosion. In the MP 3 PSS, these three types of dependencies are not all considered separately. Rather, a discussion of each type is considered in various locations, with special cases of each type also considered. These discussions include the following:

- PSS Vol. 3, Part 1 of 4, Section 2, "Plant and Systems Analysis" (particularly Sections 2.2.1, 2.2.3, and 2.2.5),
- PSS Vol. 6, Appendix 2-C, "Common Cause Failure Analysis",
- PSS Vol. 6, Appendix 2-F, "Analysis of Common Cause Service Water Strainer Plugging",
- PSS Vol. 6, Appendix 2-G, "Analysis of Common Cause Actuating System Logic Unavailability".

The remainder of this section evaluates separately the three types of dependencies as considered in the MP 3 PSS. External events and related dependencies are excluded here, but are considered in Chapter 4 of this report.

Table 3.10-1 Support state definitions.

Symbol	Definition
(1)	All support systems available
(2)	One support trains unavailable
(3)	Both support trains unavailable
(4)	All ESF signals unavailable
(5)	LOSP, all support systems available
(6)	LOSP, one support train unavailable
(7)	LOSP, both support trains unavailable
(8)	LOSP, all ESF signals unavailable

3.10.1 Common-Cause Initiating Event

Considerable attention has been given to initiating event dependencies for internal events since the publication of the Reactor Safety Study (Ref. 3.10-2). The role of such dependencies appear to have been recognized and appropriately considered in PSS Section 2, Vol. 3, with the following exception:

- It was assumed that the power conversion system would be isolated and unavailable for all transient initiating events. This is a conservative assumption which is considered further in Section 3.1. In actuality, it appears that the PCS would be available for many transients and could serve as a system for core cooling.

In reviewing PSS Section 2.2, a number of inconsistencies and errors were found which appear to be minor. They are as follows:

(1) Figure 2.2.3.2-5. There appears to be an incorrect double entry ("Failure of Either Pressurizer PORV Block Valve to Open") on this fault tree.

(2) Page 2.2-45. The quantity Q (TK) in Eq. 2.2.3.3-2 is not defined, and the quantity Q (TR) is not in Eq. 2.2.3.3-2.

(3) Page 2.2-50, Item 7. Pressure relief failure during ATWS is stated to be dominated by failure of pressurizer relief valves to close. It is not clear how this failure causes failure of the overpressure function.

(4) Page 2.2-65. It is stated here that "..only the loss-of-offsite-power initiator was adjudged to have the potential for initiating an accident and then influencing the accident progression sequence." The interfacing systems LOCA accident initiator is an even more important example of this type, wherein the LPIS is failed and the containment is bypassed.

(5) Table 2.2.1.3.1-1 (Pg. 2.2-76). Does not include the support systems which provide pump room cooling or lube oil and lube oil cooling for any

plant systems. It is not clear that these support systems have been determined to be unnecessary for the plant systems. They have been found to be important in other PRAs.

(6) Item 3 on Page 2.2.7.1-8. Indicates that cooling is necessary for high pressure injection pumps. However, no such dependency is indicated in Table 2.2.1.3.1-1 on Page 2.2-76.

(7) On Page 2.2.714B-4. A loss of AC power scenario is described, with operation of the steam generator PORVs in conjunction with the turbine-driven AFW pump utilized to depressurize the primary system. However, on page 2.2.7.14B-2 it is stated that "...potentially the steam generator PORVs would be disabled by the loss of AC power...".

A number of conservative assumptions were found in the review of PSS Section 2.2 even though on page 2.2-24 it is stated that "The ultimate objective...is to present realistic estimates of public risk...". These can tend to bias the risk towards a high value and should be considered for proper perspective in PRA reviews. These conservatisms are listed in Table 3.10-2. The table includes the location in the PSS where the conservatism is described and an assessment of the potential significance.

3.10.2 Intersystem Dependency

This subsection provides a brief overview of the results of an assessment of the MP 3 PSS method of accounting for intersystem dependencies.

The Millstone 3 PSS uses support states to represent the dependencies of front-line systems on support systems. A major assumption in this method is that no subtle interfaces or interactions within or between the various support system trains exist. That is, the support system trains are truly independent and affect only the associated front-line system trains. This is the design philosophy for the plant. However, other studies which have done more rigorous analysis of support system interfaces through the propagation of the connections through detailed fault tree models, e.g. - the interim reliability analysis program (IREP) studies, have shown that this assumption is not always valid. While there are no obvious deficiencies in this area in the PSS, it is beyond the scope of this review to invest the required effort to determine if any subtle dependencies exist which were missed. There is no easy way to determine if anything of significance was omitted. This would require using fully integrated fault trees for each accident sequence or performing a separate component level systems interaction study.

Another problem area comes from the need to combine the many different possible support states into a much smaller number of simplified support states. These simplified support states consist of collections of actual support states which are similar in their effect on the plant response, but not completely identical. The assumption made in the analysis is that they are similar enough to be treated equally and that the effects of any simplified support state on the plant response are taken to be the effects of the most limiting actual support state in the group. This may add an element of conservatism in the analysis. However, this is a simplification which may or may not be valid and which is beyond the scope of this review to evaluate. In either case, it can be stated that this treatment does not accurately

Table 3.10-2 Conservatisms claimed in PSS System Analysis.

Item	Location in PSS	Significance	Comments
1. Using 8 "support states" to represent all combinations of support systems.	Vol. 3, Pg. 2.2-12	Undetermined	PSS claims 8 support states conservatively used to bound 72 states initially identified.
2. Several actuation signals, plant systems, and operator actions not modeled.	Vol. 3, Pg. 2.2-19	Could be significant	PSS Pg. 2.2-20 lists examples of these.
3. Some success criteria utilized conservative FSAR analysis.	Vol. 3, Pg. 2.2-23	Probably not significant since important sequences used realistic analysis.	
4. PORV block valves assumed closed during operation.	Vol. 3, Pg. 2.2-32 and Pg. 2.2-52	25% reduction in failure of feed and bleed.	During plant tour of October 1983, PORV block valves were stated to remain open during operation.
5. Failure of RT-4 (manual or automatic reactor trip) results in core melt.	Vol. 3, Pg. 2.2-49	Appears not significant..	
6. All three pressurizer relief valves assumed to lift during ATWS.	Vol. 3, Pg. 2.2-50	Not significant (ATWS sequences do not contribute to risk).	
7. Operator assumed to isolate PORV in 10 min.	Vol. 3, Pg. 2.2-59	Appears not significant.	
8. For non-LOOP transients and support state 7, DCP seal LOCA occurs.	Vol. 3, Pg. 2.2-60	Not significant.	
9. Accumulator failure causes core melt for large break LOCA.	Vol. 3, Pg. 2.2.7.1-5	Not significant - large LOCA accidents not significant to CMF.	Large LOCA does have a minor contribution to core melt (See Section 5.3).
10. If containment spray injection and quench spray fail, neither LPRS or CSRS can succeed.	Vol. 3, Pg. 2.2.7.1-6	Could be significant, but it does not appear this assumption was retained.	PSS Pg. 4.4-27 indicates recirculation spray is operable in the absence of previous containment spray injection.
11. Accumulator failure causes core melt for medium break LOCAs.	Vol. 3, Pg. 2.2.7.2-7	Not significant to public risk since medium LOCAs are not risk significant.	Medium LOCA with accumulator failure not a dominant sequence for core melt.

represent the various possible effects and conditions stemming from the dependence of front-line systems on support systems.

The above discussion points out problems with the support state method of analysis which would apply to any study which utilized it. As stated, it is not possible within the scope and time available to perform this review to determine if any of these problems are significant to the PSS. It is important to note, however, that other studies have demonstrated the potential for errors to be introduced in this way. Support system interfaces have been shown to be very important to risk and sometimes very subtle in nature. The support state method tends to treat these interfaces in a less rigorous manner than the use of fully integrated fault tree analysis. The use of the support state method may inject additional uncertainty into the PSS.

As far as the application of the support state method in the PSS is concerned, the potential loss of DC power was not treated in the support states utilized. Although electric power was selected as one of the support systems, the concentration was on the unavailability of the main AC engineered safety features busses. The effect of losing one DC power train can be more far-reaching than the loss of an AC train in that it causes more equipment failures. Additionally, the loss of some or all DC power following a loss of offsite power will have a significant effect on recovery of offsite power due to the unavailability of various control room indications and control circuits for breaker manipulations. It is generally assumed that in the total absence of DC power it is not possible to recover AC power in any reasonable amount of time. Although loss of DC power is treated as an initiating event, its lack of treatment in the support state analysis is a deficiency in the PSS. In examining the significance of this deficiency, it has been concluded that the omission is probably not significant if the turbine-driven auxiliary feedwater pump can successfully operate without DC power as maintained by the applicant during a meeting at NU headquarters in December 1983.

3.10.3 Common-Cause Failure Analysis

The MP 3 PSS employed the binominal failure rate model to assist in quantifying the contribution of common-cause failures to system failure rates. Common-cause failures have long been recognized to have a very important impact on nuclear power plant system failure rates. This occurs because many of these systems have redundant trains, each of which are generally of high reliability. Under these circumstances, common-cause failures are almost always dominant contributors to system failures. Since common-cause failures have been very rare at nuclear plants, there is generally insufficient data to permit a direct quantification of common-cause failure contributions. As a result, various mathematical models have been proposed, and quantification of common-cause failures in probabilistic risk assessments remains an uncertain and somewhat controversial area.

Of various models to quantify common-cause failures, two are generally preferred by the reactor risk assessment community (Ref. 3.10-3). These are the β-factor model and the binominal failure rate (BFR) model. These two models are similar, and for two redundant train systems they produce equivalent results. The BFR is somewhat more sophisticated and generally represents the state of the art in common-cause failure modeling. Much literature is available (Ref. 3.10-3, -4, -5) which describe models. Thus, a detailed description will not be provided here.

It is important to recognize that the BFR and β-factor models do not produce common-cause failure rates from strictly random failure rates. Instead, they require input from the analyst on the potential for common-cause failures. This is obtained usually by examination of data to determine which observed failure mechanisms contained the potential for common-cause failure, or by actual use of common-cause failure data if available. (For example, for a three-train system, common-cause failures of two trains can be input to the BFR model in order to compute the common-cause rate for three trains.) These data can be from identical systems or, if data are sparse, may be inferred from data on similar systems. In any case, considerable judgement is frequently required on the part of the analyst in inputting data (or assumptions related to data) to the BFR or in deriving a value for β for the β-factor model. As a result, significantly different results can be obtained by different analysts for the same system with the same model. Thus, while use of the BFR for common-cause failures in the MP 3 PSS represents a generally acceptable state-of-the-art model, its use does not necessarily assure that common-cause failures have been realistically estimated.

A general description of the MP 3 PSS common-cause failure assessment is discussed in PSS Appendix 2-C. This description appears adequate and includes a consideration of the important aspects of common-cause failures. The appendix includes a description of the BFR model and provides data used to quantify the common-cause contribution.

Two specific common-cause assessments are provided in the MP 3 PSS as indicated previously. These are common-cause service water strainer plugging (Appendix 2-5) and best estimate common-cause actuating logic unavailability. The SWS failure assessment and related implications are discussed in Section 3.6 of this report. Based on that discussion, it appears that SWS common-cause failure is not of concern for the MP 3 plant. The assessment of actuating system logic appears reasonable.

In summary, it is concluded that the MP 3 PSS common-cause failure models are reasonable and valid. The actual quantification of common-cause failures is discussed, as part of the overall assessment of system failures, in Sections 3.4 and 3.6 of this report.

3.10.4 References for Section 3.10

3.10-1 K. N. Fleming et al., "On the Analysis of Dependent Failures in Risk Assessment and Reliability Evaluation," Nuclear Safety (Vol. 24-5), September-October 1983, p. 637.

3.10-2 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.

3.10-3 U.S. Nuclear Regulatory Commission, "PRA Procedures Guide - A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants," USNRC Report NUREG/CR-2300, January 1983.

3.10-4 C. L. Atwood, EG&G Idaho, Inc., "Data Analysis Using the Binomial Failure Rate Common Cause Model," USNRC Report NUREG/CR-3437, September 1983.

3.10-5 C. L. Altwood, EG&G Idaho, Inc., "Estimators for the Binomial Failure Rate Common Cause Model," USNRC Report NUREG/CR-1401, April 1980.

3.11 Quantification

The purpose of this section is to review and summarize the approach used in the Millstone 3 PSS to quantify the frequency of the plant damage states using the results of the event tree, support state and fault tree models. The results of the quantification were assembled into the combined internal plant damage state matrix - referred to as the "M matrix." Each entry in the M matrix represents a conditional probability of a plant damage state given a particular initiator. The event tree for each initiating event was quantified eight times, once for each support state. Also considered is the propagation of uncertainty through the quantification process.

3.11.1 Development of Quantitative Results in the Millstone 3 PSS

Plant system event trees were quantified by combining results into an internal plant damage state matrix - the M matrix. Each sequence in an event tree was assigned a plant damage state. Often several sequences in an event tree can lead to the same plant damage state. For a particular initiating event and support state, the probabilities of event tree sequences having the same plant damage state were summed together. The sum is the conditional probability of a plant damage state given a particular initiator and support state. This sum was multiplied by its corresponding support state probability (or split fraction). The resulting products for each support state were added together for each event tree. The final values obtained in this process are the conditional probabilities of plant damage states for a given initiator. This process produces the entries in the M matrix. Each entry in the M matrix corresponds to a specific damage state and initiating event. The entries of the M matrix as calculated in the Millstone PSS are provided in Table 3.11.1.

3.11.2 Quantification of Uncertainties

Uncertainty analysis involves the estimation of uncertainties in the input of event and fault tree models used to describe plant behavior and the propagation of these uncertainties through the trees. The authors of the Millstone PSS states that the study "attempts to better account for overall uncertainties by formally recognizing and propagating uncertainties originating from ..." 1) initiator frequencies, 2) system unavailability, 3) core melt frequency, 4) frequency of containment failure, 5) uncertainties in fission product source terms and 6) uncertainties in public consequences. Our objectives in this review were limited us to consideration of uncertainties in the first four categories. In general, we found the propagation of uncertainties from variances in individual component failure rates to system failure more traceable then the propagation from fault trees to event trees and plant damage states.

The frequencies of initiating events at Millstone 3 were described by the mean and variance of an assumed lognormal distribution. The frequency of common

Table 3.11-1
Internal Plant Damage State Matrix (M)[a]
(Source: Millstone 3 PSS)

Plant Damage States

Initiators	AEC	AEC'	AE	ALC	ALC'	ALC"	AL	SEC	SEC'	SE	S'E
	SLC	SLC'	SLC"	SL	S'L	TEC	TEC'	TE	V2EC	V2EC'	
	V2E	V2LC	V2LC'	V2LC"	V2L	V	Success				
Large LOCA	1.92E-3	4.17E-6	2.68E-6	3.17E-3	4.85E-4	2.69E-6	2.29E-7	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	
	0	0	0	0	0	0	9.94E-1				
Medium LOCA	1.93E-3	4.18E-6	2.69E-6	6.55E-3	4.91E-4	3.89E-6	2.42E-7	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	
	0	0	0	0	0	0	9.91E-1				
Small LOCA	0	0	0	0	0	0	0	9.75E-6	2.52E-8	1.99E-6	0
	1.57E-4	5.15E-6	7.30E-8	2.71E-9	0	0	0	0	0	0	
	0	0	0	0	0	0	1.0				
Steam generator	0	0	0	0	0	0	0	6.53E-6	1.41E-8	1.50E-6	0
tube rupture	1.29E-5	6.97E-7	8.27E-8	3.93-E9	0	1.68E-5	2.05E-7	2.01E-7	2.83E-6	2.63E-8	
	3.29E-7	7.04E-8	3.80E-9	4.50E-10	2.14E-11	0	1.0				
Steamline break	0	0	0	0	0	0	0	2.94E-10	7.60E-13	5.80E-11	0
inside	1.82E-5	1.09E-6	8.61E-8	4.14E-9	0	4.78E-5	2.91E-7	1.80E-6	0	0	
containment	0	0	0	0	0	0	1.0				
Steamline break	0	0	0	0	0	0	0	2.94E-10	7.60E-13	5.80E-11	0
outside	2.26E-5	1.42E-6	8.86E-8	4.30E-9	0	6.66E-5	3.31E-7	1.80E-6	0	0	
containment	0	0	0	0	0	0	1.0				
Loss of reactor	0	0	0	0	0	0	0	6.56E-8	1.41E-10	8.10E-11	0
coolant system	5.68E-7	3.90E-8	1.27E-9	6.37E-11	0	2.18E-6	7.19E-9	2.28E-7	0	0	
flow	0	0	0	0	0	0	1.0				
Loss of main	0	0	0	0	0	0	0	6.56E-8	1.41E-10	8.10E-11	0
feedwater	5.68-7	3.90E-8	1.27E-9	6.37E-11	0	2.18E-6	7.19E-9	2.28E-7	0	0	
	0	0	0	0	0	0	1.0				
Primary to	0	0	0	0	0	0	0	6.56E-8	1.41E-10	8.10E-11	0
secondary power	5.68E-7	3.90E-8	1.27E-9	6.37E-11	0	2.18E-6	7.19E-9	2.28E-7	0	0	
mismatch	0	0	0	0	0	0	1.0				
Turbine trip	0	0	0	0	0	0	0	6.56E-8	1.41E-10	8.10E-11	0
	5.68E-7	3.90E-8	1.27E-9	6.37E-11	0	2.18E-6	7.19E-9	2.28E-7	0	0	
	0	0	0	0	0	0	1.0				
Reactor trip	0	0	0	0	0	0	0	6.56E-8	1.41E-10	8.10E-11	0
	5.68E-7	3.90E-8	1.27E-9	6.37E-11	0	2.18E-6	7.19E-9	2.28E-7	0	0	
	0	0	0	0	0	0	1.0				
Core power	0	0	0	0	0	0	0	6.56E-8	1.41E-10	8.10E-11	0
excursion	5.68E-7	3.90E-8	1.27E-9	6.37E-11	0	2.18E-6	7.19E-9	2.28E-7	0	0	
	0	0	0	0	0	0	1.0				

Table 3.11-1 (Continued)

Initiators	AEC	AEC'	AE	ALC	ALC'	ALC"	AL	SEC	SEC'	SE	S'E
	SLC	SLC'	SLC"	SL	S'L	TEC	TEC'	TE	V2EC	V2EC'	
	V2E	V2LC	V2LC'	V2LC"	V2L	V	Success				
Spurious Safety	0	0	0	0	0	0	0	6.56E.8	1.41E-10	8.10E-11	0
Injection	5.68E-7	3.90E-8	1.27E-9	6.37E-11	0	2.18E-6	7.19E-9	2.28E-7	0	0	
	0	0	0	0	0	0	1.0				
Loss of Offsite	0	0	0	0	0	0	0	1.93E-7	4.29E-10	3.47E-7	0
Power	6.83E-7	5.16E-8	2.21E-10	1.66E-11	0	7.98E-5	1.01E-6	1.59E-5	0	0	
	0	0	0	0	0	0	1.0				
Incore Instrument	0	0	0	0	0	0	0	9.75E-6	2.52E-8	0	1.99E-6
Tube Rupture	1.57E-4	5.15E-6	6.57E-8	0	3.64E-7	0	0	0	0	0	
	0	0	0	0	0	0	1.0				
Inferfacing	0	0	0	0	0	0	0	0	0	0	0
Systems LOCA	0	0	0	0	0	0	0	0	0	0	
V-Sequence	0	0	0	0	0	1.0	0				

[a] These are conditional core melt probabilities and <u>must</u> be multiplied by the initial event frequency to calculate core melt frequency.

transients was obtained using classical estimation methods. In these cases, the initiating event frequency was treated as a random variable, the distribution of which reflects inherent plant-to-plant variability. The distribution parameters for these events were obtained by matching the moments of the population data to the moments of a lognormal distribution. For those events which have not occurred, a Baysian approach was used. A distribution is established which represents the prior state of knowledge about the frequency of a particular event. This distribution is then revised, via Bayes´ theorem, to reflect observed operating experience. The resulting distributions are fit to a lognormal distribution in order to obtain uncertainty parameters.

System unavailability (failure/demand) was calculated from the system fault trees using the WAMCUT computer code. The WAMCUT code uses the method of moments to propagate variance of individual components to an overall variance in system unavailability. The method of moments uses the moments of component distributions to determine the moments of this system distribution. Random component failures and the variance in these failures were obtained primarily from the proprietary Westinghouse Data Base.

Discrete probability distribution (DPD) arithmetic was used to determine the variance in the plant damage states. Uncertainty in the frequency of core melt was obtained by propagating the variance in top events through event trees using DPD arithmetic. The uncertainty in the frequency of containment failure was treated using DPD arithmetic with input variances propagated from the fault and event tree models combined with best estimate uncertainties derived from engineering judgement. According to the PSS, a discussion of the overall uncertainty analysis is provided in Appendix L. However, all that was provided regarding the use of DPD arithmetic was a tutorial on DPD arithmetic. No description was provided for how DPD arithmetic was used for Millstone 3. We were, thus, unable to review the specific procedures used to propagate uncertainties using DPD arithmetic for the PSS.

3.12 Requantification Summary for the Internal Event Accident Sequences

A simplified requantification of the internal event accident sequences contained in the new/revised event trees presented in Section 3.2 was performed as a part of this review.

This section provides a summary of the input data used in the requantification, tables of definitions and descriptions applicable to the event trees, and an annotated set of the event trees from Section 3.2 which show the values used for specific events in all sequences whose frequency of occurrence was evaluated as greater than or equal to 1E-7 per year.

The results presented here are necessarily based on many assumptions and subject to many qualifications. The reader is referred to Section 3.2 for a detailed discussion of the event trees, and to other sections of this report for additional information on initiating events, data, etc. That information is not repeated here.

The reader is cautioned to keep in mind that the support state methodology used in the MP 3 PSS requires an evaluation of each event tree for each applicable support state. In most cases here, one or two support states (typically the support states numbered 1 and 2 in the PSS) are so dominant that it is unnecessary to evaluate the others. In the event trees presented in this section, we have adopted a convention to simplify the presentation of results: unless otherwise noted, numbers shown above an event line are for support state 1 and numbers below the line are for support state 2. Where an ambiguity might occur, the support state is identified.

The eight tables and 11 annotated event trees which are shown on the following pages are listed below for the convenience of the reader.

Table	Content
3.12-1	Initiating event frequencies
3.12-2	Support state probabilities
3.12-3	System failure and human error event probabilities
3.12-4	Offsite power recovery factors
3.12-5	System failure and human error event probabilities for the ATWS event tree
3.12-6	Event tree top event definitions
3.12-7	Support state definitions
3.12-8	Plant damage state descriptions

Figure	Event Tree
3.12-1	Large LOCA
3.12-2	Medium LOCA
3.12-3	Small LOCA
3.12-4	Incore instrument tube rupture
3.12-5	Steam generator tube rupture
3.12-6	Steamline break inside (& outside) containment
3.12-7	Power conversion system available
3.12-8a	Loss of power conversion system (support states 1,2)
3.12-8b	Loss of power conversion system (support states 5,6)
3.12-8c	Loss of a single DC bus
3.12-8d	Loss of vital AC bus 1 or 2
3.12-8e	Loss of vital AC bus 3 or 4
3.12-8f	Loss of a single service water train
3.12-9	Loss of offsite power (support state 7)
3.12-10	Spurious safety injection
3.12-11	Anticipated transients without scram

Table 3.12-1. Initiating event frequencies
(Source: Table 3.1-3, fifth column)

Event class	Event name	Point estimate frequency (per year)
1	Large LOCA	1E-4
2	Medium LOCA	3E-4
3	Small LOCA	1E-3(see note 1)
4	Steam generator tube rupture	2E-2
5	Steamline break inside containment	4E-2
6	Steamline break outside containment	1E-4
7	PCS available	7.24
8	Loss of PCS	2.32
13	Spurious safety injection	6E-2
14	Loss of offsite power	1E-1
15	Incore instrument tube rupture	4E-4
16a	Interfacing systems LOCA	8E-7
17	Loss of a single service water train	2E-2
18	Loss of a single vital DC bus	4E-2
19	Total loss of vital DC power	ε (see note 2)
20	Loss of vital AC bus 120-VAC-1 or -2	7E-2
21	Loss of vital AC bus 120-VAC-3 or -4	7E-2

Notes:
1. Support state 1 only, 2E-2 for all other states.
2. ε < 1E-7 per year.

Table 3.12-2 Support state probabilities
(Source: Millstone Unit 3 PSS Tables 2.2.6.1-1 through 2.2.6.1-7 except as noted)

	Support State Probability							
Initiator type	1	2	3	4	5	6	7	8
Non-support system related	0.996	0.004	2.6E-7	1.6E-7	3E-4	4.9E-6	6.5E-8	9.6E-11
Loss of offsite power	N/A	N/A	N/A	N/A	0.958[a]	0.04[a]	.002[a]	3.6E-7
Loss of single service water train	N/A	0.999	4.5E-5	1.6E-7	N/A	3.1E-4	1.6E-6	9.6E-11
Loss of single vital DC bus	N/A	0.999	1.6E-5	1.2E-5	N/A	3.1E-4	1.6E-6	7E-9
Loss of single vital AC bus (120 VAC-1 or -2)	N/A	0.999	1.6E-5	1.2E-5	N/A	3.1E-4	1.6E-6	7E-9
Loss of single vital AC bus (120 VAC-3 or -4)	N/A	0.999	2.7E-5	1.6E-7	N/A	3.1E-4	1.6E-6	9.6E-11

[a] Revised - see Section 3.6

Table 3.12-3 System failure and human error event probabilities
(Source: Millstone Unit 3 PSS Tables 2.2.3.2-1 through 2.2.3.5-1 except as noted).

	Support state							
System/event	1	2	3	4	5	6	7	8
OA-1	0.02	0.02	1.0	1.0	0.02	0.026	1.0	1.0
OA-1'	0.1	0.1	1.0	1.0	0.1	0.1	1.0	1.0
OA-2	0.01	0.01	1.0	1.0	0.01	0.01	1.0	1.0
OA-2-E[a]	0.001	0.001	0.0	0.0	0.001	0.001	0.0	0.0
OA-3	0.03	0.03	1.0	1.0	0.03	1.0	1.0	1.0
OA-4	0.02	0.02	1.0	1.0	0.02	0.02	1.0	1.0
OA-5	0.5	0.5	1.0	1.0	0.5	1.0	1.0	1.0
OA-6	0.01	0.001	1.0	1.0	0.01	.001	1.0	1.0
OA-6'	0.1	0.01	1.0	1.0	0.1	0.01	1.0	1.0
OA-6-E[a]	1E-4	1E-4	0.0	0.0	1E-4	1E-4	0.0	0.0
OA-7	0.03	0.03[b]	1.0	1.0	0.3	1.0	1.0	1.0
OA-7'	N/A	N/A	N/A	N/A	N/A	N/A	0.01	N/A
OA-8[a]	0.001	0.001	1.0	1.0	0.001	.001	1.0	1.0
OA-9[a]	0.5	0.5	0.0	0.0	0.5	0.5	0.0	0.0
OA-10[a]	1E-4	1E-4	0.0	0.0	1E-4	1E-4	1E-4	0.0
ACC	2E-3	2E-3	2E-3	2E-3	2E-3	2E-3	2E-3	2E-3
LP	2E-4	5E-3	1.0	1.0	2E-4	5E-3	1.0	1.0
HP-1	1E-4	5E-2	1.0	1.0	1E-4	5E-2	1.0	1.0

Table 3.12-3 (Continued).

	Support state							
System/event	1	2	3	4	5	6	7	8
HP-2	6E-5	7E-4	1.0	1.0	6E-5	7E-4	1.0	1.0
AF-1	7E-5	6E-4	6E-4	1.0	7E-5	6E-4	5E-2	1.0
AF-2	5E-4	5E-2	5E-2	1.0	5E-4	5E-2	5E-2	1.0
AF-3	N/A	N/A	N/A	N/A	N/A	N/A	3E-4	N/A
QS	3E-4	8E-3	1.0	1.0	3E-4	8E-3	1.0	1.0
QS|HP-2	7E-4	8E-3	1.0	1.0	7E-4	8E-3	1.0	1.0
R1	4E-3	5E-2	1.0	1.0	4E-3	5E-2	1.0	1.0
R2	7E-3	6E-2	1.0	1.0	7E-3	6E-2	1.0	1.0
R-2|OA-2	2E-2	7E-2	1.0	1.0	2E-2	7E-2	1.0	1.0
R-3	2E-3	4E-2	1.0	1.0	2E-3	4E-2	1.0	1.0
R-3|R-1	1E-1	5E-2	1.0	1.0	1E-1	5E-2	1.0	1.0
R-3|R-2	7E-2	5E-2	1.0	1.0	7E-2	5E-2	1.0	1.0
R-3|R-2 + OA-2	3E-2	4E-2	1.0	1.0	3E-2	4E-2	1.0	1.0
RT-1, RT-2	3E-5	3E-5	3E-5	3E-5	3E-5	3E-5	3E-5	3E-5
RT-3	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01
SA	2E-6	2E-6	2E-6	2E-6	2E-6	2E-6	2E-6	2E-6
TK	2E-8	2E-8	2E-8	2E-8	2E-8	2E-8	2E-8	2E-8

Table 3.12-3 (Continued).

	Support state							
System/event	1	2	3	4	5	6	7	8
SL	5E-3	5E-3	5E-3	5E-3	5E-3	5E-3	5E-3	5E-3
SL|(AF-2 + OA-3)	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1
S2	3E-5	3E-5	3E-5	3E-5	3E-5	3E-5	1.0[c]	1.0
SBO	5E-4	5E-4	5E-4	5E-4	0.0	0.0	0.0	0.0
SBI	2.2E-4	2.2E-4	2.2E-4	2.2E-4	0.024	0.024	0.024	0.024

(a) From Table 3.5.1
(b) 1.0 for loss of a single vital DC bus initiator (from PSS)
(c) 0.4 if offsite power restored within one hour (Section 3.2.3.1)

Table 3.12-4 Offsite power recovery factors
(Source: Millstone Unit 3 PSS, Section 2.2.6.1.1).

Recovery Time	Failure to Recover Probability
0 - 1/2 hour	0.33
1/2 - 1 hour	0.65
1 - 2 hour	0.59
2 - 8 hour	0.23

Table 3.12-5 System failure and human error probabilities for the ATWS event tree

Event	Probability	Source
RPS (Mechanical)	1E-5	ATWS Rule*
RPS(Electrical)	2E-5	ATWS Rule
RT3	0.01	Table 3.5-1
TT	0.1	PSS Table 2.2.3.4-1
PL**	0.01	ATWS Rule
PL|TT*	0.1	ATWS Rule
AF1	7E-5	PSS Table 2.2.3.3-1
PR	0.3	PSS Table 2.2.3.4-1
OA8***	0.001	Table 3.5.1
OA8R***	0.1	Table 3.5.1
QS	3E-4	PSS Table 2.2.3.3-1
R2	7E-3	PSS Table 2.2.3.3-2
R3	2E-3	PSS Table 2.2.3.3-2
R3|R2	7E-2	PSS Table 2.2.3.3-2

*10CFR50.62

**Defined as moderator temperature coefficient-overpressure by the ATWS Rule.

***Defined as high pressure injection by the AWTS Rule.

Table 3.12-6 Event tree top event definitions.

Symbol	Definition
ACC	Failure of accumulators
AF1	Failure of auxiliary feedwater
AF2	Failure of auxiliary feedwater (SGTR and streamline breaks)
AF3	Failure to recover auxiliary feedwater motor pumps (LOSP)
E60	Failure to restore offsite power in 1 hour
E120	Failure to restore offsite power in 1-2 hours
HP2	Failure of high pressure injection
LP	Failure of low pressure injection
OA1	Operator fails to blow down SGs and initiate LPI
OA2	Operator fails to conserve RWST inventory (control flow)
OA2E	Operator overthrottles HPI resulting in inadequate flow
OA3	Operator fails to establish primary bleed
OA4	Operator fails to blow down SGs during SGTR
OA5	Operator fails to establish primary bleed during SGTR
OA6	Operator fails to prevent pressurizer overfill (control HPI)
OA6E	Operator erroneously terminates high pressure injection
OA7	Operator fails to establish primary bleed and feed
OA8	Operator fails to establish emergency boration during ATWS
OA8R	Operator fails to establish HPI during ATWS consequential LOCA
OA9	Operator fails to delay recirculation when sump empty
OA10	Operator fails to control HPI during SGTR
PCS	Failure of power conversion system
PL	ATWS pressure spike exceeds service level C (unfavorable MTC)
PR	Consequential LOCA due to moderate ATWS pressure spike
QS	Failure of quench spray
QS'	Failure to recover quench spray (i.e., restore OSP in 2-8 hours)
RPS(E)	Failure to scram - electrical failure of RPS
RPS(M)	Failure to scram - mechanical failure of RPS
RT1	Failure of automatic reactor scram
RT3	Operator fails to manually scram reactor
RT4	Failure of both automatic and operator manual reactor scram
R1	Failure of low pressure recirculation
R2	Failure of high pressure recirculation
R3	Failure of containment spray recirculation
SA	Failure of safety injection actuation
SBI	Consequential steamline break inside containment
SBO	Consequential steamline Brbak outside containment
S2	Consequential small LOCA
SL	Consequential steamline leak during SGTR
TK	Failure of RWST
TT	ATWS turbine trip fails

Note: Tree top events which are "primed" (e.g., OA7') and not listed individually on this table have the same definition as the "unprimed" version, but are quantified differently to account for differences in the particular scenarios in which they appear.

Table 3.12-7 Support state definitions.

Symbol	Definition
(1)	All support systems available
(2)	One support train unavailable
(3)	Both support trains unavailable
(4)	All ESF signals unavailable
(5)	LOSP, all support systems available
(6)	LOSP, one support train unavailable
(7)	LOSP, both support trains unavailable
(8)	LOSP, all ESF signals unavailable

Table 3.12-8 Plant damage state descriptions.

Symbol	Definition
AEC	Large LOCA, early melt
AEC	Large LOCA, early melt, failure of recirculation spray
AEC"	Large LOCA, early melt, failure of quench spray
AE	Large LOCA, early melt, no containment cooling
ALC	Large LOCA, late melt
ALC'	Large LOCA, late melt, failure of recirculation spray
ALC"	Large LOCA, late melt, failure of quench spray
AL	Large LOCA, late melt, no containment cooling
SEC	Small LOCA, early melt
SEC'	Small LOCA, early melt, failure of recirculation spray
SEC"	Small LOCA, early melt, failures of quench spray
SE	Small LOCA, early melt, no containment cooling
SLC	Small LOCA, late melt
SLC'	Small LOCA, late melt, failure of recirculation spray
SLC"	Small LOCA, late melt, failure of quench spray
SL	Small LOCA, late melt, no containment cooling
TEC	Transient, early melt
TEC'	Transient, early melt, failure of recirculation spray
TEC"	Transient, early melt, failure of quench spray
TE	Transient, early melt, no containment cooling
TLC	Transient, late melt
TLC'	Transient, late melt, failure of recirculation spray
TL	Transient, late melt, no containment cooling
S'EC	Incore instrument tube LOCA, early melt
S'E	Incore instrument tube LOCA, early melt, no containment cooling
S'L	Incore instrument tube LOCA, late melt, no containment cooling
V2EC	Steam generator tube rupture, steam leak, early melt
V2EC'	SGTR, steam leak, early melt, failure of recirculation spray
V2EC"	SGTR, steam leak, early melt, failure of quench spray
V2E	SGTR, steam leak, early melt, no containment cooling
V2LC	SGTR, steam leak, late melt
V2LC'	SGTR, steam leak, late melt, failure of recirculation spray
V2LC"	SGTR, steam leak, late melt, failure of quench spray
V2L	SGTR, steam leak, late melt, no containment cooling
V	Interfacing systems LOCA

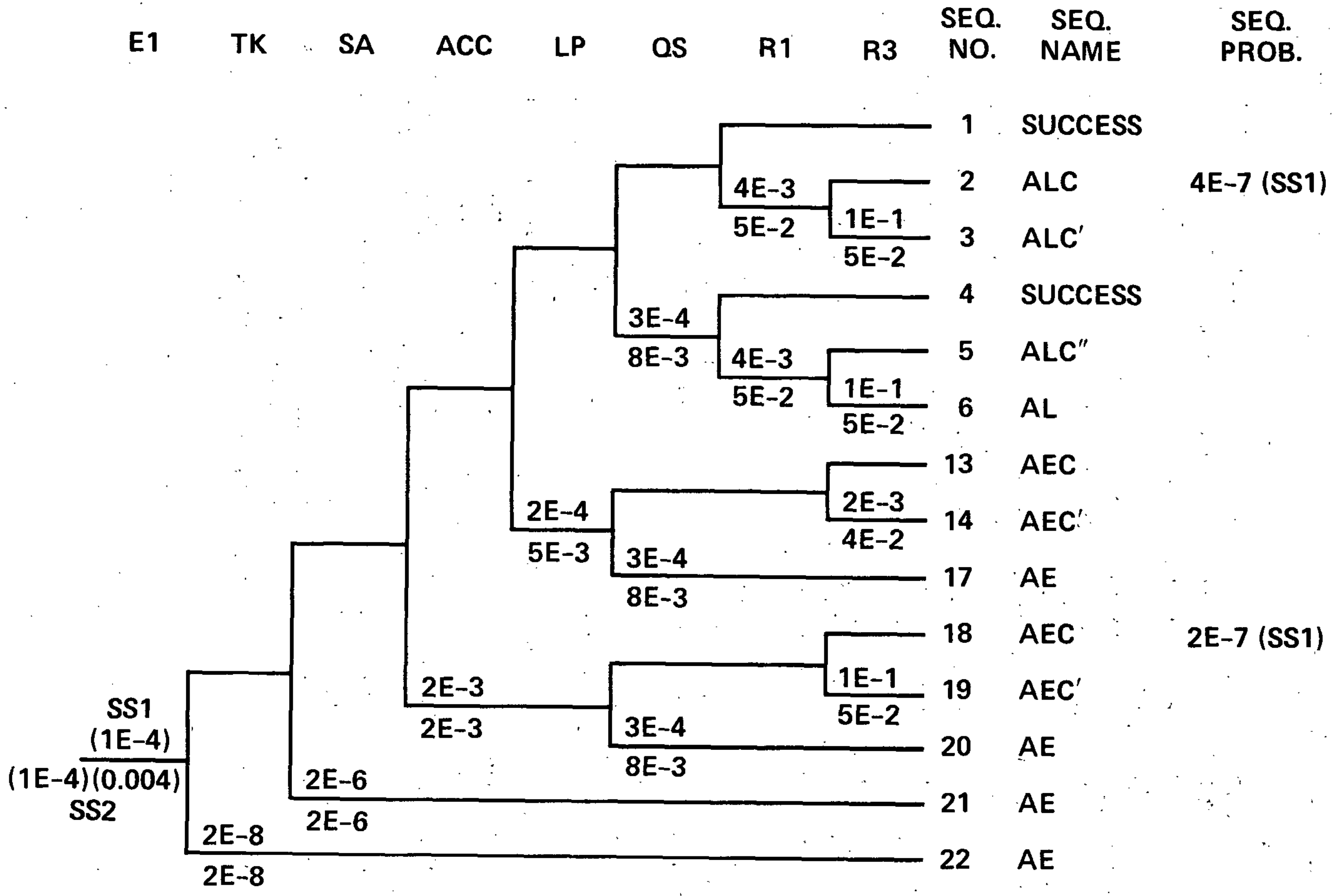


Fig. 3.12-1 Large LOCA event tree

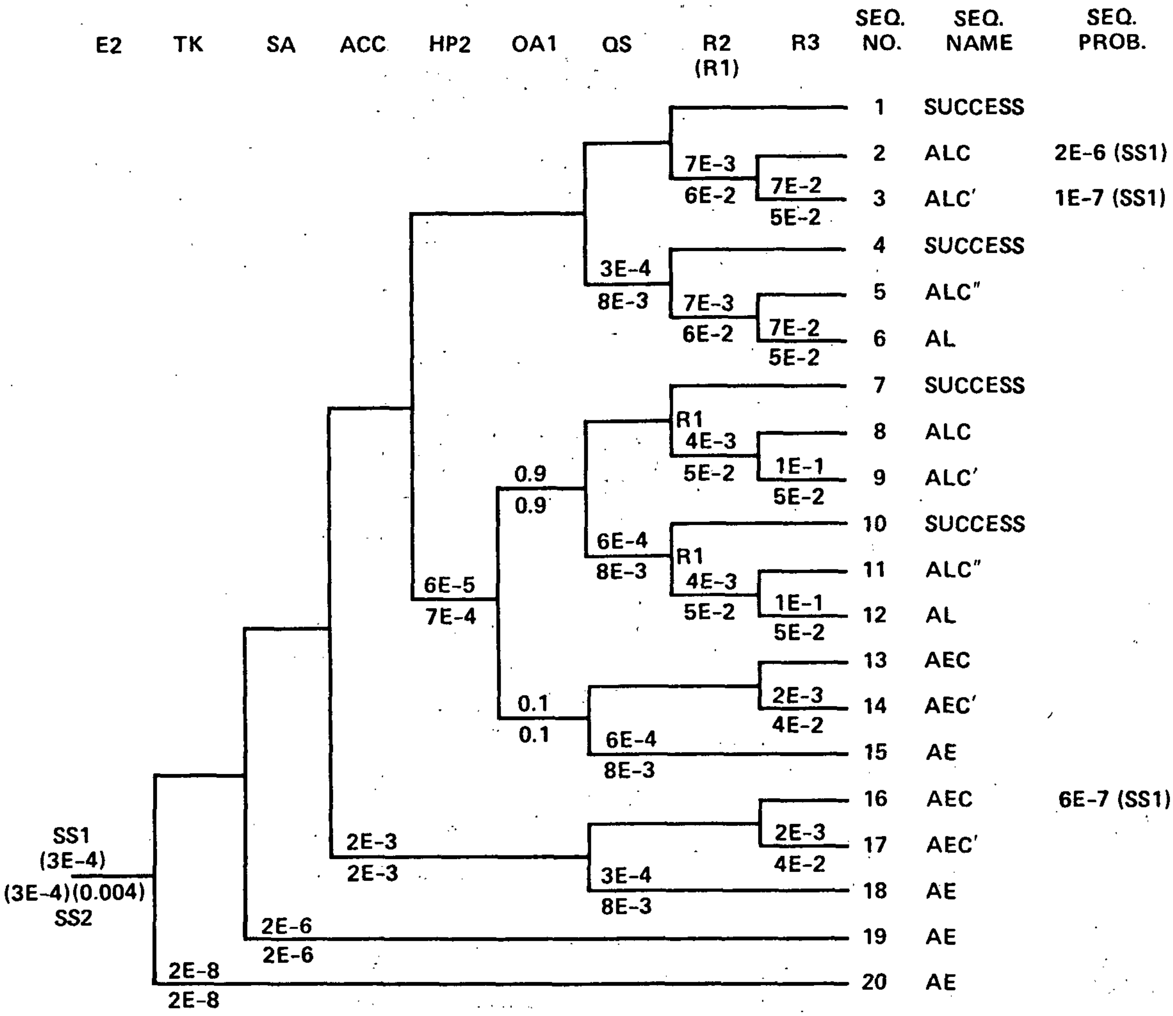
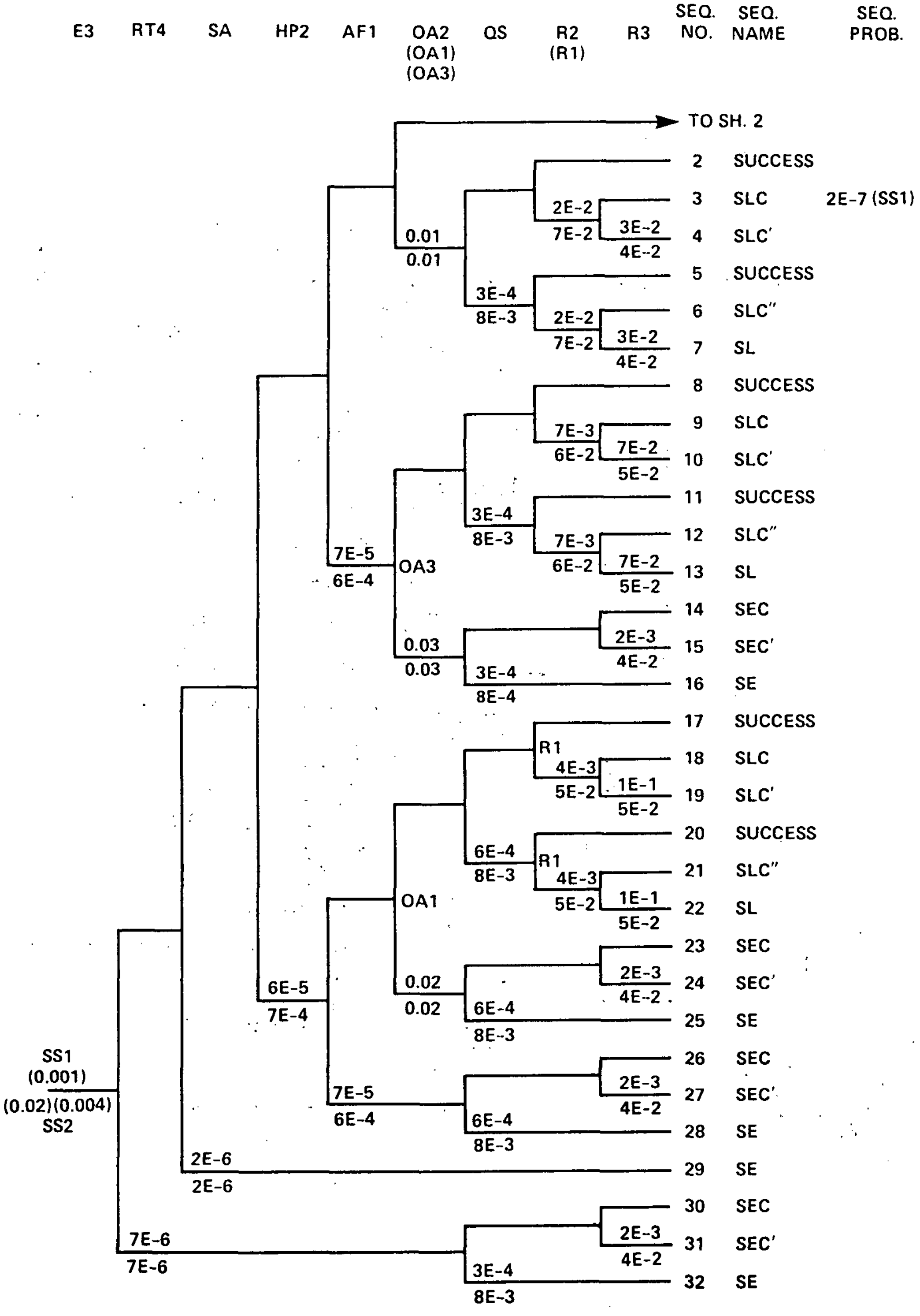


Fig. 3.12-2 Medium LOCA event tree



SS3 → (0.02)(2.5E-7) = 5E-9
SS4 → (0.02)(1.6E-7) = 3E-9

Fig. 3.12-3 Small LOCA event tree (sheet 1 of 2).

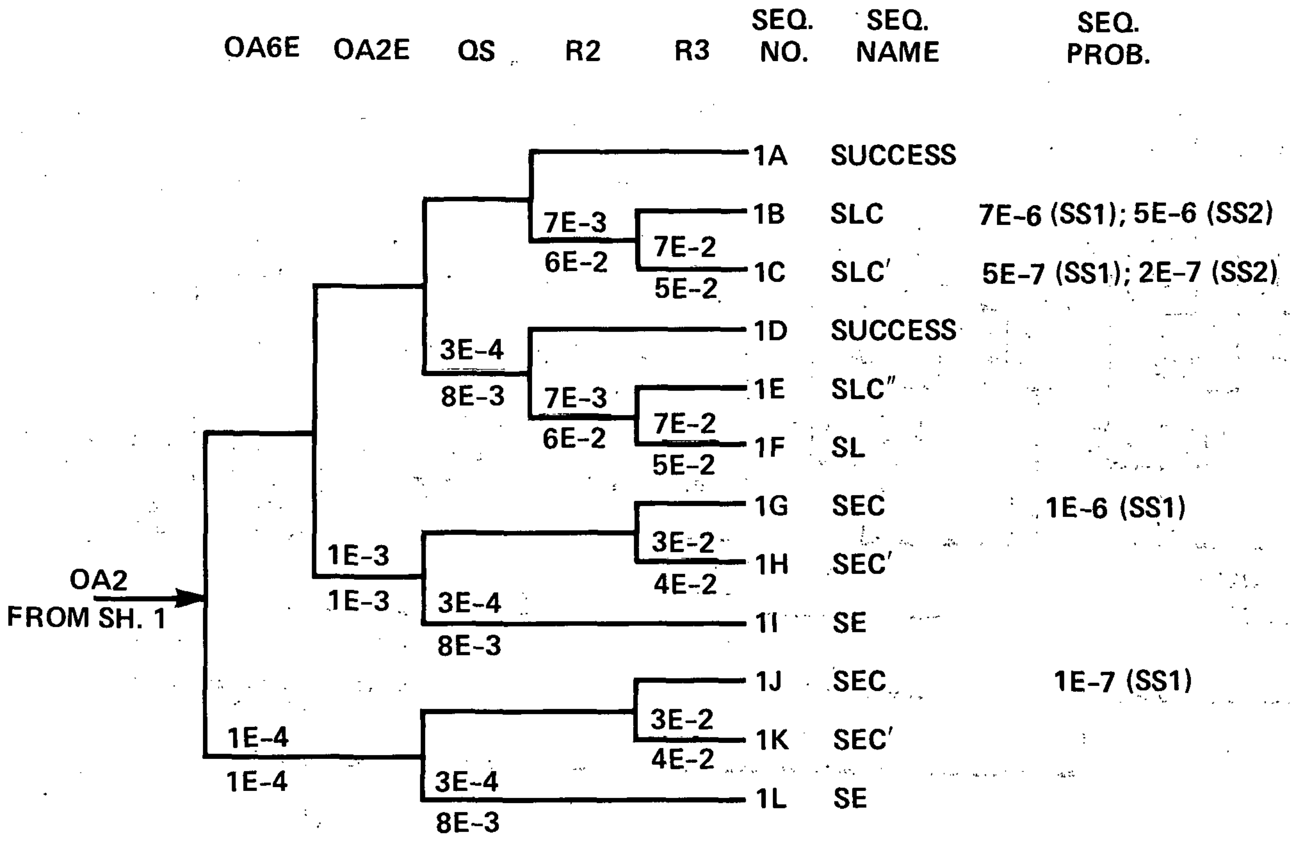


Fig. 3.12-3a Small Loca event tree (sheet 2 of 2).

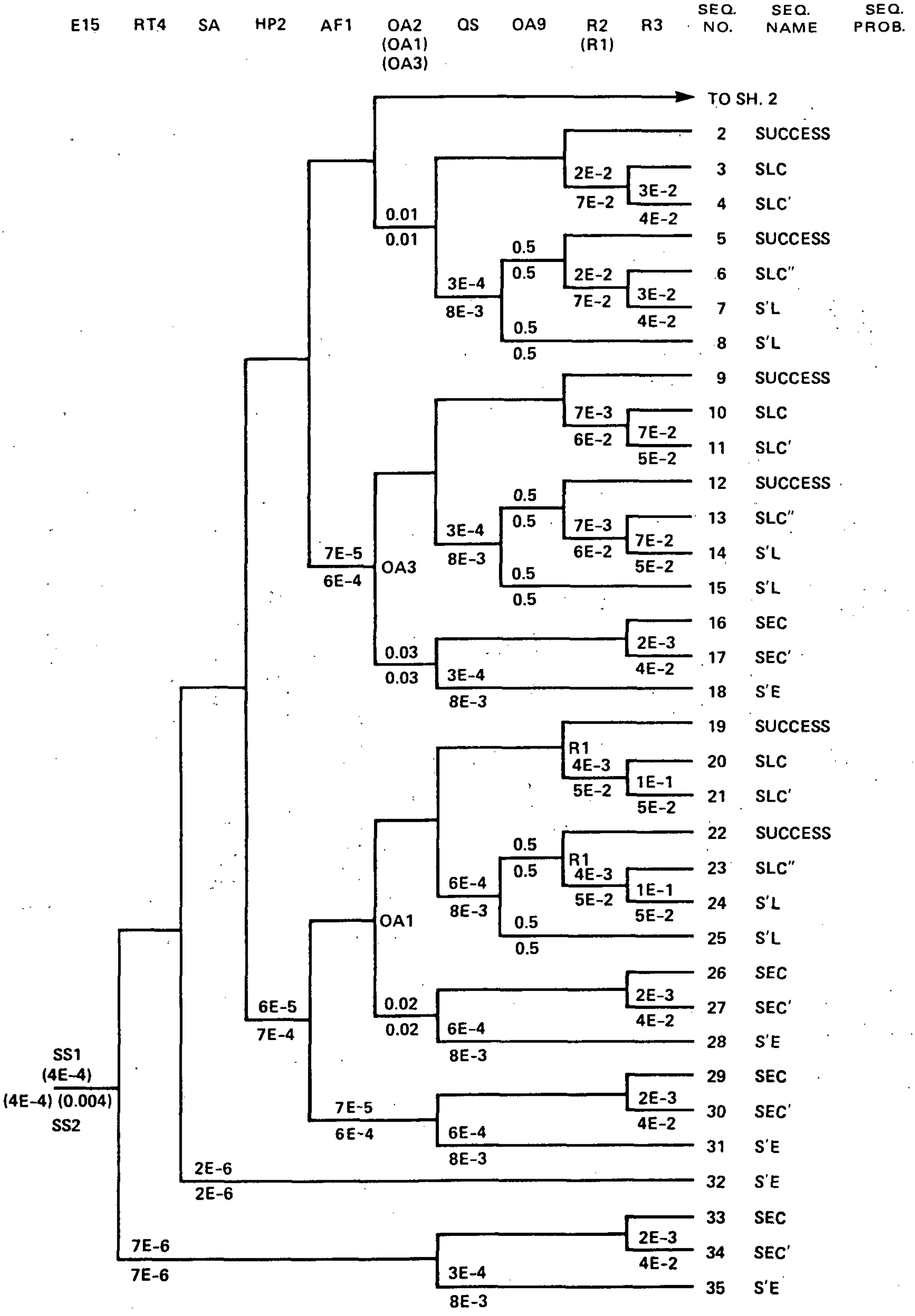


Fig. 3.12-4 Incore instrument tube rupture event tree (sheet 1 of 2).

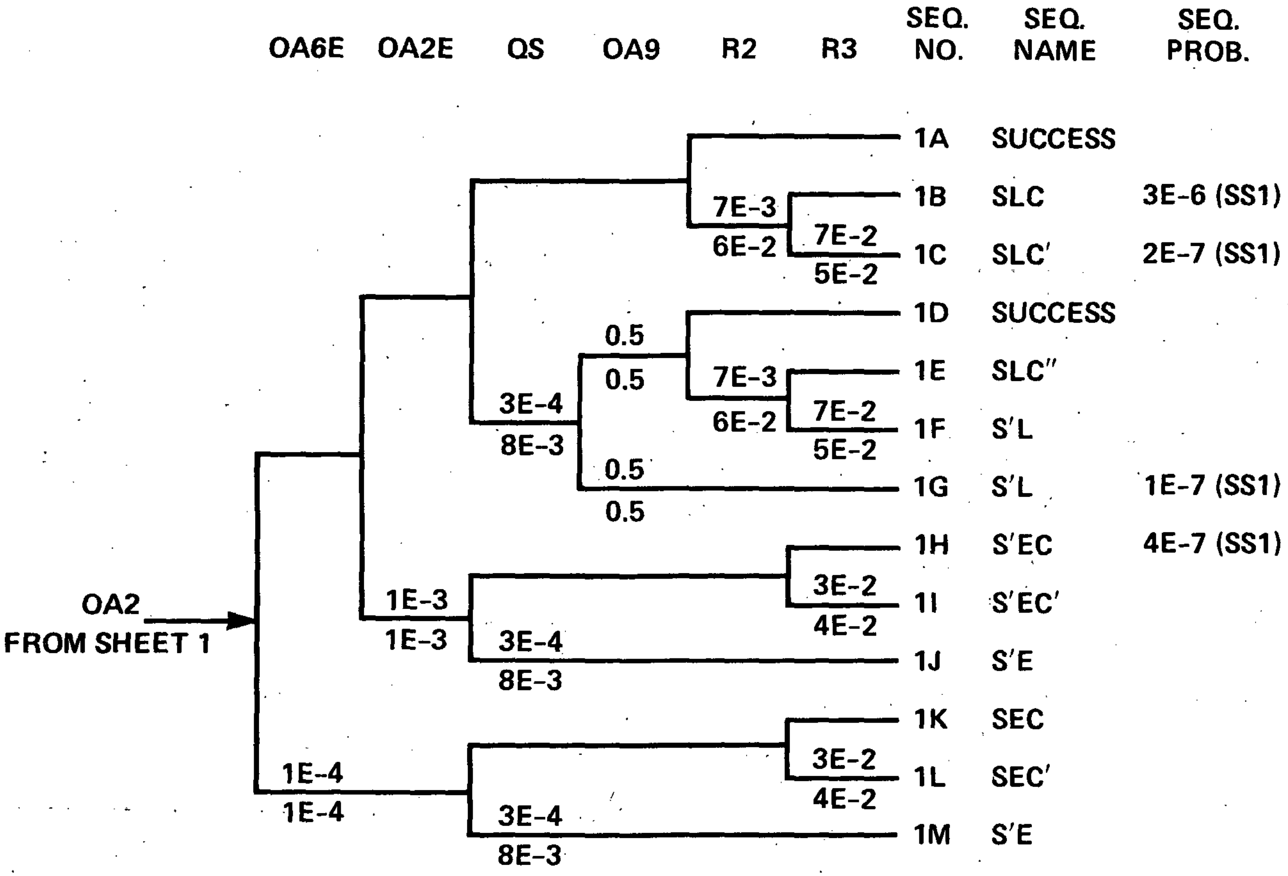


Fig. 3.12-4a Incore instrument tube rupture event tree (sheet 2 of 2)

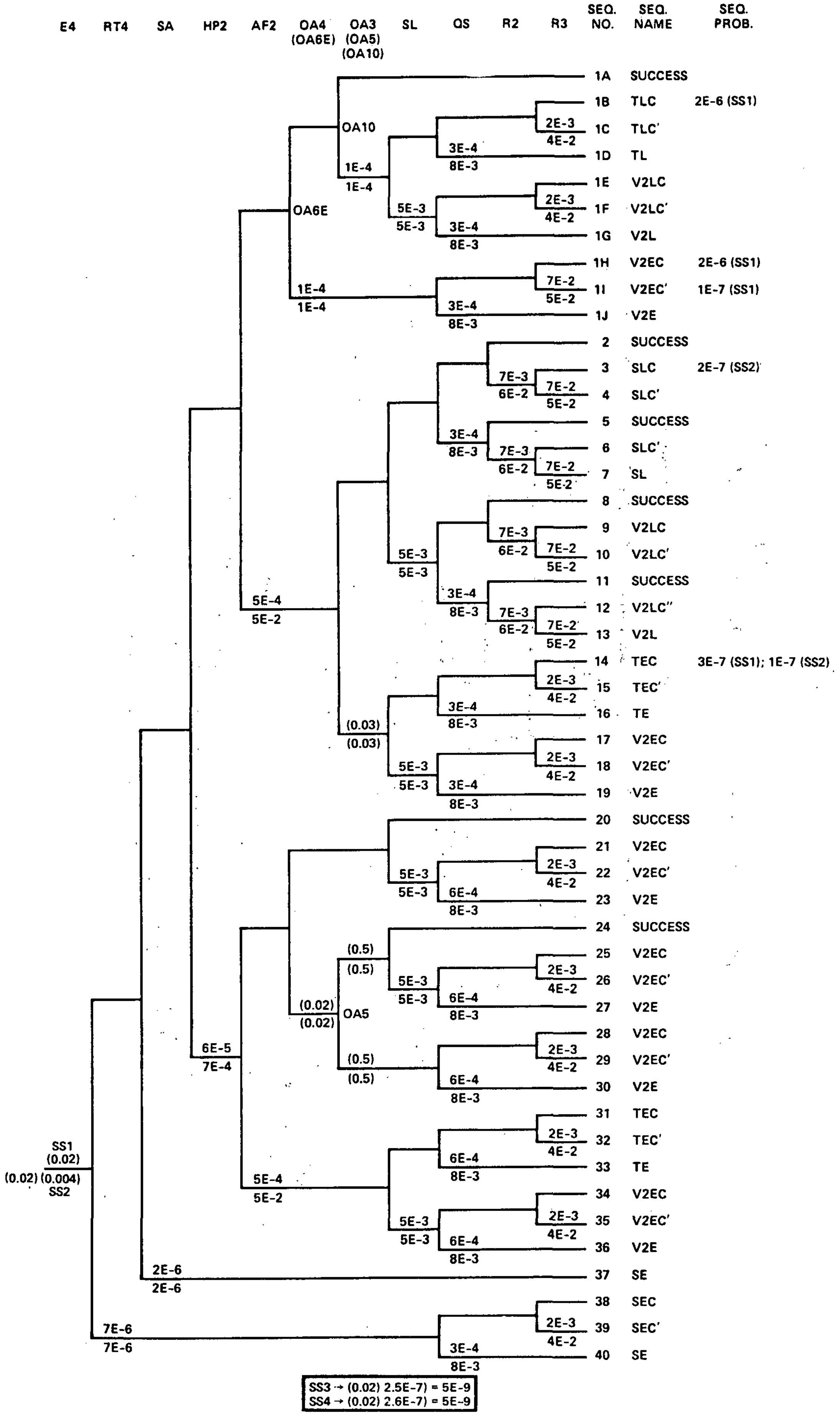


Fig. 3.12-5 Steam generator tube rupture event tree.

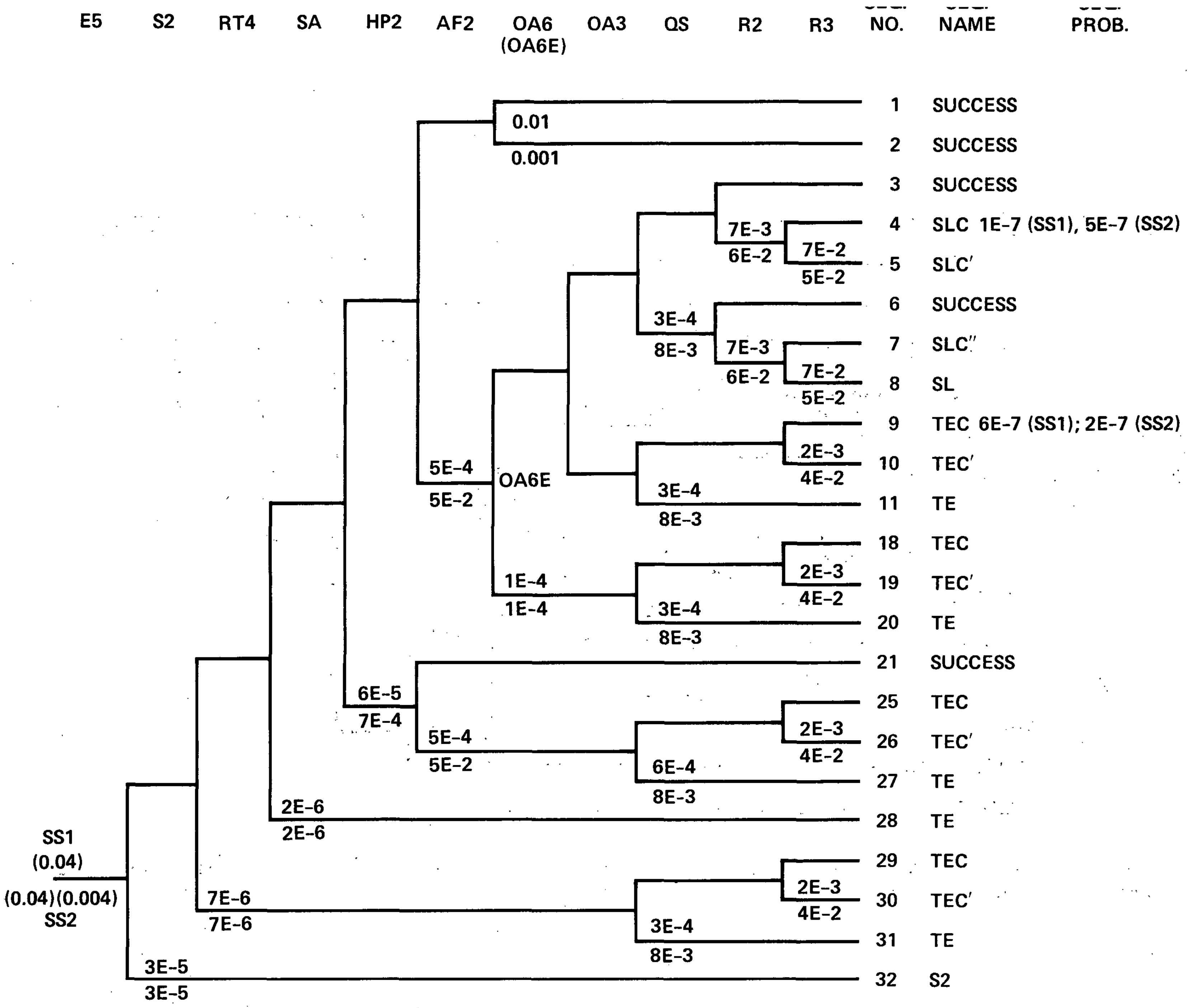


Fig. 3.12-6 Steamline break inside (and outside) containment event tree.

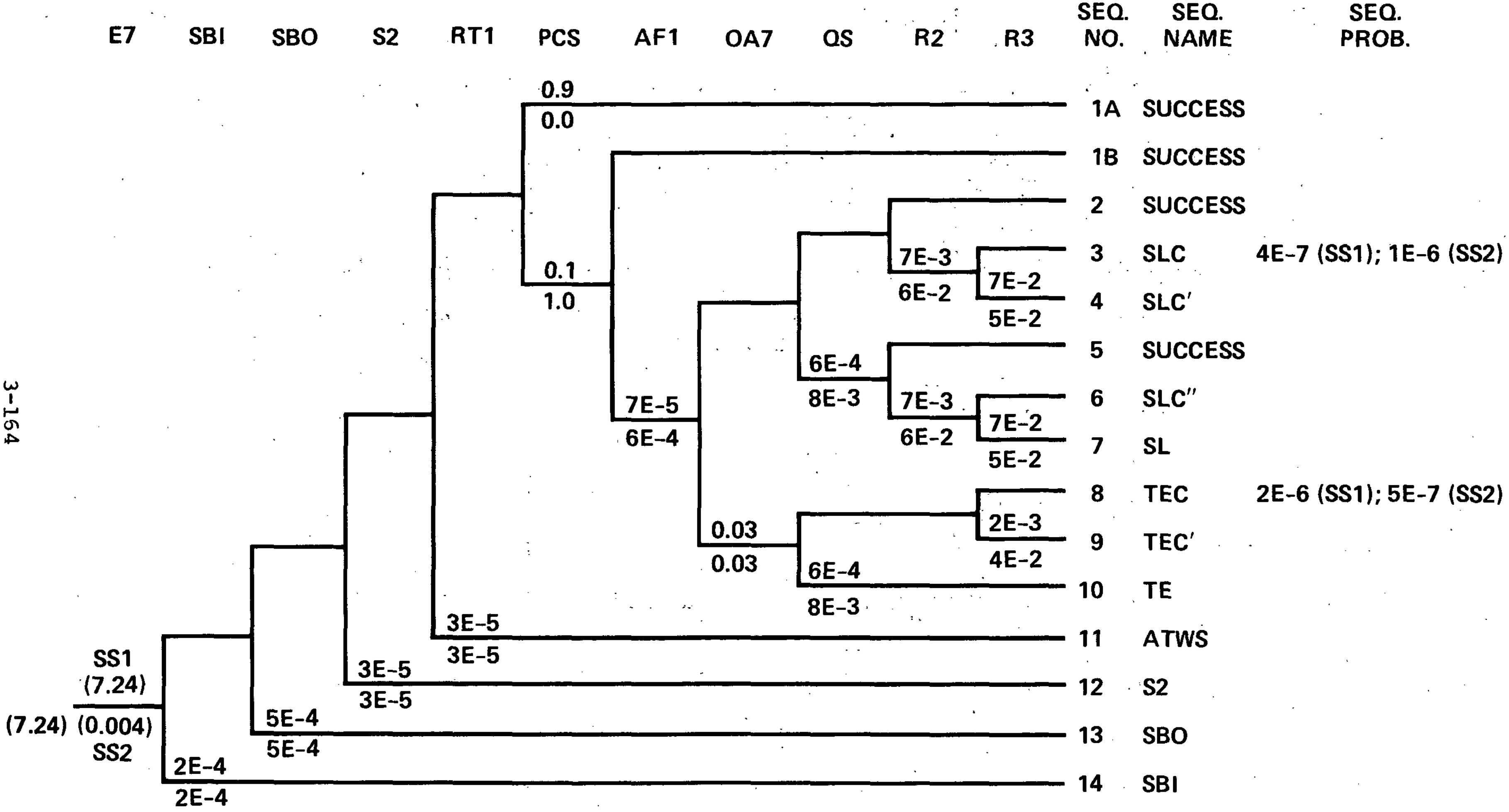


Fig. 3.12-7 Power conversion system available event tree.

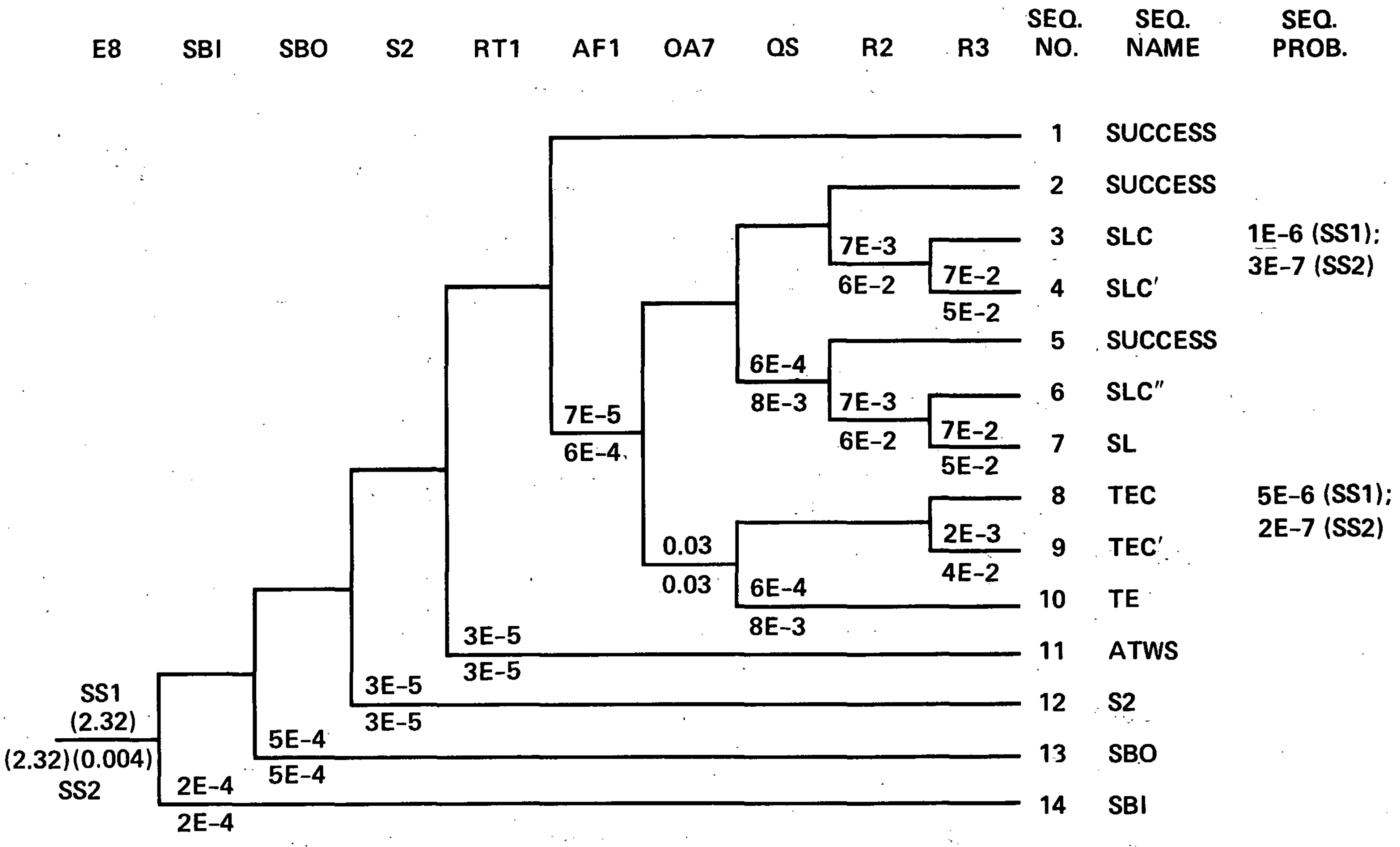


Fig. 3.12-8a Loss of power conversion system (support states 1, 2) event tree.

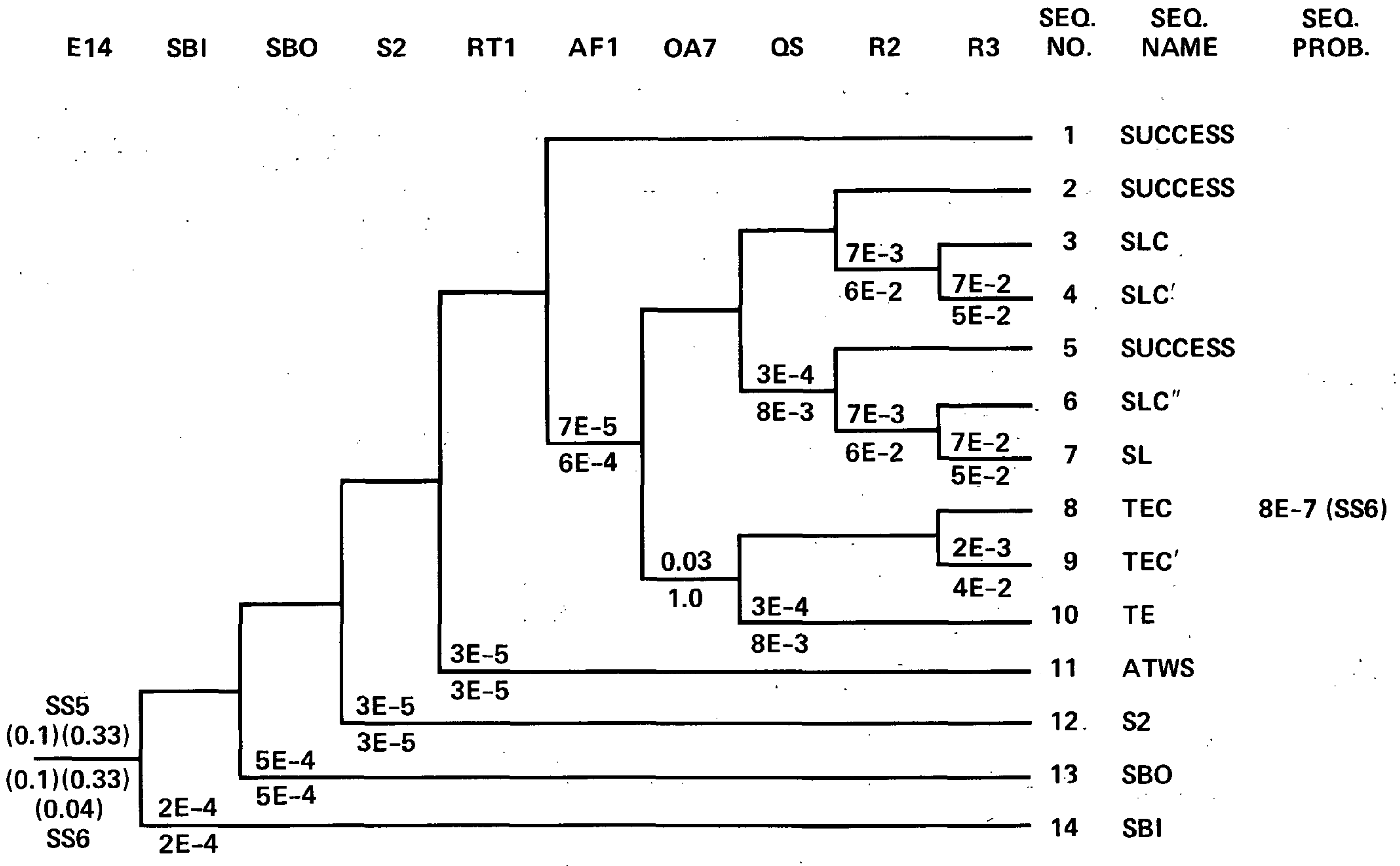
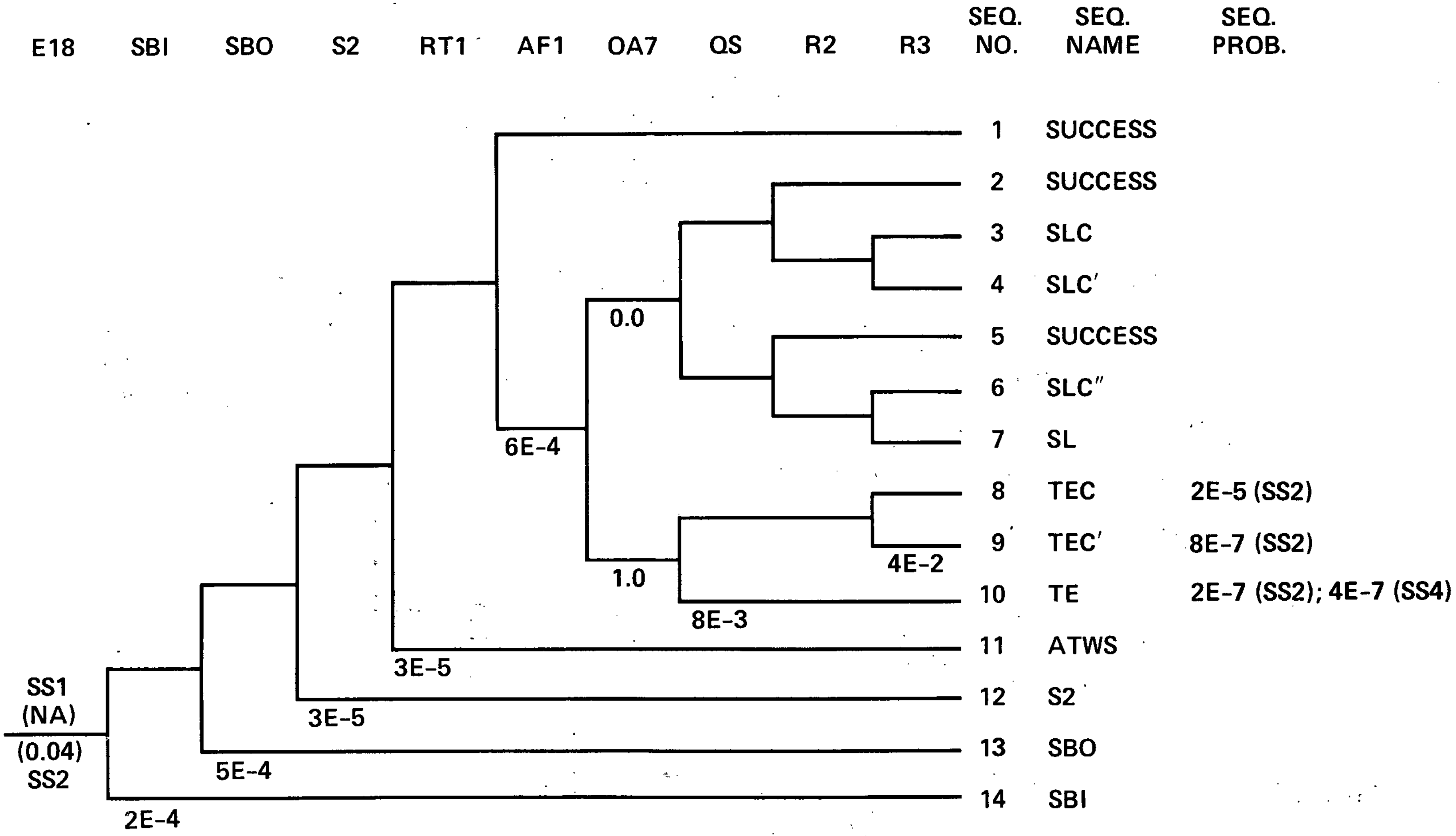
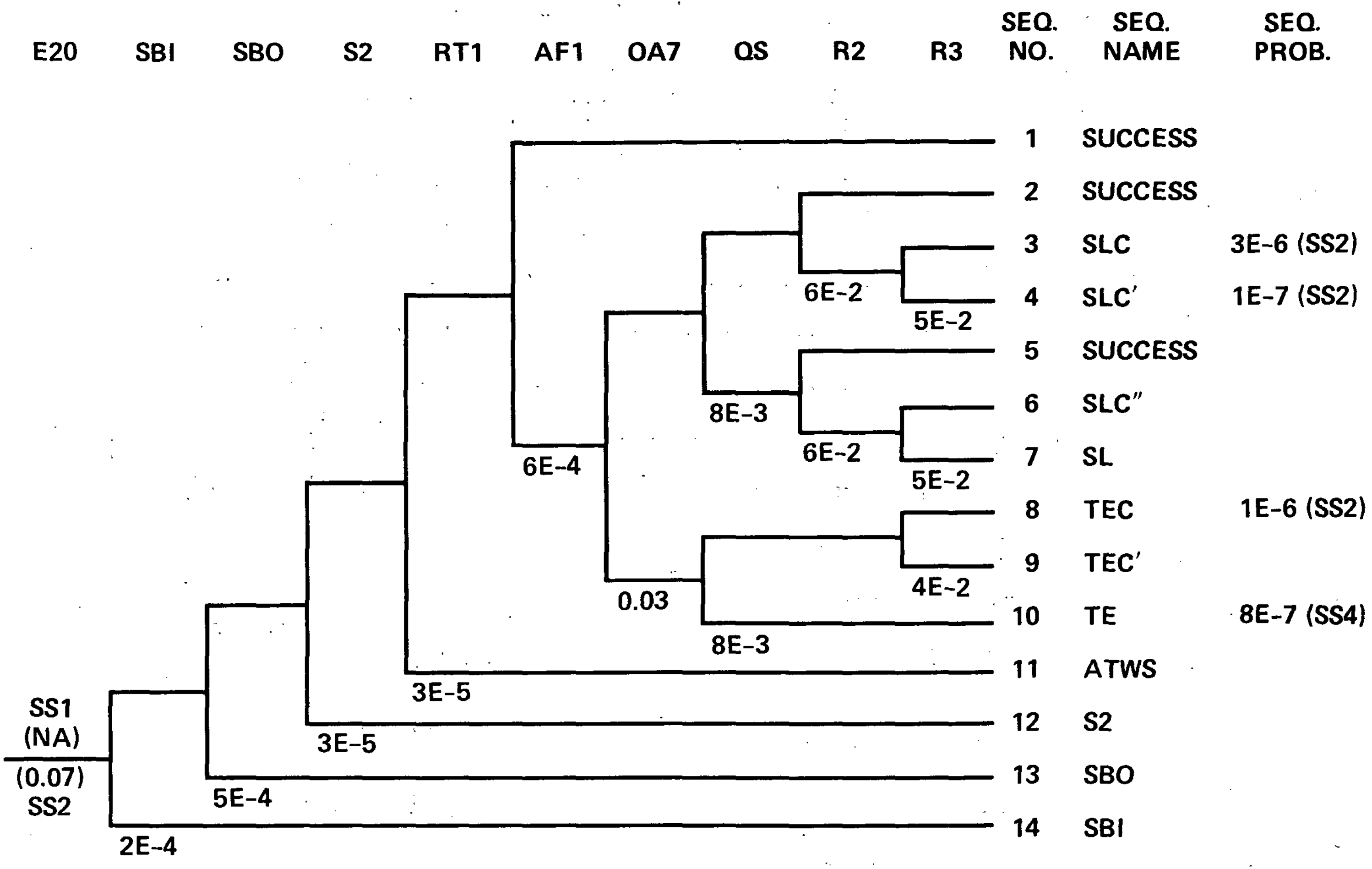


Fig. 3.12-8b Loss of offsite power (support states 5, 6) event tree.



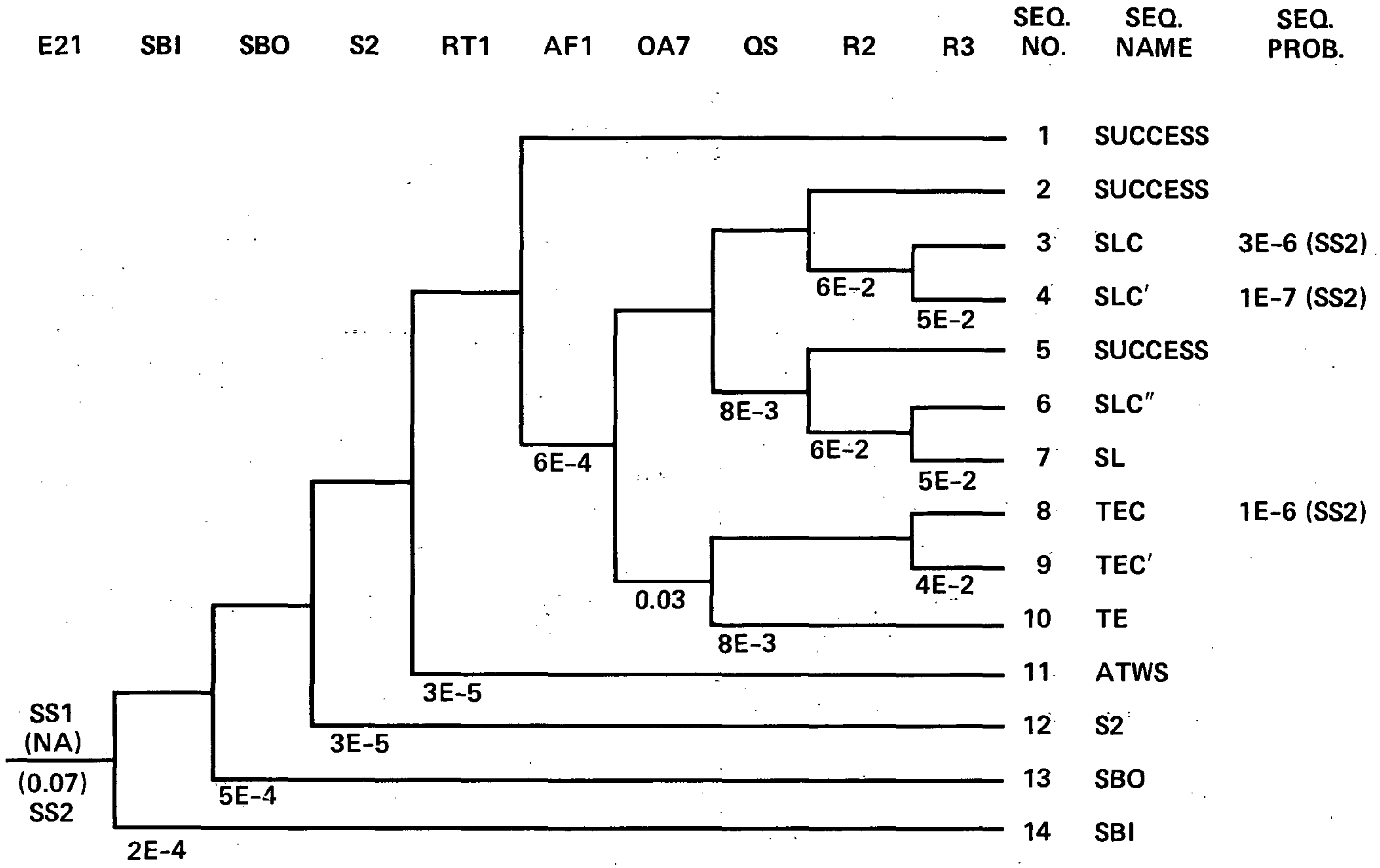
SS3 → (0.04)(1.6E-5)(6E-4) = 4E-10
SS4 → (0.04)(1.2E-5) = 4E-7 (TE)

Fig. 3.12-8c Loss of single DC bus event tree (Train A or B).



SS3 → (0.07)(1.6E-5)(6E-4) = 7E-10
SS4 → (0.07)(1.2E-5) = 8E-7 (TE)

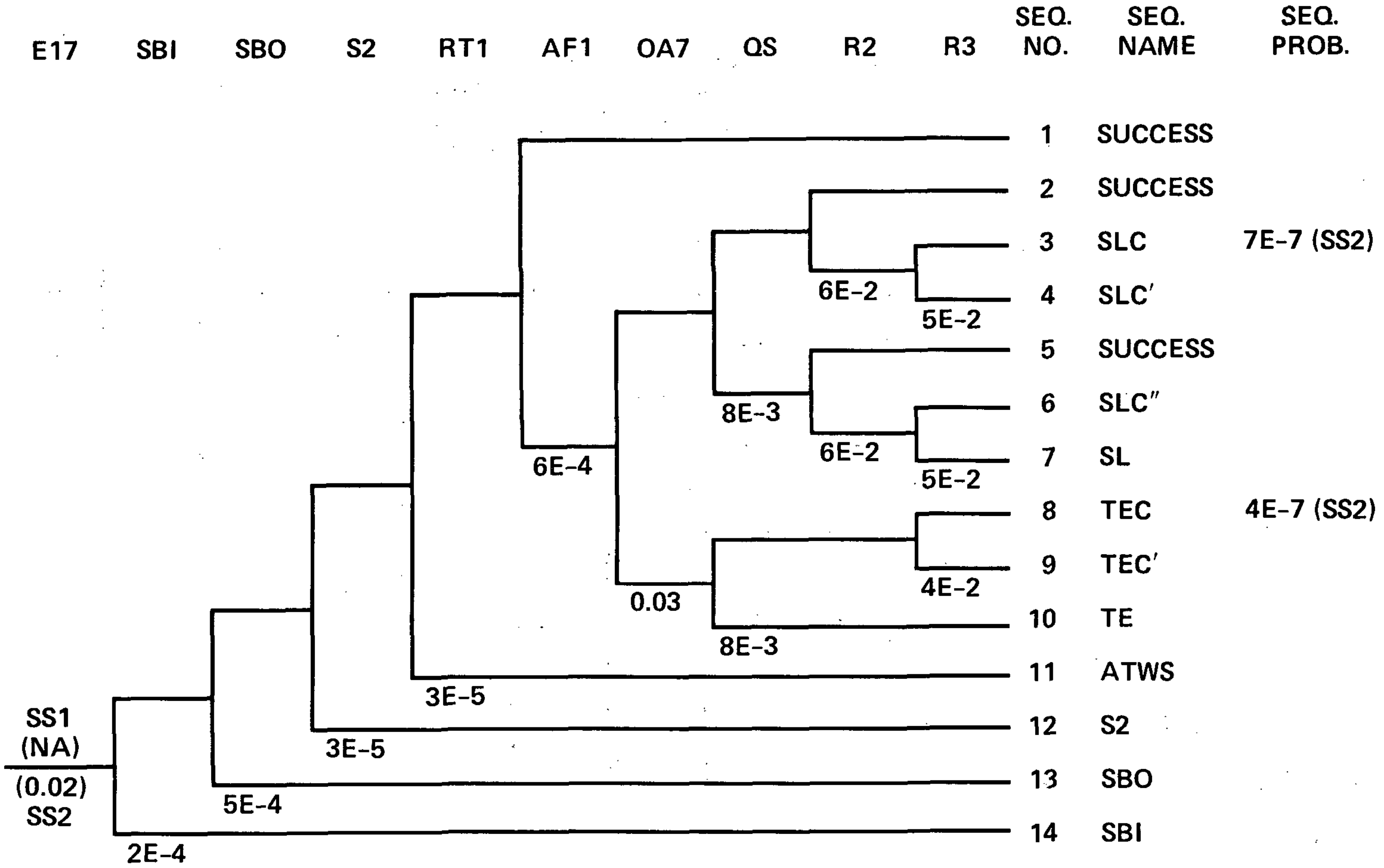
Fig. 3.12-8d Loss of vital AC bus 1 or 2 event tree.



SS3 → (0.07)(2.74E-5)(6E-4) = 1E-9

SS4 → (0.07)(1.61E-7) = 1E-8

Fig. 3.12-8e Loss of vital AC bus 3 or 4 event tree.



SS3 → (0.02)(4.47E-5)(6E-4) = 5E-10
SS4 → (0.02)(1.6E-7) = 3E-9

Fig. 3.12-8f Loss of a single service water train event tree.

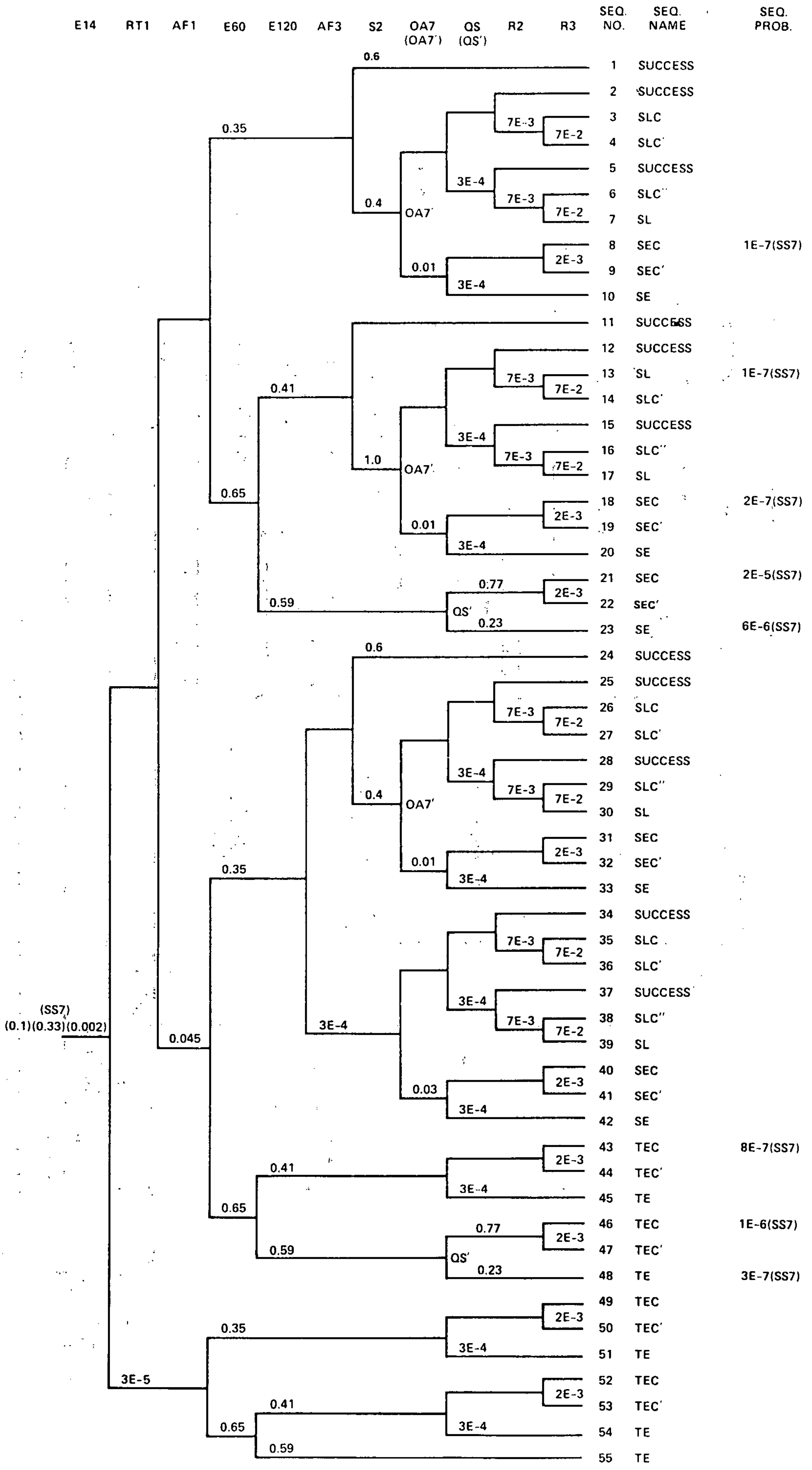


Fig. 3.12-9 Loss of offsite power (support state 7) event tree.

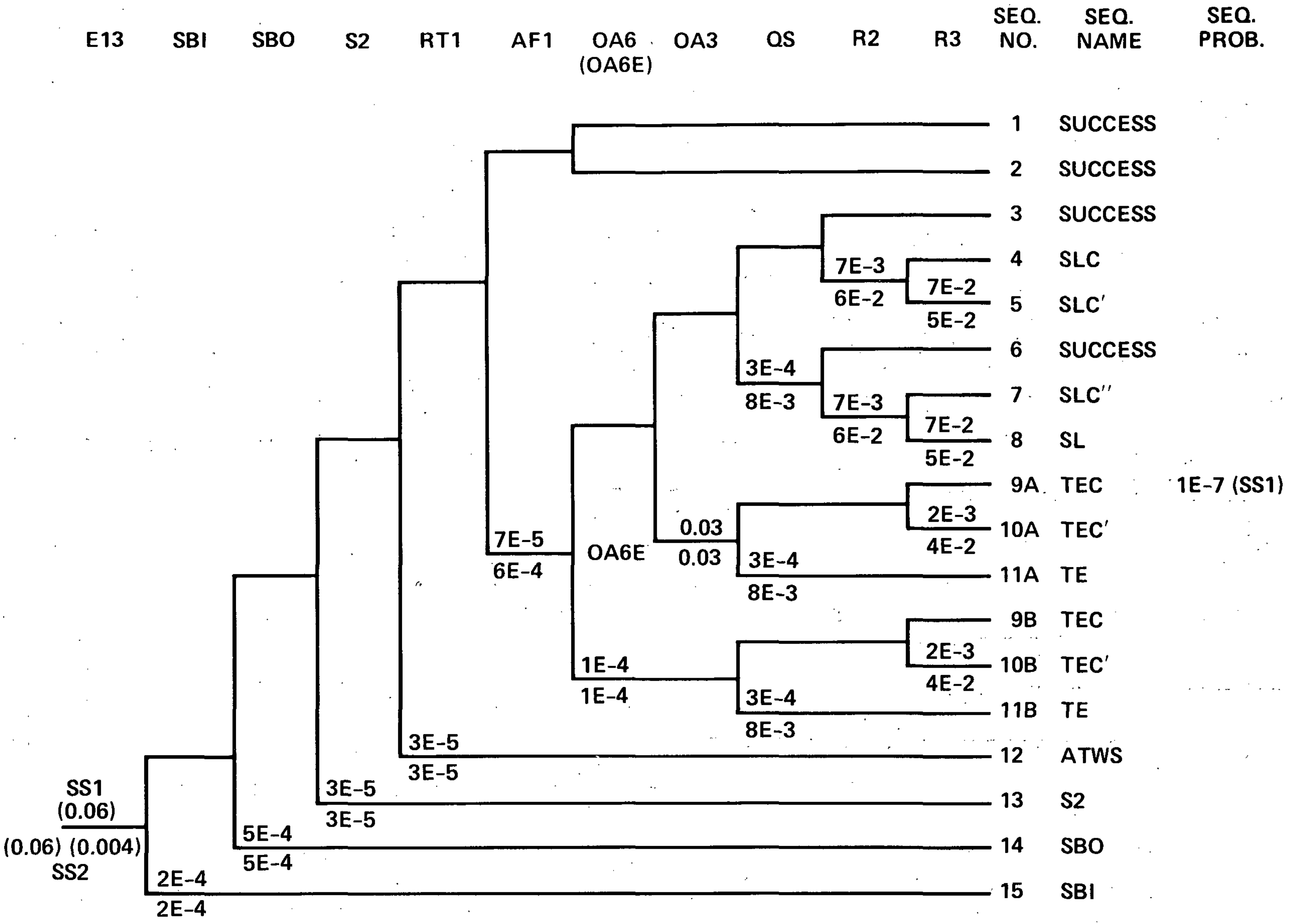


Fig. 3.12-10 Spurious safety injection event tree.

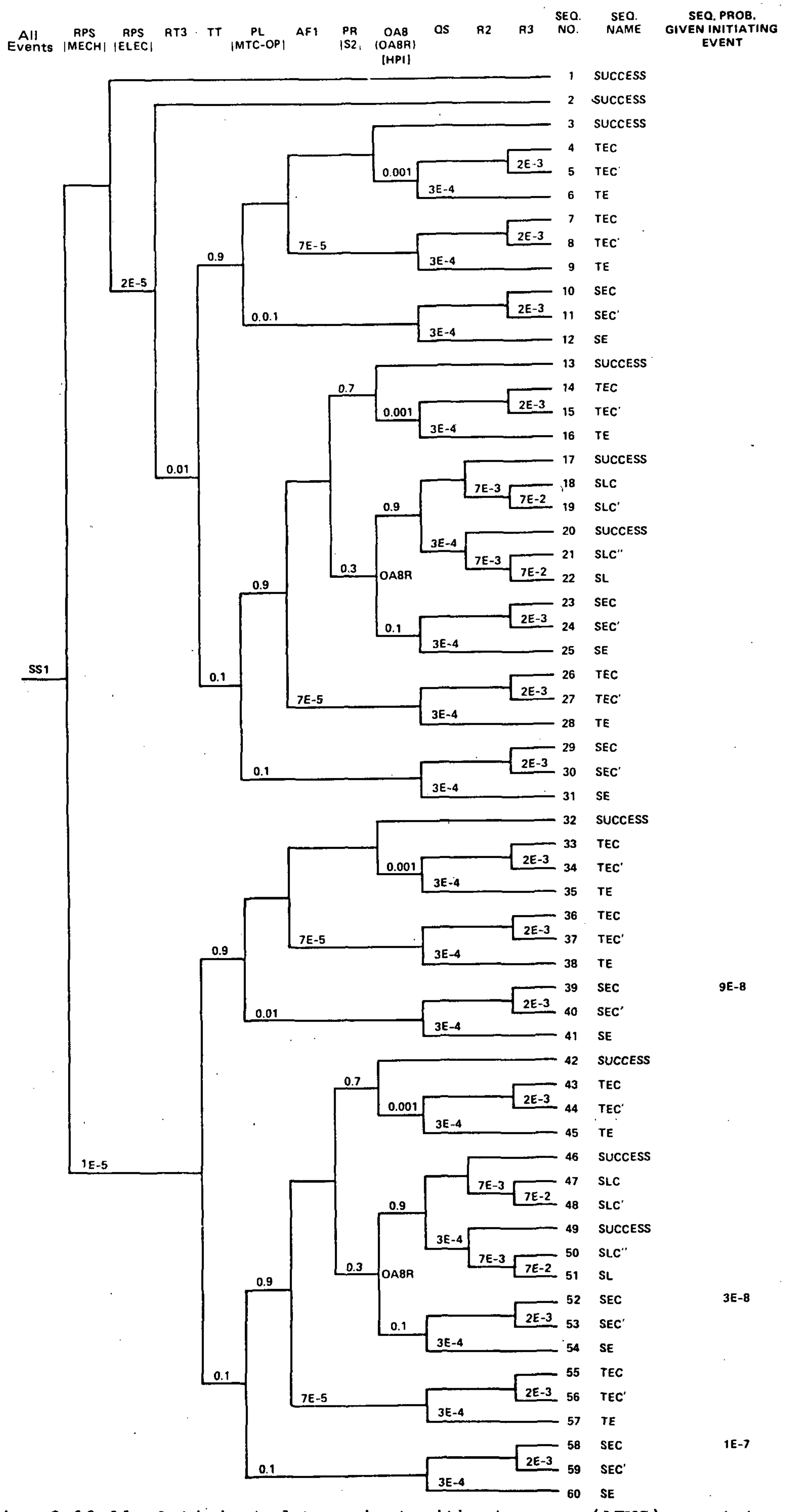


Fig. 3.12-11 Anticipated transient without scram (ATWS) event tree.

4. EXTERNAL EVENT ANALYSIS

The approach to the evaluation of external events taken in the MP 3 PSS included a screening analysis of a number of external events to identify those whose frequency of occurrence and consequences were significant enough to warrant additional detailed assessments. The screening evaluation reported in PSS Section 1.2 addresses earthquakes, fires, external flooding, internal flooding, extreme winds, aircraft accidents, hazardous materials, and turbine missiles. Only earthquakes and fires survived the screening analysis and were subjected to detailed assessments, which are reported in PSS Section 2.5. Our review covers each of these subjects in the sections which follow.

In general, the range of external event types considered in the PSS is reasonable and consistent with the external events assessed in other PRAs as well as those suggested by the PRA Procedures Guide. It should be noted that external events other than seismic and fire were treated only in a cursory manner.

We have numerous disagreements with the application and execution of the selected methodologies, both in the screening evaluation and in the detailed assessments. Areas of disagreement concern completeness, conceptual and logical errors, data, and the treatment of uncertainty. Examples of both conservative and optimistic treatment of the parameters are described below. In particular, important areas of disagreement exist in the evaluation of fire, external flood, and internal flood which have the potential to significantly increase the calculated core melt frequency for these events.

4.1 Seismic Events

LLNL reviewed the seismic event evaluation contained in the original PSS. This review included a review of seismic hazard, seismic-induced initiating events, seismic fragilities, and seismic core melt models. The overall results of this review, which are reported in Appendix A, were that the evaluation of seismic hazard was optimistic and not consistent with the state of the art, and that the fragility analysis was conservative and contained numerous errors. Details of the fragility review are contained in Appendix B.

After the review of the original PSS material was completed, NU submitted a substantially revised seismic evaluation as PSS Amendment 2, dated April 1984. The revised evaluation utilized extensively modified hazard and fragility curves. At NRC request, LLNL performed a review of the revised seismic fragility analysis contained in this amendment. The revised analysis was found to be consistent with the state of the art in this field. The details of this review are contained in Appendix C. The revised hazard curves were not reviewed by LLNL.

NU submitted a further revised seismic evaluation to NRC as PSS Amendment 3, dated November 1984, in which mathematical errors in the earlier documents were reported to be corrected. LLNL did not review this submittal.

4.2 Fire Events

This review is limited to an evaluation of the methodology for the assessment of risks from fires at Millstone Unit 3 nuclear power generation station. The validity of the event trees for the plant response given a fire has not been examined. Furthermore, the statements of the Millstone 3 PSS concerning the contents of various compartments and fire areas have not been verified.

It is convenient to conduct the evaluation of the analysis in terms of its three major parts, i.e.,

Part

I. The identification and screening of critical areas. The areas of the plant are screened to identify a limited number in which a fire can cause an initiating event (IE) and, at the same time, affect the performance of safety systems. The frequency of fires in these areas is assessed and a detailed analysis is performed. This part is contained in PSS Section 1.2.2.

II. The analysis of the fires in critical areas. Included in this part are the effects of detection and suppression on the growth of fires, as well as the identification of the impact of the fires on plant systems, and is contained in PSS Section 2.5.2.1.

III. Event tree analysis. This part includes the analysis of accident sequences induced by the fires. It produces the frequencies of relevant plant states and of core melt. It is found in PSS Section 2.5.2.2.

4.2.1 Overall Assessment

Regarding the methodology and its implementation, we find that:

(1) The screening process (Part I) is reasonable and complete. All fire areas warranting detailed analysis and evaluation have been identified. The frequencies of fires in various compartments are estimated using acceptable methods and are reasonable.

(2) The analysis of the loss-of-safety functions due to fires in the critical areas (Part II) is not rigorous and explicit. Cable routing and room configurations are neither used nor given. Thermal models for fire propagation are not used, in contrast to other PRAs, e.g., Zion (Ref. 4.2-1) Indian Point (Ref. 4.2-2) Limerick (Ref. 4.2-3), and Seabrook (Ref. 4.2-4). However, this lack of detail appears to lead the PSS to conservative values for the conditional frequency of losing all the safety functions that depend on a critical area (PSS Table 2.5.3.1-3). This issue is discussed further in Section 4.2.2.1 of this review.

(3) The event tree analysis (Part III) is reasonable (assuming the system unavailabilities are reasonable) with one exception. The error rate for the failure of the operators to switch control of the plant from the control room to the auxiliary shutdown panel is too low (see Section 4.2.2.2).

(4) The method of combining histograms two at a time leads to erroneous estimation of uncertainties when dependencies are present (see Section 4.2.2.3).

(5) The following items have not been addressed in the PSS:

a. The impact of earthquakes on fires and fire protection systems, e.g., fires started by earthquakes, sprinkler systems activated by earthquakes, etc.

b. Effects of the suppression agents on equipment.

c. Issues related to the response of equipment and cables to high heat fluxes and temperatures, e.g., fire barrier degradation, effects of hot-gas layers on cables, etc. (see comment (2) above).

It should be pointed out, however, that items (a) and (b) have never been addressed in any PRA performed to date.

(6) The impact on the numerical results of the conservatism noted in comment (2) and optimism noted in comment (3) above has been assessed in a crude sensitivity analysis in Section 4.2.2.4. It is found that the mean frequencies of plant damage state TE and core melt could be raised from 1.39E-6/RY and 4.80E-6/RY, respectively to 2.46E-5/RY and 2.80E-5/RY, respectively. This shows that the mean core melt frequency could be underestimated by the PSS by as much as a factor of roughly 6, (see Table 4.2-1).

4.2.2 Discussion of Findings

4.2.2.1 Thermal Models

Most major PRAs, e.g., those for Zion, Indian Point, Limerick, and Seabrook use the thermal models of Refs. 4.2-5 through 4.2-8. The principal tool in this approach is the computer program COMPBRN, which, essentially begins with the burning fuel element, releasing heat at a certain rate, then transmits this heat by convection and/or radiation to other elements, e.g., cables, and finally calculates the ignition time of these elements. Typical cases that have been analyzed in this manner include vertical fire propagation within a stack of horizontal cable trays, horizontal propagation across the width of a horizontal tray, and fire propagation among a group of separated trays when an external exposure fire is present. Special models have been developed for situations that do not fall in the preceding classes, e.g., for cabinets exposed to fires, for fire barriers, etc.

This approach requires knowledge of the location of the cable trays and cabinets, as well as their contents, in order to assess the fire's impact. The importance of transient fuels, exact location of the fire within the room, and the impact of special measures, like the installation of fire barriers, are some of the issues addressed in this approach. The detection and suppression times are represented by probability distributions that are combined with results of the thermal models to produce the fraction of fires that cause damage (Ref. 4.2-9).

This approach is not followed in the PSS. Cable tray configurations are not presented, although it is claimed on page 2.5-23 that they have been used. The notions of the total safety loss and partial safety loss are introduced to indicate whether all the safety functions or only part of them (in a fire area) have not been lost. The impact of detection and suppression is assessed using event trees.

The lack of detail has led the PSS to values for the conditional fraction of fires that cause safety loss that are high (the mean values reported in PSS Table 2.5.2.1-3 are in the neighborhood of 0.1).

As an example, we use the cable spreading room (CSR). The fraction of fires causing a safety loss given a fire in the CSR is given as 9.25E-2 PSS Table 2.5.2.1-3). This number is derived from the event tree of PSS Fig. 2.5.2.1.2-1 which assesses the impact of the detection and suppression capabilities in the room. Even though the Indian Point 3 PRA does not follow the methodology of the Millstone 3 PSS, we can derive the corresponding number for the CSR by multiplying the mean value of the fraction of CSR fires that are "large and near the center of the northern wall" (0.026) with the mean value of the conditional frequency of fire propagation (0.44, the result of COMPBRN and the detection and suppression distributions). The result is 1.1E-2, i.e., nearly an order of magnitude smaller than the PSS number. The main reason is that the Indian Point PRA has taken advantage of the fact that only fires "near the center of the northern wall" within the CSR can cause significant damage. Recent evidence (Ref. 4.2-10) suggests that even COMPBRN may be too conservative in some cases, so that the mean value of the conditional frequency of fire propagation may, in fact, be lower than 0.44. It appears, therefore, reasonable to say that the Indian Point number is roughly one order of magnitude lower than that of the PSS.

4.2.2.2 Human Error Rate

The human error rate of 0.001 (error factor of 3) for failure to switch control to the auxiliary shutdown panel (basic event SEQ) is not adequately justified and is too low. Furthermore, the distribution of this rate appears to be too narrow. It is explained on PSS page 2-D-8 that the procedure for transferring of control to the ASP will be practiced on a regular basis by the

Table 4.2-1 Results of the sensitivity analysis (all frequencies are reactor-year).

	PSS	Modified results
Contribution to TE from the control room, instrument rack room, and cable spreading room	1.222E-6	2.444E-5
Contribution to TE from other areas	1.68E-7	1.68E-7
Total TE frequency	1.39E-6	2.46E-5
Total core melt frequency	4.80E-6	2.80E-5
Percent contribution of TE to core melt frequency	29%	88%

operations personnel; therefore, "the NREP screening value for human errors occurring within a procedural framework where recovery is possible at the point of erroneous action is used to estimate the HEP for this analysis." This argument, however, ignores the fact that the switching would have to take place under accident conditions during which stress on the operators would be high.

A similar human error is analyzed in Section 9.4.6.4.2 of the Seabrook PRA (Ref. 4.2-4). It is stated there that the "stress level is deemed to be high because of the...very confusing conditions in the control room." The mean value of 0.23 is proposed for this error rate (the 5th percentile is assessed to be on the order of 0.02, still substantially higher than the values of the MP 3 PSS).

4.2.2.3 Method of Calculation

When the uncertainties are propagated through a function (by DPD, Monte Carlo, or any other method), the dependencies between events must be correctly accounted for. This does not seem to be the case here, where the histograms are combined two at a time. The impact of this omission is not expected to be large, because of the simplicity of expressions that are calculated.

An interesting argument appears on PSS page 2.5-31. There seems to be an attempt here to justify the difference between the "point" estimate and the mean of the histogram that is calculated using DPD arithmetic. This is unnecessary. The point estimate calculations usually ignore various dependencies which DPD can easily handle (but, unfortunately not here, as indicated earlier). Furthermore, there is no reason to increase the upper tail of a histogram in order to make the probabilities add up to unity. A simple renormalization would be sufficient. Again, the impact of this practice is expected to be minor.

4.2.2.4 Sensitivity Analysis

We assess here the impact on the numerical results of the PSS of the two major findings of this review. In Section 4.2.2.1 we argued that the conditional fractions of total safety loss are roughly one order of magnitude too high. In Section 4.2.2.2 we found that the human error rate for basic event SEQ could be too low by roughly a factor of 200 (all our values are mean values). The plant damage state that is affected the most by these two findings is TE (see PSS Fig. 2.5.2.2.2-1), to which fires in the control room (CR), instrument rack room (IRR), and cable spreading room (CSR) are the major contributors. To do a crude sensitivity analysis, we assume that the combined impact of these two findings is to increase the contribution to TE from these three fire zones by a factor of 20.

In PSS Table 2.5.2.3-1 we find that the contribution to TE from these three rooms is 4.54E-7 + 1.52E-7 + 6.16E-7 = 1.222E-6/RY. Therefore, the contribution from other areas to TE is 1.39E-6 - 1.222E-6 = 1.68E-7/RY.

The new contribution from the CR, IRR and CSR is 1.222E-6 x 20 = 2.444E-5/RY and the new total frequency of TE is 2.444E-5 + 1.68E-7 = 2.46E-5/RY.

The mean core melt frequency is reported in PSS Table 2.5.2.3-1 as 4.80E-6/RY. Of this, 1.39E-6 (29%) is due to TE and 3.41E-6 (71%) is due to other plant damage states (the dominant one being TEC). With the new numbers, the total core melt frequency is 2.46E-5 + 3.41E-6 = 2.80E-5/RY. The dominant plant state is now TE (87.8%). We note that the core melt frequency has been increased by a factor of about 6. These results are summarized in Table 4.2-1.

It should be noted that the contribution from zones other than the CR, IRR, and CSR would actually be smaller because only the conservative number of the PSS appears there and not SEQ, assuming, of course, that the unavailabilities of the system listed in PSS Table 2.5.2.2.1-1 are accurate.

This crude sensitivity analysis addresses only the two identified issues. An accurate reassessment must consider the full distributions and not only mean values. Furthermore, this analysis does not include the impact of the items that are beyond the state-of-the-art (listed under comment (5) of Section 2). Since no PRA has attempted to investigate them, it is difficult to assess their significance.

Finally, we note that the PSS analysis has addressed the issue of major fires that could, in combination with other failures, lead to core melt. In fact, it is stated on PSS page 1.2-7 that "critical" areas are areas where a fire can cause an initiating event and fail engineered safeguards. While it is reasonable to consider only the "critical" areas in the fire analysis, fires in other areas should be included in the calculations of frequencies of initiating events and system unavailabilities as appropriate. We are unable to judge whether these fires have been so included.

4.2.3 References for Section 4.2

4.2-1 Commonwealth Edison Company, "Zion Probabilistic Safety Study," 1981.

4.2-2 Pickard, Lowe and Garrick, Inc., "Indian Point Probabilistic Safety Study," prepared for Power Authority of the State of New York, and Consolidated Edison Company of New York, Inc., 1982.

4.2-3 NUS Corporation, "Severe Accident Risk Assessment for the Limerick Generating Station," prepared for Philadelphia Electric Company, April 1983.

4.2-4 Pickard, Lowe and Garrick, Inc., "Seabrook Station Probabilistic Safety Assessment," prepared for Public Service Company of New Hampshire and Yankee Atomic Electric Company, 1983.

4.2-5 N. O. Siu, "Probabilistic Models for the Behavior of Compartment Fires," USNRC Report NUREG/CR-2269, August 1981.

4.2-6 N. O. Siu, "COMPBRN-A Computer Code for Modeling Compartment Fires," USNRC Report NUREG/CR-3239, May 1983.

4.2-7 N. O. Siu and G. Apostolakis, "Probabilistic Models for Cable Tray Fires," Reliability Engineering, 3:213-227, May 1982.

4.2-8 N. O. Siu, "Physical Models for Compartment Fires," Reliability Engineering, 3:229-252, May 1982.

4.2-9 G. Apostolakis, M. Kazarians and D. C. Bley, "Methodology for Assessing the Risk from Cable Fires," Nuclear Safety, 23:391-407, July-August 1982.

4.2-10 G. Chung, N. O. Siu and G. Apostolakis, "COMPBRN II: Code Description and Simulation of Experiments," Draft Report, UCLA-ENG-8404, University of California, Los Angeles, March 1984.

4.3 External Flooding[a]

In Section 1.2.3 of the Millstone PSS, it is concluded that external flooding is an insignificant contributor to plant risk. Only two sources of external flooding are considered to potentially impact the Millstone site - tidal flooding and intense precipitation. Since there are no major rivers or streams in the vicinity of Millstone Point, river flooding and dam failure are not considered applicable to the site. Tsunamis are also excluded since there is an extremely low probability that these events will occur along the North Atlantic coast line.

The justification for excluding external flooding from the formal risk analysis is made on a qualitative basis. No formal probabilistic analysis was performed. Tidal flooding and intense precipitation are based on the effects of the probable maximum hurricane (PMH) and the probable maximum precipitation (PMP), respectively. No probability values are given; however, these events are judged to have a point estimate frequency of occurrence between 1E-6 to 1E-4/RY. This estimate is based on an approximate analysis using available hurricane hazard data in the vicinity of the Millstone site (Refs. 4.3-1 and 4.3-2).

The description of the calculations, which were conducted to obtain the maximum wave runup and standing wave height due to the PMH and the flood depth due to the PMP, are contained in the FSAR (Ref. 4.3-3). It is apparent from the description given that conservatisms were included in the calculations (e.g., the most severe combination of hurricane parameters were used to represent the PMH and the site yard drains were considered ineffective in the PMP analysis). However, the amount of additional conservatism is not known. It is not necessarily true that single extreme events are the only circumstances that contribute to the risk. Also, the PMH and PMP may be correlated since the PMP could be caused by the PMH.

In contrast to the seismic analysis, the external flooding analysis did not explicitly consider the uncertainty (which is large) in the underlying parameters and models. Even at the 100-year storm level, the coefficient of variation on water depth is expected to be approximately 0.2 to 0.3. Thus, the conclusion that external flooding has a very low frequency of occurence is not convincing without some formal quantification of the hazard.

[a] This section is reproduced here from Appendix B, with minor editorial changes, for the convenience of the reader.

In including the effect of uncertainties in the external flood analysis, a distribution on the frequency of occurrence can be obtained. The present analysis implies that the frequency of flooding above the protected elevation is small. However, the margin of safety above the PMH and PMP design elevation is also small (less than one foot for the PMH and less than an inch for the PMP).

As an example, the point estimate for the PMH might be 1E-5/year; however, because of the large uncertainties that are present, there is a small but finite probability that the frequency of the PMH is 1E-4/year or larger. Similarly, it can be argued that there is a potential hurricane bigger than the PMH which could produce a wave runup which exceeds the watertight elevation of 25.5 feet mean sea level (msl). The point estimate for this event might be on the order of 1E-6/year; however, due to uncertainty, there also is a small but finite probability that it is 1E-5/year or larger. Proceeding in this manner, it can be shown that including uncertainty will result in a family of hazard curves which may increase the mean frequency of water depth above the value obtained using only a single point estimate value (i.e., the PMH). In order to evaluate the implications of a water level greater than 25.5 feet msl, it is necessary to either conservatively assume core melt or to develop event trees, fault trees, and equipment fragilities to systematically incorporate the plant's unique features into the uncertainty analysis.

In summary, a formal analysis should be conducted which provides frequencies of occurrence and includes uncertainty in the external flood models and parameters. Because of the large uncertainties which exist for external flood, there is the possibility that the mean frequency of core melt is larger than 1E-6. In order to conclude that the contribution from external flooding is insignificant relative to other hazards, a complete statement of the probability distribution on frequency of occurrence should be provided.

4.3.1 References for Section 4.3

4.3-1 Pickard, Lowe and Garrick, Inc., "Indian Point Probabilistic Safety Study," prepared for Power Authority of the State of New York, and Consolidated Edison Company of New York, Inc., 1982.

4.3-2 M. E. Batts, et al., "Hurricane Wind Speeds in the United State," NBS Building Science Series 124, National Bureau of Standards, May 1980.

4.3.3 Northeast Utilities, "Final Safety Analysis Report, Millstone Unit 3," 1983.

4.4 Internal Floods

This section describes the review of methods and procedures used in the Millstone 3 PSS for assessing the consequences of reactor accidents involving internal floods. The conclusion of this review is that the flood analysis is incomplete and the results of the analysis are speculative. A major limitation of the analysis is the absence of calculations for flow rates, drainage rates, and flood levels. Instead, the PSS presents a qualitative treatment of flood hazard and concludes that internal flooding is not a significant contributor to core melt. A particular concern is that the approach used could downgrade the importance of flooding in some zones such as the switchgear and cable spreading rooms.

The PRA procedures guide (Ref. 4.4-1) states that, for some nuclear power plants, internal floods can be an important cause of multiple dependent failures. This guide proposes that a flood risk analysis consists of a hazard assessment, a component fragility evaluation, a plant system repsonse assessment, and a release frequency analysis. The hazard assessment involves both a qualitative evaluation in which specific flood scenarios are selected for quantification and a quantitative assessment that provides an estimate of the frequency of specific damage states. The flood hazard assessment is conceptually similar to a fire hazard assessment. However, according to the procedures guide, significant among the distinctions between these assessments are that sources of flooding should be more easily and completely enumerated and that floods are more likely to propagate.

4.4.1 Overview of the Millstone 3 Internal Flood Analysis

The risk assessment of internal flooding for Millstone 3 consisted of a qualitative evaluation in which specific scenarios were selected for further evaluation, and a quantitative evaluation where the frequency of exceeding various accident consequences was estimated. The qualitative analysis involved an evaluation of floor plans at various elevations to determine the critical safety-related components or systems that would be affected by a single flooding event. In order to conduct this analysis, buildings and facilities at the Millstone 3 site were divided into "flood zones." According to the PSS, the flood zones were established using fire boundary areas but fire boundary areas "did not constitute the sole basis for establishment of a flood zone." Whatever additional criteria were used to establish these zones were not discussed in the PSS.

The established flood zones were reviewed for possible sources of internal flooding. Table 4.4-1 provides a list of plant systems considered credible flood sources in the PSS. Each source was assumed to have a flooding frequency of 2E-3/year. It is stated that this is derived from the WASH-1400 estimate for the frequency of a pipe break greater than 6 inches. A postulated flood was assumed to disable all components within the flood zone corresponding to the source. Consideration was also given to progressive flooding, in which sufficient water is discharged in one zone to flow to and affect safety equipment in an adjacent zone. Where the potential exists for progressive flooding, all components in the progressively flooded zone are also assumed to be disabled.

If the loss of all components within a flooded zone would not initiate a transient or LOCA or if no safe shutdown equipment was disabled, that flood zone is removed from further analysis. Flood zones not removed by this screening process were subjected to further analysis. This consisted of multiplying the unavailability (2E-3/year) of the systems disabled by flooding by the unavailability of redundant or alternate systems that could substitute for the flood-damaged systems in preventing core damage. The latter unavailabilities were taken from the results of the plant event and fault tree analyses.

The procedures described above were used to determine that core melt induced by internal flooding has an estimated frequency of 8.5E-7/year. Based on the analysis, the PSS further concludes that internal flooding does not significantly contribute to overall plant risk.

4.4.2 State-of-the-Art in Flood Risk Analysis

The most extensive analysis system currently available for assessing the risks associated with internal floods is the ESP-NOAH code package (Ref. 4.2-2). The flood risk analysis methods in this package are designed to identify and quantify flood impacts by using the results of the plant's systems failure analysis. ESP identifies accident sequences and systems that can contribute to plant risk as result of floods. The input to ESP consists of accident sequences and system failure probabilities obtained from the fault and event tree analysis, engineering criteria describing system susceptibility to flooding, and the flood probabilities. ESP screens the accident sequences based on the engineering criteria and determines important system failures and accident sequences along with a quantitative estimate of each sequence's contibution to overall flood risk. The important system failures identified by ESP are candidates for a more detailed systems analysis using NOAH.

Table 4.4-1 Plant systems considered as credible flood sources.

1.	Main feedwater system
2.	Auxiliary feedwater system
3.	Service water system
4.	Chemical and volume control system
5.	Reactor plant component cooling water system
6.	Turbine plant component cooling water system
7.	Chilled water system
8.	Site fire protection system
9.	High pressure safety injection system
10	Low pressure safety injection system
11.	Condensate and demineralized water storage system
12.	Boron recovery system
13.	Gaseous waste disposal system
14.	Circulating water system

The NOAH program also uses system fault trees as input to make a quantitative flood risk assessment. Other inputs to NOAH include flood level increments within the plant (discretized flood level profile) and the effective elevation of each component in a fault tree (component vulnerability elevation). With this information, NOAH simulates the flooding of components in the fault tree. The output of this simulation is the order of component submersion and the flooded minimal cut sets, if any exist. If no flooded minimal cut sets exist, NOAH determines partially flooded minimal cut sets. These cut sets represent the system failure modes during flooding and provide input to the quantitative evaluation of system failure probability as a function of flood level.

4.4.3 Comments on the Internal Flooding Analysis in the Millstone PSS

Each zone containing a flood source is assumed to have a flood frequency of 2E-3/year. The basis for selecting this value is quite weak. It was stated to be derived from a WASH-1400 estimate for breaks in pipes with a diameter greater than six inches. This approach provides no estimate of the actual flood sources present in each zone. As far as we can determine, WASH-1400 only provides pipe break frequencies per hour per pipe segment as a function of pipe size. The PSS does not make clear how this information could be used to calculate or estimate this "generic" value for flood frequency. The only apparent way that flood frequencies could be calculated from WASH-1400 data is to count all pipe segments in a zone in each size category and use the pipe segment failure frequencies together with flow capacities to calculate the annual probability of exceeding a given flood hazard in each zone. The simplistic approach actually employed in the PSS leaves doubt as to whether the analysis is capable of screening the potentially important flood sources in the Millstone plant.

Inadvertent actuation of fire protection equipment was not considered as a potential flooding source. Excluding such sources is likely to make the results optimistic, since fire sprinklers generally spray directly onto components so that significant water heights may not be necessary to cause equipment failures. However, some consideration of this problem should be, and usually is, taken up during plant design.

The PSS made the conservative assumption that all components in a flood zone are disabled if a flood occurs in that zone.

It is stated in the PSS that the flooding analysis includes ruptures of pipes, tanks, or vessels. However, the review found no tanks or vessels used as flood sources. The RWST was included in the analysis, but only in terms of the pipes that lead from it, not rupture of the vessel itself. The PSS states that flooding caused by overfilling of tanks is bounded by the effects of pipe breaks. This assumption was used without even a qualitative justification, which we believe diminishes the value of the analysis.

Although the PSS deals with progressive flooding (from one zone to another), it is difficult to determine the modeling assumptions used to treat this process. In particular, it is difficult to establish what criteria were used to decide when progressive flooding occurs. A review of the progressive flooding tables in the PSS reveals that progressive flooding was considered between some, but not all, adjacent zones connected by a door. Similarly, progressive flooding to zones directly below a flooded zone was assessed in some cases but not in others. There were also cases in which flooding occurs between zones with common walls but no door. The PSS states that a progressive flood will occur when the water level in a particular zone reaches 5 feet. This is based on the assumption that the fire boundary can withstand a differential pressure of 2 psid. This assumption appears reasonable even though no actual boundary analysis was performed. Nevertheless, the procedure used to determine if a flood could reach this height was not described. The only relevant information included was that closed systems (such as component cooling) did not contain enough water to cause progressive flooding - a reasonable assumption. It could not be determined from the PSS what analysis was used to determine the volume of water released in flooding by sources other than closed systems.

The PSS assumes that a reactor trip occurs following any flood-induced initiating event. This appears to be an optimistic assumption; however, it is not likely that the implications of this assumption are significant.

The PSS assumes that if a flood in a given zone does not initiate a transient or LOCA (by impacting a component necessary for normal operation) or disable safe shutdown equipment, then that zone can be eliminated from further consideration. This assumption is questionable because it implies that a plant continues to run during a flood. Futhermore, it excludes from the analysis those zones that contain important safety equipment not directly necessary for normal operation or shutdown. It may be more reasonable to assume that operators would be required to shut down when significant flooding is discovered in any area of the plant.

The analysis of flooding in the switchgear and cable-spreading rooms indicates that core melt induced by flooding in these areas has a frequency of about 1E-6/year. Because of the large uncertainty in the screening analysis performed for Millstone PSS internal flooding, a frequency of this magnitude should suggest the need for additional analysis. However, no further analysis was performed. Instead, the PSS reduced the frequency by multiplying with the factor 0.7, which is described as the probability of damaging all cables in the room. The basis of this factor is not described or justified. Futhermore, the results of the flooding analysis strongly suggest that internal flooding can not simply be dismissed as comparable to fires as a cause of core melt, contrary to the conclusions of the PSS.

4.4.4 Conclusions

The internal flooding analysis performed in the Millstone PSS can be characterized as a predominately qualitative screening analysis with numbers attached to reflect the authors' best estimates. The process results in an estimated frequency of internal flood-induced core melt of 1E-6/year. The simplistic approach leads us to question whether the analysis is capable of screening the potentially important flood sources in the Millstone plant. In addition, the uncertainties inherent in the analysis indicate that the results could be in error by orders of magnitude. The results of the screening analysis would have to be at least an order of magnitude lower to allow internal flooding to be dismissed as a contributor to core melt risk. In our opinion, internal flooding in the cable spreading and switchgear rooms should have been assessed in more detail using realistic flow rates, drainage rates and flood levels rather than arbitrary values.

4.4.5 References for Section 4.4

4.4-1 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.

4.4-2 D. P. Wagner, M. L. Casada, and J. B. Fussell, "Flood Risk Analysis Methodology Development Project Final Report," USNRC Report NUREG/CR-2678 (ORNL/TM-8314), 1983.

4.5 Extreme Winds[a]

PSS Section 1.2.5 concludes that wind does not contribute significantly to plant risk. The governing wind event at the Millstone site is the occurrence of severe tornados. In general, the effects of tornados, hurricanes, and extratropical cyclones (i.e., normal winter storms and thunderstorms) should be considered in the wind risk analysis. As discussed below, it is agreed that tornado effects, which potentially create much larger loads, do not contribute significantly to plant risk; thus, the effects of other wind loads are implicitly included.

It is stated that all Millstone Unit 3 safety-related structures are of reinforced concrete construction with wall thicknesses of at least 2 feet. Except for some of the quench spray system components, all other safety-related components are contained in safety-related structures (Ref. 4.5-1, Table 3.2-1).

Based on the analysis described in Section 1.2.5.1.1 of the Millstone 3 PSS, it is stated that the frequency of exceeding the design tornado wind speed of 360 mph is approximately 5.4E-6/year. It is believed that this value is very conservative, as discussed below.

At the Indian Point site, which is approximately 100 miles away and is in an area with higher tornado activity based on historic data, the mean maximum tornado wind speed at the 1E-7/year frequency level is 230 mph with an 80% confidence range of 170 to 340 mph (Ref. 4.5-2). Other independent point estimates for the Indian Point site at this frequency level are 236 mph and 200 mph (Ref. 4.5-3). Note that these results are significant since the reported mean rate of tornado occurrence in the Millstone Unit 3 PSS is 1.87E-4 per square mile per year, which is lower than the value of 2.4E-4/year per square mile per year used in the Indian Point study (Ref. 4.5-2).

A recent technical paper by Twisdale gives velocity frequency curves for four regions of the contiguous U.S. (Ref. 4.5-4). None of the curves extend beyond 300 mph. Finally, using an approach developed by Reinhold (Ref. 4.5-5), the mean frequency using a tornado occurrence rate of 1.87E-4 per square mile per year was found to be less than 1E-8/year. It is concluded that the mean frequency of occurrence of tornados with maximum wind speeds equal to or greater than 360 mph is less than 1E-8/year.

[a] This section is reproduced here from Appendix B, with minor editorial changes, for the convenience of the reader.

On the capacity side of the problem, all safety-related structures are designed, using code procedures and allowable strength values, to resist wind speeds of 360 mph and associated tornado missiles. From a probabilistic viewpoint, the frequency of structural failure or missile-induced damage given a 360 mph tornado would be one to two orders of magnitude lower than the frequency of the tornado occurrence.

Because of the extremely low mean frequencies of failure (i.e., on the order of 1E-9 to 1E-10/year), it can be safely concluded that tornado (and hence other lesser wind types) effects are not significant. Even considering the contribution of uncertainty, it is unlikely that the effects of wind would contribute significantly to the plant risk.

4.5.1 References for Section 4.5

4.5-1 Northeast Utilities, "Final Safety Analysis Report, Millstone Unit 3," 1982.

4.5-2 Pickard, Lowe, and Garrick, Inc., "Indian Point Probabilistic Safety Study," prepared for Power Authority of the State of New York, and Consolidated Edison Company of New York, Inc., 1982.

4.5-3 G. J. Kolb, et al., Sandia National Laboratories, "Review and Evaluation of the Indian Point Probabilistic Safety Study," USNRC Report NUREG/CR-2934, December 1982.

4.5-4 L. A. Twisdale and W. L. Dunn, "Probabilistic Analysis of Tornado Wind Risks," Journal of the Structural Division, ASCE, Vol. 109, No. 2, February 1983.

4.5-5 T. A. Reinhold and B. Ellingwood, Brookhaven National Laboratory, "Tornado Damage Risk Assessment," USNRC Report NUREG/CR-2944, September 1982.

4.6 Aircraft Accidents

The PSS analysis of on-site aircraft crashes is presented in PSS Section 1.2.6.2. It includes a quantitative assessment of crash frequency performed in accordance with NRC Standard Review Plan, Section 3.5.1.6 (Ref. 4.6-1). The results of this assessment include the following total frequency estimates for three classes of aircraft:

• general aviation	1.5E-6/year
• commercial aviation	1.2E-7/year
• military aviation	3.4E-9/year

These numbers were calculated by considering aircraft operations at two nearby airports and aircraft traffic (inflight) accidents in three nearby Federal airways.

Aircraft operations were considered at the New London-Waterford Airport, which services only general aviation, and at the Groton-New London Airport, which services general, commercial, and military aviation.

The effective plant area susceptible to damage from general aviation was taken to include only the unit 3 switchyard and determined to be 4.6E-3 square miles. The effective plant area susceptible to damage from commercial and military aviation was taken to include the containment structure, auxiliary building, control building, ESF building, main steam building, emergency generator enclosure, and the unit 3 switchyard. This area was determined to be 9.5E-3 square miles. These choices and areas are considered reasonable and conservative.

The results of the quantitative assessment of airport operations were crash frequencies of:

• general aviation	
New London - Waterford	2.5E-7/year
Groton	1.2E-6/year
• commercial (Groton)	1.1E-7/year
• military (Groton)	3.4E-9/year

Consideration of potential in-flight accidents in the three nearby Federal airways which could result in on-site aircraft crashes used an effective plant area of 9.5E-3 square miles (the figure for commercial and military aircraft) and yielded the following crash frequencies:

Airway V-16	1.1E-8/year
Airway V-58	5.5E-10/year
Airway V-374	1.5E-10/year

The overall results are consistent with the one-paragraph discussion of aircraft hazards in FSAR Section 3.5.1.6 (Ref. 4.6-2) which states that, "A study of the probability of aircraft which use nearby airports and airways colliding with the safety-related structures of the Millstone site...concludes that the aircraft accident probability would be less than 1.3E-7/year for a number of years since no increase in air traffic is projected in the vicinity of the site." The PSS, however, does not include any discussion of projected air traffic.

The PSS analysis of crash frequencies is judged to be conservative, based on their selection of conservative parameter values made in the screening evaluation for the numbers and types of flights considered. Although there is a brief discussion of the types of accident sequences that could be initiated by an on-site aircraft crash, no risk values were computed or presented in the PSS.

The most likely cause of an on-site crash identified in the evaluation is due to general aviation, with a frequency of 1.5E-6/year. The dominant contribution (1.2E-6/year) to this frequency comes from operations at the Groton Airport. Such an accident is considered to have the potential of initiating a loss-of-offsite-power accident sequence, but other (random) failures in the plant would be required to result in a core melt accident. In effect, the high predicted frequency of on-site crashes for these relatively lightweight aircraft is offset a lower conditional probability of core melt, given an accident initiated by this type of aircraft.

An on-site crash by a heavier commercial or military aircraft has the potential to initiate a greater variety of accident sequences, but these crashes have an order-of-magnitude smaller frequency of occurrence so that they are not significant contributors to core melt accidents.

The PSS analysis of on-site aircraft crashes concludes that such accidents do not contribute significantly to plant risk on the basis of their low frequencies and the low likelihood of such an accident resulting in a core melt. We agree that this conclusion is reasonable.

4.6.1 References for Section 4.6

4.6-1 U.S. Nuclear Regulatory Commission, "Standard Review Plan," USNRC Report NUREG-0800, Section 3.5.1.6, July 1981.

4.6-2 Northeast Utilities, "Final Safety Analysis Report, Millstone Unit 3," 1982.

4.7 Hazardous Materials

This section provides a review of the Millstone 3 PSS treatment of offsite and on-site incidents involving transportation and storage facilities for hazardous materials. Transportation facilities considered in the PSS were road, rail, and waterway traffic routes. Also considered were on-site storage facilities and nearby gas and oil pipelines. The conclusion of the PSS was that none of the sources of hazardous material would pose significant risk to the plant in terms of potential core melt initiation. This conclusion seems reasonable, based on the results of other PRA studies and the PRA Procedures Guide (Ref. 4.7-1). Nevertheless, the Millstone 3 PSS arrived at this conclusion using a limited and somewhat arbitrary analysis for screening potential risk contributors.

4.7.1 Identification and Screening of Hazardous Materials Initiators

The potential for core melt initiated by on-site or offsite sources of hazardous materials was assessed by considering road, rail, and water transport routes and on-site and offsite storage facilities and pipelines.

Highway routes proximate to the Millstone site reported in the PSS include Interstate 95, which passes within four miles; U.S. Highway 1, passing within three miles; and State Highway 156 within 1.5 miles. The PSS concludes that because of the distance between the plant and these routes, no accident involving explosions or toxic materials could impact the plant. The PSS makes no estimate of the frequency of accidents on these routes or of the amount of attenuation provided by atmospheric dispersion. Our own estimate reveals that under adverse conditions (F stability, 1 m/s wind velocity), the atmosphere would dilute a toxic substance released on any of these routes by at least a factor of 104 before the plume reached the plant.

On-site-transport of hazardous materials to Millstone is stated to involve truck-size quantities of hydrogen, sulfuric acid, and sodium hydroxide. Two of these materials (sulfuric acid and sodium hydroxide) are shipped to the plant every six weeks. The PSS concludes that on-site road transportation would not pose significant risk to the plant. No estimate of accident frequencies or consequences was made to support this conclusion.

The Millstone site is traversed by the Conrail/Amtrak rail system. Eighteen passenger trains and one freight train pass daily along tracks near the site. The PSS estimated the probability of rail shipment accidents and the consequent potential for missile generation, unconfined vapor cloud explosion, and control room uninhabitability. The aggregate frequency of such accidents is estimated to be 8.2E-7/year. Damage to safety-related structures as a result of railroad accident missiles is estimated to be no greater than 2.0E-8/year. The unconfined vapor cloud explosion is estimated to have a frequency of 8.4E-9/year. Control room habitability following a release of propane is determined to be a sub-lethal 19.3 g/m^3. However, the inflammability of this concentration within the control room is not discussed. Because of these low (and, judging from the use of two and three significant figures, highly accurate) estimated frequencies, railroad accidents are judged to be insignificant contributors to plant risk.

Water traffic on Long Island Sound in the vicinity of the site is stated to average 12 ships per day. It is stated that no oil barges pass within two miles of the site. No consideration is given to other hazardous material transportation on the sound. Consideration is given to possible damage of the service water pumphouse by runaway barges, but it is found that the service pumps would not be impaired by this event. Thus, it is concluded that waterway traffic does not contribute significantly to plant risk. Again, no quantitative estimates were made to support this conclusion.

Hydrogen and liquid chlorine are stated to be the only hazardous materials stored on-site in quantities greater than 100 pounds. The PSS, using information in the FSAR (Ref. 4.7-2), concludes that the hydrogen storage facility poses a negligible hazard. However, no quantitative estimate of explosion probability was made in support of this conclusion.

According to the PSS, chlorine is stored in two railroad tank cars approximately 1400 feet from the unit 3 control room air intakes. An analysis performed in the FSAR shows that the control room could be made uninhabitable if one of these tank cars were to rupture. To mitigate the consequences of this event, a chlorine detection system has been planned for unit 3. This system is described as providing warning and an automatic changeover to a closed-air recirculation system for the control room. The PSS states that because chlorine tank ruptures are rare and because of the mitigating features, the on-site storage of chlorine does not contribute significantly to plant risk. Again, no quantitative estimate of the frequency of hazard occurrence is used to support this conclusion. As a minimum, some estimate of both tank rupture frequency and the expected infiltration rate into the control room (during closed circulation mode) should have been provided. The NRC staff has found that large discrepancies exist between the leak-tightness of control ventilation systems as specified in designs and that measured in actual operating plants.[a]

It was reported in the PSS that no major gas transmission lines pass within five miles of the Millstone site, that the nearest gas distribution line is approximately three miles from the site, and there are no oil transmission or

[a] Personal Communication with Kazimieras Campe.

distribution lines located within five miles of the site. On the basis of this information, it is concluded that pipelines do not pose a credible risk to the plant and we concur.

4.7.2 Comments

In reviewing the treatment of hazardous materials as contributors to plant risk at Millstone 3, we applied three questions:

(1) Was consideration given to all potential sources?

(2) What screening criteria were used to identify important contributors?

(3) Were these screening criteria applied appropriately?

The answer to the first question is that the PSS did not make clear what procedure was used to ensure that all potential external events were considered and that all the significant ones were selected for detailed risk studies. In applying the second question, we found no well-defined screening criteria for eliminating insignificant contributors to risk. Yet all sources of hazardous material on and near the Millstone site were determined to be insignificant contributors to risk in the PSS. The only source for which a numerical estimate of potential risk was made was rail shipments of propane. In this case, the numerical estimate reveals that indeed the source is a small contribution. However, we are asked to accept the PSS judgment that all other sources are insignificant risk contributors. Finally, because the screening criteria were not explicitly stated, it was not possible to determine whether they were applied appropriately or consistently.

4.7.3 References for Section 4.7

4.7-1 U.S. Nuclear Regulatory Commission, "PRA Procedures Guide - A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants," USNRC Report NUREG/CR-2300, January 1983.

4.7-2 Northeast Utilities, "Final Safety Analysis Report, Millstone Nuclear Unit 3," 1982.

4.8 Turbine Missiles

The PSS analysis of the contribution to core melt probability from accidents that produce turbine missiles is presented in PSS Section 1.2.8. The material presented is essentially a summary of FSAR Sections 3.5.1.3, 3.5.2 and 3.5.3 (Ref. 4.8-1). The PSS and SAR state that the probability estimates were developed using the approach described by Bush (Ref. 4.8-2) in which the following expression is evaluated:

$$P4 = P1 \times P2 \times P3 \qquad (4\text{-}8)$$

where

P1 - frequency of missile generating turbine failures per year of turbine operation

P2 - conditional probability of a missile striking a critical structure or component, given missile generation

P3 - conditional probability of a missile causing significant damage, given that it strikes a critical structure or component.

Two mechanisms for turbine failure are considered: ductile fracture of rotating turbine parts under abnormal overspeed conditions and brittle fracture at or near operating speed caused by material defects or stress corrosion cracking. The source of the P1 probability used in the PSS calculations, however, is a memo report (Ref. 4.8-3) from the turbine vendor (GE) that does not consider stress corrosion cracking. The probability values are (only the 30-year numbers are presented in the report):

Condition or fracture type	Per 30-yr plant life	Per year
Brittle fracture (rated speed failure)	2.6E-7	8.7E-9
Ductile fracture (overspeed failure)	1.5E-7	5.0E-9
Total fracture	4.1E-7	1.4E-8

The probability of missile strike (P2) was calculated using a computer program which was not described.

The probability of the missile causing significant damage (P3) was evaluated using criteria from Bush (Ref. 4.8-2).

The overall results for P4 is a total probability of damage of 7.5E-9 for the 30-year life of the plant, or 2.5E-10/year, based on the total P1 probability of 4.1E-7/plant life provided by GE. This low probability does not account for recent NRC concerns with stress corrosion cracking.

The review identified two areas of concern in the PSS analysis. These are: (1) the effect of stress corrosion cracking on the P1 probability and (2) the assumption that one, and only one turbine wheel fractures during an incident.

The PSS acknowledges that the first concern exists and provides a "bounding" calculation for P4 using the P1 value of 1E-4 recommended in NRC Reg. Guide 1.115 which results in a turbine missile damage frequency of "only slightly above 1E-6/year," which the PSS judges to be acceptable due to the conservatism in the overall analysis. (The P4 value is 1.8E-6/year, based on the P2 and P3 numbers shown in the PSS.)

We note that the use of a P1 value of 1-E4/year produces a P4 value not in compliance with Reg. Guide 1.115, although this point is not important to this review. It is not clear, however, whether or not 1E-4/year is an appropriate P1 value to use in this analysis. Given the current state of the art in this area, and in the absence of better information regarding the value of P1, we would agree that the current PSS results for P4 are reasonable and acceptable.

The assumption that one, and only one turbine wheel fractures during an incident is considered realistic, although the PSS provides no discussion or justification for it.

The PSS analysis of turbine missiles concludes that they do not significantly contribute to overall plant risk on the basis of their low frequencies. We agree that this conclusion is reasonable.

4.8.1 References for Section 4.8

4.8-1 Northeast Utilities, "Final Safety Analysis Report, Millstone Unit 3," 1982.

4.8-2 S.H. Bush, "Probability of Damage to Nuclear Components Due to Turbine Failure," Nuclear Safety, Vol. 14, No. 3, May-June 1973.

4.8-3 General Electric Company, "Hypothetical Turbine Missiles - Probability of Occurrence," Memo Report, March 1973, cited in G.C.K. Yeh, "Probability and Containment of Turbine Missiles," Nuclear Engineering and Design, Vol. 37, 1976.

5. SUMMARY AND CONCLUSIONS

5.1 Dominant Sequences Corresponding to Each Plant Damage State

5.1.1 Internal Events

A simplified requantification was performed for the internal event sequences affected by the review's findings. The requantification process used and the results are presented in this section.

All of the suggested modifications to the internal events analysis that are described in Section 3 have been included in this simplified requantification. The results should be used with care, and due consideration given to potential shortcomings in these results arising from the necessarily simplified methods used to perform the requantification. The following assumptions and limitations are applicable and should be kept in mind when the results are examined.

- In general terms, the use of support state methodology significantly reduces the PRA's ability to identify subtle inter-system dependencies (see Section 3.10.2). The use of this methodology also affects the review process by effectively making it impossible to determine that all dependencies have been adequately treated. For this reason, it is not possible to provide assurance that no dependencies exist that could significantly affect the results of the requantification.

- The initiating event categories and frequencies used are the revised events and frequencies discussed in Section 3.1 and summarized in Table 3.1-1 under the column titled "Point est."

- Requantification is based on the revised event trees presented in Section 3.2. Event probabilities are generally taken from the PSS, except for system failure and human error events, and for the recirculation pump seal LOCA during station blackout (event S2 for support state 7) as described in Section 3.2.3.1.

- With two exceptions, the models and data used in the PSS to assess system failure probabilities and support state probabilities were evaluated as reasonable and used in the requantification.

  - The first exception is for LOSP in support states 6 and 7, where the data used in the PSS for diesel generators was evaluated as optimistic and discussed in Section 3.6. Using the revised diesel generator data, the support state failure probabilities changed from 0.014 to 0.04 for support state 6 and from 0.00018 to 0.002 for support state 7.

  - The second exception concerns a modeling deficiency involving the DC batteries, vital AC power supplies, and the emergency-generator load sequencers. The deficiency, which is particularly important during LOSP events, is discussed in Sections 3.4 and 3.10. The requantification did not treat this issue because the significant effort that would have been required is outside this review's scope. This is a limitation on the results of the requantification.

- The operator action failure probabilities used are the revised and appended values discussed in Section 3.5 and summarized in Table 3.5-1 in the column titled "Review assessment."

- The entire requantification effort was performed and checked by hand. No independent review of these results has been performed.

- In order to perform the requantification in a time frame and level of effort in keeping with the scope of the review, it was necessary to truncate the analysis at 1E-7/RY for any given sequence. Thus, no sequences of lower frequency are accounted for. This means two things: (1) plant damage state frequencies around 1E-7 have inherently greater uncertainty than those of higher frequency since truncated sequences could contribute significantly to them; (2) plant damage states which have no review estimate value given are not necessarily lower than 1E-7 - they simply do not have any sequences of 1E-7 or greater contributing to them. These limitations must be kept in mind when using the requantification results.

5.1.2 Requantification Results

The results of the requantification discussed above are presented in this section. It is very important to remember that these results should not be presented without reference to the assumptions and limitations discussed in Section 5.1.1. Table 5.1-1 presents the review requantification estimate for each plant damage state and compares it to the mean value from the MP 3 PSS. Table 5.1-2 presents the dominant sequences whose frequencies are at least 1E-7/RY for each plant damage state as determined by the requantification. The format of the sequence representation is the same as in the PSS. A legend to aid in interpreting the sequence representations is provided at the end of the table. The remainder of this section discusses the reasons for major differences between the PSS mean value and the review point estimate value in certain plant damage states.

5.1.2.1 Small LOCA with Early Core Melt

The principal reason for the increase in the frequency of these plant damage states (SEC, SE) is the transfer of long-term station blackout sequences with secondary cooling states from the equivalent plant damage states (TEC, TE). This is discussed in Section 3.2.3.1. Other changes made prior to this transfer also had an effect on these plant damage states. These two damage states and SEC' were affected by the reduction of the small LOCA frequency (see Section 3.1.2.8) and the inclusion of operator error OA-2-E (see Sections 3.2.1.1 and 3.5.1.4). The net effects of these two changes were insignificant, as they essentially offset one another. The re-evaluation of ATWS, which is discussed in detail in Section 3.2.2.5, resulted in increasing the frequency of damage state SEC by a factor of 3. Although many of the ATWS modifications had an effect, the increase is due primarily to the assumption that RCS pressure in excess of Service Level C results in core melt. This increase in SEC from ATWS is not important in the final results since its contribution is not significant compared to the contribution transferred from the long-term station blackout sequences.

Table 5.1-1 Plant damage state frequencies for internal events (per reactor-year).

Name	Description	PSS mean	Review estimate[a]
AEC	Large LOCA, early melt	1.92E-06	8E-7
AEC'	Large LOCA, early melt, failure of recirculation spray	4.17E-09	--
AE	Large LOCA, early melt, no containment cooling	2.68E-09	--
ALC	Large LOCA, late melt	5.44E-06	2E-6
ALC'	Large LOCA, late melt, failure of recirculation spray	4.88E-07	1E-7
ALC"	Large LOCA, late melt, failure of quench spray	3.42E-09	--
AL	Large LOCA, late melt, no containment cooling	3.36E-10	--
SEC	Small LOCA, early melt	1.12E-06	2E-5
SEC'	Small LOCA, early melt, failure of recirculation spray	2.76E-09	--
SE	Small LOCA, early melt, no containment cooling	1.17E-07	6E-6
S'EC	Incore instrument tube LOCA, early melt	--	4E-7
S'E	Incore instrument tube LOCA, early melt, no cont. cooling	1.83E-09	--
SLC	Small LOCA, late melt	9.81E-06	3E-5
SLC'	Small LOCA, late melt, failure of recirculation spray	4.79E-07	1E-6
SLC"	Small LOCA, late melt, failure of quench spray	5.77E-08	--
SL	Small LOCA, late melt, no containment cooling	2.73E-09	--
S'L	Incore instrument tube LOCA, late melt	3.35E-10	1E-7
TEC	Transient, early melt	1.81E-05	3E-5
TEC'	Transient, early melt, failure of recirculation spray	3.46E-07	8E-7
TE	Transient, early melt, no containment cooling	5.31E-06	2E-6
TLC	Transient, late melt	--	2E-6
V2EC	Steam generator tube rupture, steam leak, early melt	1.11E-07	2E-6
V2EC'	SGTR, steam leak, early melt, failure of recirc. spray	1.03E-09	1E-7
V2E	SGTR, steam leak, early melt, no containment cooling	1.29E-08	--
V2LC	SGTR, steam leak, late melt	2.76E-09	--
V2LC'	SGTR, steam leak, late melt, failure of recirc. spray	1.49E-10	--
V2LC"	SGTR, steam leak, late melt, failure of quench spray	1.77E-11	--
V2L	SGTR, steam leak, late melt, no containment cooling	8.40E-13	--
V	Interfacing systems LOCA	1.90E-06	8E-7
	Total[b]	4.53E-05	1E-4

[a] The review estimates provided are estimates based on a number of simplifying assumptions and subject to a number of limitations discussed in Section 5.1.1. The reader is cautioned to keep these assumptions and limitations in mind when considering the various potential implications of these results.

[b] It is important to note that the increase in the plant damage state frequency does not necessarily immediately imply a corresponding increase in overall public risk.

Table 5.1-2 Dominant sequences by plant damage state (all values per reactor-year).

Plant damage state		Dominant sequences	
Name	Frequency	Name	Frequency
AEC	8E-7	E2(1)/ACC	6E-7
		E1(1)/ACC	2E-7
ALC	2E-6	E2(1)/R2	2E-6
		E1(1)/R1	4E-7
ALC'	1E-7	E2(1)/R2/R3	1E-7
SEC	2E-5	E14(7)/E60/E120	2E-5
		E3(1)/OA2E	1E-6
		E7(1)/RPS(M)/TT/PL	7E-7
		E7(1)/RPS(M)/PL	7E-7
		E7(1)/RPS(M)/TT/PR/OA8R	2E-7
		E8(1)/RPS(M)/TT/PL	2E-7
		E8(1)/RPS(M)/PL	2E-7
		E14(7)/E60/0A7'	2E-7
		E3(1)/OA6E	1E-7
		E14(7)/S2/OA7'	1E-7
SE	6E-6	E14(7)/E60/E120/QS'	6E-6
S'EC	4E-7	E15(1)/OA2E	4E-7
SLC	3E-5	E3(1)/R2	7E-6
		E3(2)/R2	5E-6
		E15(1)/R2	3E-6
		E20(2)/AF1/R2	3E-6
		E21(2)/AF1/R2	3E-6
		E7(2)/PCS/AF1/R2	1E-6
		E8(1)/AF1/R2	1E-6
		E17(2)/AF1/R2	7E-7
		E5(2)/AF2/R2	5E-7
		E7(1)/PCS/AF1/R2	4E-7
		E8(2)/AF1/R2	3E-7
		E4(2)/AF2/R2	2E-7
		E14(7)/E60/S2/R2	1E-7
		E5(1)/AF2/R2	1E-7
SLC'	1E-6	E3(1)/R2/R3	5E-7
		E3(2)/R2/R3	2E-7
		E15(1)/R2/R3	2E-7

Table 5.1-2 (Continued).

Plant damage state		Dominant sequences	
Name	Frequency	Name	Frequency
		E20(2)/AF1/R2/R3	1E-7
		E21(2)/AF1/R2/R3	1E-7
S'L	1E-7	E15(1)/QS/OA9	1E-7
TEC	3E-5	E18(2)/AF1/OA7	2E-5
		E8(1)/AF1/OA7	5E-6
		E7(1)/PCS/AF1/OA7	2E-6
		E20(2)/AF1/OA7	1E-6
		E21(2)/AF1/OA7	1E-6
		E14(7)/AF1/E60/E120	1E-6
		E14(7)/AF1/E60	8E-7
		E14(6)/AF1/OA7	8E-7
		E5(1)/AF2/OA3	6E-7
		E7(2)/PCS/AF1/OA7	5E-7
		E17(2)/AF1/OA7	4E-7
		E4(1)/AF2/OA3	3E-7
		E5(2)/AF2/OA3	2E-7
		E8(2)/AF1/OA7	2E-7
		E4(2)/AF1/OA3	1E-7
		E13(1)/AF1/OA3	1E-7
TEC'	8E-7	E18(2)/AF1/OA7/R3	8E-7
TE	2E-6	E20(4)/AF1/OA7/QS	8E-7
		E18(4)/AF1/OA7/QS	4E-7
		E14(7)/AF1/E60/E120/QS'	3E-7
		E18(2)/AE1/OA7/QS	2E-7
TLC	2E-6	E4(1)/OA10	2E-6
V2EC	2E-6	E4(1)/OA6E	2E-6
V2EC'	1E-7	E4(1)/OA6E/R3	1E-7
V	8E-7	E16	8E-7

Table 5.1-2 Legend

Initiating events

E1	Large LOCA
E2	Medium LOCA
E3	Small LOCA
E4	Steam generator tube rupture
E5	Steamline break inside containment
E7	Power conversion system available
E8	Loss of power conversion system
E13	Spurious safety injection
E14	Loss of offsite power
E15	Incore instrument tube rupture
E16	Interfacing systems LOCA
E17	Loss of a single service water train
E18	Loss of a single vital DC bus
E20	Loss of vital AC bus 120-VAC-1 or 120-VAC-2
E21	Loss of vital AC bus 120-VAC-3 or 120-VAC-4

Support states

(1)	All support systems available
(2)	One support train unavailable
(4)	All ESF signals unavailable
(6)	LOSP, one support train unavailable
(7)	LOSP, both support trains unavailable

Dominant sequences by plant damage state

Events

ACC	Failure of accumulators
AF1	Failure of auxiliary feedwater
AF2	Failure of auxiliary feedwater (SGTR and steamline breaks)
E60	Failure to restore offsite power in 1/2 to 1 hour
E120	Failure to restore offsite power in 1 to 2 hours
OA2E	Operator overthrottles HPI resulting in inadequate flow
OA3	Operator fails to establish primary bleed

Table 5.1-2 Legend (Continued).

OA6E	Operator erroneously terminates high pressure injection
OA7(OA7')	Operator fails to establish primary bleed and feed
OA8R	Operator fails to establish HPI during ATWS consequential LOCA
OA9	Operator fails to delay recirculation when sump empty
OA10	Operator fails to control HPI during SGTR
PCS	Failure of power conversion system
PL	ATWS pressure spike exceeds Service Level C (unfavorable MTC)
PR	Consequential LOCA due to moderate ATWS pressure spike
QS	Failure of quench spray
QS'	Failure to recover quench spray - failure to restore offsite power in 2 to 8 hours
RPS(M)	Failure to scram - mechanical failure of RPS
R1	Failure of low pressure recirculation
R2	Failure of high pressure recirculation
R3	Failure of containment spray recirculation
S2	Consequential small LOCA
TT	ATWS turbine trip fails

5.1.2.2 Incore Instrument Tube Rupture with Early Core Melt

The principal reason for the increase in the frequency of this plant damage state (S'EC) is our inclusion of the procedural error OA-2-E. This error, which was not considered in the PSS, accounts for the operator overthrottling the high pressure injection system when attempting to take control of it during these sequences. Our evaluation is discussed in detail in Sections 3.2.1.1 and 3.5.1.4.

5.1.2.3 Small LOCA with Late Core Melt

The principal reason for the increase in the frequency of these plant damage states (SLC, SLC', S'L) is our rejection of the PSS assumption that it is possible to avoid the need for recirculation by conserving RWST inventory for these events. A detailed discussion of this subject is contained in Section 3.2.1.6 of this report. Adding the need for recirculation to these events created a new set of core melt sequences, and the PSS recirculation failure probability was high enough to raise the frequency of these damage states.

5.1.2.4 Transients with Early Core Melt

The principal reason for the frequency of these plant damage states (TEC, TE) either remaining approximately the same or decreasing is the transfer of some of the long-term station blackout sequences, which would have been dominant contributors, to the small LOCA plant damage states (SEC, SE) as described in Section 5.1.2.1 and discussed in Section 3.2.3.1. It is important to note, however, that the frequency of the sequences which were transferred to other plant damage states, and the frequency of the loss of offsite power sequences which remain in the TEC and TE plant damage states, increased due to our reanalysis. The remainder of this section discusses the reasons for the increase, and thus also applies to plant damage states SEC and SE. It should also be noted that the large increase in the frequency of loss of a DC bus had a significant effect on the TEC and TE damage states.

There are two principal reasons for the increase in the frequency of the long-term station blackout sequences. The first is the increase in the support states 6 and 7 probabilities discussed in Sections 5.1.1 and 3.6. The second is the change in recirculation pump seal failure probability discussed in Section 3.2.3.1. These items, in combination, contribute most of the increase in frequency of these sequences. It is important to note that the modeling deficiency concerning loss of offsite power discussed in Section 5.1.1 might have caused a greater increase in the frequency of these sequences if it could have been treated in the review. It is also worth noting that the use of unmodified EPRI recovery factors for loss of offsite power (rather than the PSS modified values), with the assumption that RCP seal LOCA occurs at 30 minutes, would have resulted in additional increases in the frequency of three of the four plant damage states affected by these sequences. Damage state SEC would have increased by an additional 25%, which would not have affected our results; damage state TE would have increased by an additional factor of 2, to 4E-6; and damage state SE would have increased by an additional factor of 3, to 2E-5.

5.1.2.5 Transients with Late Core Melt

The principal reason for the increase in the frequency of this plant damage state (TLC) is inclusion of operator action OA-10 for steam generator tube rupture events. This action represents a requirement that the operator must act to reduce primary system pressure by controlling HPI flow for steam generator tube rupture events where both auxiliary feedwater and high pressure injection are functioning. This requirement, which was not considered in the PSS, is evaluated and discussed in detail in Section 3.2.2.2.

5.1.2.6 Steam Generator Tube Rupture with Steam Leak and Early Core Melt

The principal reason for the increase in frequency of these plant damage states (V2EC, V2EC') is inclusion of operator action OA-6-E. This error, which was not considered in the PSS, accounts for the operator misdiagnosing the plant conditions and terminating high pressure injection when it should not be terminated. The error is evaluated and discussed in detail in Sections 3.2.1.1 and 3.5.1.5.

5.1.2.7 Interfacing Systems LOCA

The principal reason for the decrease in the frequency of this plant damage state (V) is requantification of the initiator frequency, which is evaluated and discussed in detail in Section 3.1.2.7. This re-analysis does not include the considerations discussed in Section 3.9, which would reduce interfacing systems LOCA probability even further.

5.1.3 External Events

The external event analysis presented in the PSS was not as detailed as the internal event analysis. Although, in general terms, the range of external event types considered is reasonable and consistent, detailed evaluations were performed only for earthquakes and fires. All other external events were dismissed on the basis of screening evaluations performed in a cursory manner.

The seismic evaluation presented in the PSS was substantially revised by Amendment 2 to the PSS. Both the seismic hazard and seismic fragility assessments were extensively revised. The original core melt frequency due to seismic events of 9.4E-5 per reactor year (RY) was the dominant contributor to core melt events from all causes. The seismic core damage frequency in PSS Amendment 2 of 1.7E-5/RY is still a significant contributor to total core damage frequency. The revised evaluation utilized extensively modified hazard and fragility curves. LLNL reviewed only the revised fragility evaluation.

A further revision in PSS Amendment 3, dated November 1984, is purported to correct mathematical errors in the Amendment 2 analysis. This resulted in an insignificant reduction in the Amendment 2 seismic core melt frequency to 9.1E-6/RY. Amendment 3 has not been reviewed by LLNL.

Fire events were estimated to contribute 4.8E-6/RY, or about 5% of the total core melt probability in the PSS. A simplified requantification, based on a sensitivity analysis, resulted in an increase by a factor of about 6 to 2.8E-5/RY in this contribution.

The remaining external events considered were evaluated as insignificant in the PSS. Our review agreed with this finding for extreme winds, aircraft accidents, and turbine missiles, but there are significant disagreements for the other external events, as outlined below.

- An uncertainty assessment was not performed for external flooding. The margin of safety above design flood elevations is very small.
- The estimated frequency of core melt due to internal flooding is too large to dismiss on the basis of a screening analysis.
- The evaluation of hazardous materials as an insignificant contributor to core melt frequency lacked justification in several areas, e.g., on-site chlorine storage and on-site transportation of various toxic materials.

5.2 Treatment of Uncertainties

This section reviews the quantification and propagation of uncertainties in the Millstone 3 PSS. Consideration is given to the methods used to identify, quantify and propagate uncertainties. The PRA procedures guide (Ref. 5.2-1) states that:

> Uncertainty analysis is an integral part of a risk assessment regardless of scope. There are uncertainties in every step of a PRA, and some of them may be large. Whether qualitative or quantitative in nature, the analysis considers uncertainties in the data base, uncertainties arising from assumptions in modeling, and the completeness of the analysis. To the extent possible, these uncertainties are propagated through the analysis. Where this is impractical, a sensitivity analysis provides insight into the possible range of results.

Ideally, the treatment of uncertainty in a PRA should include three elements: (1) random variability in component performance data, (2) inaccuracies in the models used to assess system performance, and (3) failure to include all the important sequences (completeness). The uncertainty contributed by random variability consists of plant-to-plant variations and the random distribution of component failure data. Uncertainty contributed by model errors results from the aggregation of entities and processes into state variables and functions, and the exclusion of other entities and processes - procedures that inevitably undercut the accuracy of a model. Completeness uncertainties are related to the inability of the analyst to fully evaluate all contributions to risk. The Millstone PSS addressed all three elements of uncertainty. However, the attention given to completeness was quite limited when compared to the treatment of parameter and modeling errors.

The PRA procedures guide suggests that each type of uncertainty (i.e., parameter, modeling and completeness) can be characterized either qualitatively or quantitatively. The extent to which uncertainty is quantified defines four levels of uncertainty analysis. The first level consists of a qualitative treatment of all three uncertainty elements. The Limerick PRA (Ref. 5.2-2) provides an example of this level of analysis. The second level is characterized by a quantitative treatment of data uncertainty and a qualitative treatment of modeling and completeness uncertainties as was done in the German Risk Study (Ref. 5.2-3). The third level involves quantitative treatment of data and modeling uncertainty with qualitative treatment of completeness errors. The fourth level includes a quantitative treatment of all three uncertainty types. This type of uncertainty analysis was used in the Zion study. The Millstone 3 PSS can be characterized as providing quantitative treatment of parameter and modeling uncertainty with limited qualitative treatment of completeness uncertainties. The Millstone 3 PSS treated uncertainties for both internally and externally initiated events. In general, the treatment of uncertainties for internally initiated events involved more detail and rigor than that for externally initiated events. To some extent, this is because much of the uncertainty in the internal events results from random variability in failure. Propagating these variations through fault and event trees is a straightforward process. In contrast, much of the uncertainty in the external events analysis results from uncertainties in the models and questions of completeness. The uncertainty analysis in the PSS is encumbered by the limited consideration given to questions of completeness in the external events analysis.

5.2.1 Treatment of Uncertainties for Internal Events

The Millstone 3 PSS treats uncertainties in the estimates of risks contributed by internal events using a combination of what the authors call the method of moments[a] and discrete probability distribution (DPD) arithmetic. The PSS identifies and propagates uncertainties in the core melt frequency evaluation originating from the following sources:

(1) initiating event frequencies

(2) system unavailabilities

(3) frequency of core melt

Table 5.2-1 provides a summary of each source of uncertainty and how it was treated in the PSS. Discussion of these sources of uncertainties and comments about their treatment is provided in the following paragraphs. The PSS also treats uncertainties in the analysis of containment failure, source term and public consequences. These uncertainties are not discussed here.

The frequencies of initiating events at Millstone 3 were described by the mean and variance of an assumed log normal distribution. The frequency of common transients was obtained using classical estimation methods. In these cases, the initiating event frequency was treated as a random variable, whose distribution reflects inherent plant-to-plant variability. The distribution parameters for these events were obtained by matching the moments of the population data to the moments of a lognormal distribution. For those events which have not occurred, a Bayesian approach was used. A distribution was established to represent the prior state of knowledge about the frequency of a particular event. This distribution was then revised, via Baye's theorem, to reflect observed operating experience. The resulting distributions were fit to a lognormal distribution in order to obtain uncertainty parameters.

System unavailability (failure/demand) was calculated from the system fault trees using the WAMCUT computer code. The WAMCUT code uses the method of moments to propagate variance of individual components to an overall variance in system unavailability. The method of moments uses the moments of component distributions to determine the moments of the system distribution. Random component failures and the variance in these failures were obtained primarily from a proprietary Westinghouse data base.

Uncertainty in the frequency of core melt was obtained by propagating the variance of top event unavailabilities through the event trees using DPD arithmetic. The top event unavailabilities or system unavailabilities for each event tree were quantified using system fault trees. Each top event mean

[a] The procedure described in the PSS as the method of moments is simply elementary probability theory of functions of random variables.

Table 5.2-1 Sources of uncertainty and their treatment in the Millstone 3 PSS.

Source of uncertainty	Type of uncertainty	Treatment
Initiating event frequencies	Data/model	Calculated variance
System unavailabilities	Model	Method of moments
Frequency of core melt	Model	DPD arithmetic

unavailability has an associated variance. The top event unavailabilities are multiplied through the event trees to obtain the probability of each event tree sequence for each support state. The resulting damage state probabilities were then multiplied by the corresponding support state probability. Uncertainty in the damage state frequency (i.e., core melt) was obtained by propagating top event variances through the event trees using DPD arithmetic.

5.2.2 Treatment of Uncertainties for External Events

The Millstone 3 PSS reviewed earthquakes, fires, external flooding, internal flooding, extreme winds, aircraft accidents, hazardous materials, and turbine missiles as external initiators that could contribute significantly to plant risk. The PSS found only fires and seismic events to be important to risk. The selection of these two external events for detailed analysis was based on a preliminary screening of all external events. This screening used estimates of frequency and consequences as a basis for excluding external events that were not considered to be significant risk contributors. Since fires and earthquakes were the only events selected for detailed analysis, these were the only events for which the uncertainty in the analysis was treated. Thus, there was no formal treatment in the PSS of the uncertainty associated with risks contributed by external flooding, internal flooding, extreme winds, aircraft accidents, hazardous materials, and turbine missiles.

The treatment of uncertainties in the analysis of earthquakes and fires was quite limited in scope relative to the internal events analysis. In both cases the uncertainty analysis was limited to dominant accident sequences of the plant logic models which were simplified versions of the plant logic models used for the internally-initiated events analysis.

5.2.3 Comment on the Treatment of Uncertainties

The task of identifying, quantifying, and propagating uncertainty in a PRA can be both amorphous and formidable. There is not yet an established literature on this subject. For this reason, the Millstone 3 PSS should be commended for dealing with the difficult task of quantifying uncertainties. However, it should also be recognized that several aspects of the uncertainty analysis in the PSS were incomplete or questionable. The propagation of random variability through fault and event trees is consistent with the state of the art. Uncertainty arising from modeling assumptions was treated using DPD arithmetic. Little effort was made to treat uncertainty arising from the completeness of the analysis. In addition, the PSS did not attempt to quantify uncertainties contributed by initiating events that were excluded from further analysis by a screening calculation. This is a consistent problem in the external events analysis. As an example, because a rough point estimate of the risk contributed by some external events (i.e, internal flooding, external flooding, hazardous materials) indicated that their risk was low, they received no detailed analysis. Thus, no uncertainty analysis was performed for these initiators. However, these events might become important contributors to risk when uncertainties about frequency of occurrence and propagation sequences are considered. A more complete treatment of uncertainties would include additional work on the contribution to risk of these excluded events. In particular, the analysis performed for internal flooding was of such a limited nature, with a relatively large point estimate and potentially large uncertainty, that a more detailed analysis of internal flooding would be desirable.

5.2.4 References for Section 5.2

5.2-1 U.S. Nuclear Regulatory Commission, "PRA Procedures Guide - A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants," USNRC Report NUREG/CR-2300, January 1983.

5.2-2 Philadelphia Electric Company, "Probabilistic Risk Assessment, Limerick Generating Station," U.S. Nuclear Regulatory Commission Docket Numbers 50-352, 50-353, 1981.

5.2-3 Electric Power Research Institute, "German Risk Study - Main Report: A Study of the Risk Due to Accidents in Nuclear Power Plants," English Translation, EPRI Report NP-1804-SR, 1981.

5.3 Insights

The insights gained from the review and requantification of the MP 3 PSS are separately described for internal and external events in the following sections. Since the requantification effort covered only internal events, the insights described for external events, particularly for seismic initiators, are necessarily more limited in their overall usefulness. They nevertheless provide a relatively concise description of general observations about the PSS made in the course of the review.

5.3.1 Internal Event Insights

The description of internal event insights is divided into two sections: one to describe overall sensitivity perspectives and a second to provide concise descriptions of specific insights.

5.3.1.1 General Sensitivity Perspectives

Valuable insights into the important and unimportant "elements" of a nuclear power plant can be obtained by a relative evaluation of pertinent PRA results in a broad perspective which considers the objectives and intended use of the study. This type of evaluation can identify the elements that are driving the results as well as those that have insignificant influence, so that it can assist in focussing a PRA review on those elements with significant influence on risk. This section describes the sensitivity perspectives obtained for internal events by employing this method early in the review on the information presented in the PSS.

First, a review of the objectives and intended use of the PSS. The primary objectives of the PSS are to (Ref. 5.3-1):

(1) characterize public risk from MP 3 from internal and external events

(2) compare risks from internal events to those predicted by the reactor safety study

(3) develop tools to support management decisions for improving safety

The first objective implies that the emphasis in the study (and the review) should be more on public risk assessment and less on core melt probability. As is the case in most PRAs, the dominant core melt sequences in the PSS are not the same sequences which contribute to risk, although some interesting overlap exists.

The second and third objectives are not particularly germane to the technical details of the study. The second objective is merely a comparison which is provided in PSS Volume 1. The last objective implies that the review should assure that the study be accurate on a <u>relative</u> basis. In other words, it should not contain discrepancies or outliers which would inspire management decisions that are ineffective (or worse, detrimental) with respect to improving plant safety.

The PSS results contained in PSS Volume 1 describe the dominant accident sequences in terms of three indices: core melt frequency, early fatalities (>100), and late fatalities (>1000). These internal event results are presented in PSS Table V-1. The following paragraphs present our perspectives on the core melt frequency results in the PSS. The scope of our review did not include the other risk indices.

<u>Core Melt Frequency (CMF)</u>

A somewhat unusual result (compared to other PRAs) in the PSS with respect to the dominant core melt accident sequences is that a relatively large number of sequences contribute to the core melt frequency, with the largest contributor being only 8.5% of the total (sequence 1, PSS Table V-1). This result, singularly, does not imply or suggest that the PSS is flawed. However, it provides a basis for several interesting implications and it also tends to make determinations of the significance of changes or errors more complicated and uncertain than would be the case if only a few sequences were dominant.

A large number of small contributors to a total immediately suggests two conclusions: (1) the value of any single contributor would have to be increased by a large amount to have a significant influence on the total, and (2) the elimination of (or a significant reduction in the value of) any single contributor has essentially no impact. To quantitatively illustrate the first point, the frequency of the largest contributor in the PSS to core melt frequency would have to be increased by a factor of 13 to cause a (very modest) factor of 2 increase in total CMF. Conversely, if the most dominant contributor were eliminated, the total CMF would retain over 90% of its previous value. These results further imply that any new sequence (overlooked in the PSS) which might be derived from the review must have a frequency over ten times greater than the largest existing sequence to approach a factor of 2 increase in CMF.

In view of these circumstances, it is helpful to examine the elements (initiating events, system failures, and unavailabilities) which make up the dominant sequences in order to determine if a method could be devised to ascertain their individual risk significance. **Table 5.3-1** is the first step in this process. The table shows all elements which appear in the 10 sequences which dominate (all greater than 3%) the core melt frequency. The first row shows the accident sequence number (corresponding to the rank with respect to core melt from PSS Table V-1). The second row gives the percent contribution to the total CMF represented by each sequence. The remaining 20 rows list all elements that appear in the 10 sequences. The first 10 elements (rows) are initiating events, while the second 10 are consequential failures and system failures. From this matrix, some qualitative perspectives begin to emerge with respect to the risk dominant elements in the 10 sequences. For example, high pressure recirculation (ECCS) failure appears in four sequences, as does auxiliary feedwater failure. Diesel generator failures appear only once.

In order to quantify the relative CMF significance of each **Table 5.3-1** element, **Table 5.3-2** was formulated. The 20 elements are listed in the first column, separated between initiating events and subsequent failures. The second column is a relative contribution percentage which is obtained by summing the percentage CMF contribution from the accident sequences in which the element appears. For example, loss of offsite power (LOSP) has a relative contribution of 7.2%, which is the sum of the overall contribution to CMF in Table 5.3.1 for accident sequences 5 (3.6%) and 8 (3.6%) in which LOSP appears.

The next step is to formulate a generalized relationship which equates the increase in CMF as a function of increase in the probability of an element. This is a trivial exercise which results in the following:

$$\Delta CMF_i = 1 + (F_i - 1)R \qquad (5\text{-}1)$$

where

ΔCMF_i = factor of increase in the total core melt frequency

F_i = factor of increase in the probability of the element under consideration

R = the fractional contribution (% ÷ 100) of each element determined by summing the fractional contribution of all sequences in which it appears.

Table 5.3-1 Matrix of elements from core melt frequency dominant accident sequences.

	Accident sequence no.	1	2	3	4	5	6	7	8	9	10
	Contribution to CMF (%)	8.5	4.9	4.4	4.4	4.2	3.6	3.6	3.4	3.1	3.0
Initiating Events	Large LOCA										X
	Medium LOCA	X									
	Small LOCA									X	
	Steamline break (inside)							X			
	Steamline break (outside)								X		
	Event V					X					
	DC bus (1 or 2)		X								
	AC bus (1 or 2)			X							
	AC bus (3 or 4)				X						
	LOSP						X	X			
System Failures	High pressure recirculation	X		X	X					X	
	Low pressure recirculation										X
	Auxiliary feedwater		X	X	X			X			
	Feed and bleed		X					X	X		
	Steamline isolation								X		
	ESF bus							X			
	Diesel generator						X				
	Quench spray						X				
	6-hr offsite AC recovery						X				
	Controlled P.S. depress.									X	

Table 5.3-2 Contribution to CMF from dominant accident sequence elements.

	Element	Relative contribution (%)	CMF increase factor from 10 x element increase
Initiating Events	Medium LOCA	8.5	1.76
	LOSP	7.2	1.65
	DC bus (1 or 2)	4.9	1.44
	AC bus (1 or 2)	4.4	1.40
	AC bus (3 or 4)	4.4	1.40
	V	4.2	1.38
	Steamline break (in)	3.6	1.32
	Steamline break (out)	3.4	1.31
	Small LOCA	3.1	1.28
	Large LOCA	3.0	1.27
System Failures	High pressure recirculation	20.4	2.83
	Auxiliary feedwater	17.3	2.56
	Feed and bleed	11.9	2.07
	ESF bus	3.6	1.32
	Quench spray	3.6	1.32
	6-hr recovery	3.6	1.32
	Diesels	3.6	1.32
	Steamline isolation	3.4	1.31
	Control P.S. depress.	3.1	1.28
	Low pressure recirculation	3.0	1.27

Conversely, the factor of reduction in CMF is obtained by:

$$\Delta CMF_r = 1 - R(1 + 1/F_r) \qquad (5\text{-}2)$$

where the subscript r denotes reduction factor.

An example serves to illustrate use of the formulas. For this example, it is assumed that the failure of both diesel generator units at Millstone 3 could be a factor or 10 higher than used in the PSS. To determine the sensitivity of CMF to this change, Eq. 5-1 is used, which yields:

$$\Delta CMF_i = 1 + (10 - 1)0.036 = 1.324. \qquad (5\text{-}3)$$

Thus, the new core melt frequency would be

$$(1.324)(4.5E\text{-}5) = 5.96E\text{-}5 \qquad (5\text{-}4)$$

This is a very small increase from which it can be tentatively concluded that CMF is not significantly influenced by increases in diesel generator failure.

The last column in Table 5.3-2 shows the increase in CMF for a factor of 10 increase in the probability of each of the elements. The elements are ranked in order of their influence on CMF for initiating events and system unavailability. It is of interest to note that three elements, high pressure recirculation, auxiliary feedwater, and feed and bleed have a more significant influence on CMF than the most dominant accident sequence (represented by medium LOCA at 8.5%).

Caution is necessary in applying the method. The probabilities of some of the system failures are dependent on the initiating event. In these cases, the system failure rate sensitivities to CMF need to be computed on an individual accident sequence basis with appropriate adjustments made to the frequency of each sequence. This can still be accomplished using Eq. 5-1 and inputting appropriate values for each accident sequence or group of sequences.

5.3.1.2 Specific Internal Event Insights

Specific insights gained from the internal event review and requantification are briefly described in the following paragraphs. The listing of necessity cannot be all-inclusive; only those which were judged to be significant are included. The reader should note that these insights apply to the new results generated by this review, whereas the general sensitivity perspectives contained in the preceding section apply to the original PSS results.

(1) Loss of offsite power contributes about one-third (33%) of the total core melt frequency, and it is the single largest identifiable contribution. Almost all of this contribution is due to extended station blackout (failure of all on-site AC with failure to recover offsite power within two hours, in time to prevent core melt), which results in reactor coolant pump seal LOCA with failure of all ECC systems.

In addition, these station blackout sequences contribute about 80% of the total frequency of key plant damage states (early melt with no containment cooling). Almost all of this contribution is due to the failure to recover offsite power extending past eight hours.

(2) Small LOCA contributes about 15% of the total core melt frequency. Almost all of this contribution is due to failure of high pressure recirculation following a small LOCA induced by a random pipe break.

(3) Plant damage state V (interfacing systems LOCA), the potentially most risk significant plant damage state by virtue of its exceedingly high consequences, contributes less than 1% to the total core melt frequency.

(4) The results are extremely uncertain where human actions are concerned. The plant lacks precise operating procedures because it is still too early in the plant's construction for the procedures to exist. Thus, it was necessary to use screening estimates of human error probability throughout the analysis, based on rough procedure guidelines. Those dominant sequences containing human errors should be requantified after procedures become available.

(5) Random (or spontaneous) small LOCAs caused by failure of reactor coolant pump seals, which have been shown to be large contributors to core melt frequency for other PWRs, are not a major contributor at this plant. The presence of loop stop (isolation) valves, which allows the operator to isolate these LOCAs, is responsible for this result.

(6) Approximately 35% of the total core melt frequency involves the failure of support systems either as an initiator or following initiators other than LOSP. Of the 20% which involve support system initiators other than LOSP, the contributions were split about 70-15-15% between (respectively) loss of a single vital DC bus, loss of 120V vital AC bus 1 or 2, and loss of 120V vital AC bus 3 or 4. Of the 15% which involve support system failure subsequent to an initiating event other than LOSP, the dominant contributor is failure of control logic (either loss of a single ESF cabinet or loss of a single EGLS cabinet).

(7) The results are subject to the limitation that the support state method used is highly dependent on the ability of the analysts to recognize any subtle interfaces or interactions within or between the systems, without the help of an integrated fault tree-event tree model. We found that it is extremely difficult, if not impossible, to verify that all of these subtleties have been properly treated (see Section 3.10.2).

(8) In general, the results are insensitive to the selection of means or medians for the presentation of the results, with the notable exception of event V. This stems from an unrealistic failure rate distribution for the disc rupture failure mode for valves, which was evaluated in the PSS by using the same techniques as for other components. This illustrates the importance of applying judgment in areas where the use of a standard technique yields an answer contradictory to common sense. These areas must be separately reviewed and evaluated to determine if the answer has an underlying valid and reasonable basis, or whether it is an artifact of an inappropriate application of a specific or general method.

5.3.2 External Event Insights

The insights obtained from the review of the external event analysis are described in the following paragraphs. Most of these insights are general and, therefore, of limited usefulness, since most of the external events did not receive detailed analysis in the PSS.

No significant insights are included for seismic events because a review and evaluation of major changes to the seismic hazard analysis and the overall effect of these changes was not performed by LLNL.

5.3.2.1 Earthquakes

Amendment 2 to the PSS provided a completely revised seismic event evaluation based on extensively revised hazard and fragility assessments. The revised core melt frequency is 1.7E-5/RY, a factor of 5.5 smaller than the original PSS value of 9.4E-5/RY. The new results are reported to be dominated by contributions from plant damage states TE (44.9%) and SE (42.5%).

5.3.2.2 Fires

Fire events in the PSS contributed 4.8E-6 (5%) to the total core melt frequency. Plant damage state TE was the single largest contributor, providing about 29% of the core melt frequency due to fire events. Fires in the control room, instrument rack room, and cable spreading room were the major contributors to plant damage state TE, with about 88% of the total TE frequency.

The contribution to TE from the control room, instrument rack room, and cable spreading room was increased by a factor of 20 in a simplified sensitivity analysis in this review to account for the combination of (1) a human error rate used in the PSS that is too low by a factor of about 200 and (2) an assumption concerning total loss of safety functions that is too high by a factor of about 10. This increased the core melt frequency due to fire by a factor of about six, increased the contribution from TE to about 88%, and increased the contribution to TE from the three rooms noted above to about 99%. Considered alone, i.e., without changes to the internal event analysis, etc., this increased frequency of fire events contributes about 17% to the total core melt frequency.

5.3.2.3 External Flooding

The margin of safety above the design elevation for tidal flooding resulting from the probable maximum hurricane (PMH) is less than one foot.

The margin of safety above the design elevation for flooding resulting from a probable maximum precipitation (PMP) event is less than one inch.

If uncertainty had been considered in the analysis, the coefficient of variation on water depth, which we would expect to be approximately 0.2 to 0.3 at the 100-year storm level, may change the conclusion that external flooding has a sufficiently low frequency of occurence to be dismissed as a significant contributor to the core melt frequency. This issue should be addressed in the PSS.

5.3.2.4 Internal Floods

The absence of a detailed analysis of important plant areas, particularly the cable spreading and switchgear rooms, is not justified. In addition, the absence of an uncertainty analysis in this evaluation is not justified, given an estimated frequency of internal flood-induced core melt of 8.7E-7/RY.

5.3.2.5 Extreme Winds

Structural failure or missile-induced damage from winds as severe as a 360 mph tornado are considered very unlikely and, therefore, insignificant contributors to core melt. The principal reasons for this finding are (1) a relatively low likelihood of high winds and (2) protection of safety-related equipment in safety-related structures having reinforced concrete walls and roofs at least two feet thick.

5.3.2.6 Aircraft Accidents

Aircraft accidents are considered insignificant contributors to core melt on the basis of their low frequencies.

The dominant contribution to on-site aircraft crashes is due to general aviation operations at the Groton-New London Airport, with a predicted frequency of 1.2E-6/RY. This accident could initiate a loss of offsite power event.

On-site crashes by heavier commercial or military aircraft have a predicted frequency of 1.2E-7/RY. Those accidents have the potential to initiate a larger variety of accidents because they could penetrate some safety-related structures.

5.3.2.7 Hazardous Materials

The control room could be made uninhabitable in the event of the rupture of either of the two railroad tank cars used for on-site storage of chlorine located approximately 1400 feet from the control room air intakes. A chlorine detection system has been planned to provide warning and automatic changeover to a closed air recirculation system for the control room.

5.3.2.8 Turbine Missiles

The turbine missile damage frequency calculated in the PSS using information supplied by GE for turbine failure was 2.5E-10/RY. This did not consider stress corrosion cracking of turbine wheels. A separate PSS calculation, using the turbine failure rate of 1E-4/RY recommended in NRC's Reg. Guide 1.115 results in the significantly higher turbine missile damage frequency of 1.8E-6/RY.

5.3.3 References for Section 5.3

5.3-1 Northeast Utilities, "Final Report of the Level 3 Review Board on the Millstone Unit 3 Probabilistic Safety Study," August 1983.

APPENDIX A

REVIEW OF THE ORIGINAL MILLSTONE UNIT 3 PROBABILISTIC SAFETY STUDY SEISMIC EVENT EVALUATION

Prepared by

Lawrence Livermore National Laboratory

Livermore, California

APPENDIX A.

A.1 Summary of results[a]

The methodology used in the PSS for the evaluation of seismic events is generally consistent with the state-of-the-art of commercial PRAs, except for the evaluation of fragility. The methodology used, however, is not found to be acceptable.

We have numerous disagreements with the methodology used to develop the hazard function(s). We find that the mean and median values of these functions are optimistic, and that the uncertainty is underestimated.

Numerous conceptual and logical errors in the fragility assessment led us to develop a lack of confidence in the adequacy of this analysis, in spite of many conservative assumptions that are evident - chiefly in the structural fragilities. Our concerns go further than these conservatisms, which were acknowledged in the PSS and with which we generally agree.

The PSS did not provide an adequate description of the methodology used to identify or estimate the probability of seismic initiating events. We believe that important initiating events may have been omitted from the PSS, e.g., steam generator tube rupture, and that the probabilities of those included may be optimistic.

The methodology used to condense the internal-initiated plant logic models to the seismic-initiated plant logic models was difficult to follow and unconvincing.

We have numerous points of disagreement with the calculational methodology used to assemble hazard, fragility and plant logic models:

(1) Correlation of seismic response was not included in the calculation of initiating event probabilities, which leads to optimistic estimates of these probabilities.

(2) Correlation of seismic response of components in the plant logic model was not included in the calculation, which leads to optimistic estimates of the core melt probabilities and radioactive releases.

(3) Correlation was not included in the uncertainty analysis, which leads to an optimistic estimate of uncertainty.

(4) The uncertainty analysis was performed only on the dominant seismic accident sequences that were based on simplified plant logic models from the internal-initiated analysis, so that both the results and the uncertainties are likely to be optimistic.

[a] The evaluation of seismic hazard and fragility contained in the PSS were subsequently redone by NU contractors. The review of the original hazard evaluation is described in this appendix; the revised evaluation was not included in the scope of the review. Both fragility evaluations were reviewed. The reports of these reviews are included here in Appendices B and C for the original and revised evaluations, respectively.

(5) The uncertainty calculation did not include the sampling error that results from the use of a five-element vector in the DPD arithmetic, so that the uncertainty results are optimistic.

(6) The methodology used in the dominance study included only random variability in the fragilities. It did not include the total variability; i.e., randomness plus uncertainty, thus making the results unconvincing.

(7) The results of the dominance study are seriously flawed by limitations in the state-of-the-art of fragility assessment. Uncertainties in fragilities make it difficult to conclude that the correct conclusions can be drawn from simple dominance studies.

A.2. Seismic Hazard Assessment

A.2.1 Introduction

The seismic hazard curves used in the Millstone PSS were developed in Appendix 1-B of the PSS report by Dames and Moore. For easy reference, this PSS appendix will be referred to as the "D&M report." The seismic hazard analysis presented in the D&M report contains a number of errors in the sense that the text does not appear to agree with the calculation. In addition, the D&M report does not contain sufficient information to allow an adequate evaluation of the results presented on their own merit. To overcome this difficulty, an independent seismic hazard analysis was performed for the Millstone site. It was possible to do this in a timely and cost-effective manner because Millstone was one of the sites examined in an earlier seismic hazard evaluation for SEP plant sites (Ref. A-1). Consequently, the input data needed to perform a seismic hazard analysis was available.

First, this section discussed the review of the D&M report and describes its major deficiencies. This is followed by a brief discussion of our independent hazard analysis for the Millstone site and the implications of this analysis for the PSS.

A.2.2 Seismic Hazard Model

The seismic hazard model used in the D&M report is the model described in Ref. A-2. The McGuire seismic hazard model is a typical seismic hazard analysis model and incorporates the usual assumptions. While some of the basic assumptions, e.g., that earthquakes occur in time around the site as a Poisson process, are questionable they are generally made in analyses of this type and sufficient data does not exist to allow the use of more realistic models.

In a probabilistic analysis, one of the most important and more difficult tasks is incorporating the uncertainty in our knowledge about the key input parameters of the model being used to assess the seismic hazard at a site. The major difference between the D&M report and the SEP study (Ref. A-3) lies in the treatment of uncertainty, i.e., how uncertainty bounds are obtained and how uncertainty entered into the analysis. In the SEP study, 10 experts were used to provide a range of input data. This resulted in 10 different overall earthquake occurrence models, including models very similar to those used in the D&M report. Examination of the data provided in Tera (Ref. A-4) and Bernreuter (Ref. A-3) shows that significant differences about all of the input parameters exist between the experts used in the SEP study. A new study (Ref. A-5) currently in progress at LLNL for NRC, while still in its preliminary stage, reconfirms the conclusion that there are significant differences between experts about the zonation and choice of seismicity parameters for the EUS.

The use of Eq. A-1 in the D&M report relating magnitude to intensity is not appropriate. The relation given,

$$M = 1 + 0.67\, I_o \qquad (A-1)$$

was derived for the Western U.S. (WUS) and the magnitude M is the local (California) magnitude defined by Richter. In the Eastern U.S. (EUS) bodywave m_b or one second L_g wave magnitude is generally used, and the relation

$$I_o = 2m_{bLg} - 3.5 \qquad (A-2)$$

developed by Nuttli is often used.

A.2.3 Seismic Source Zones

One major weakness of the D&M report is the limited number of zonations considered in the analysis. Only four sets of zones were considered. As noted in the previous section, there is a considerable difference of opinion as to how the EUS should be zoned. This is particularly true for New England. The geometry of the problem (i.e., the shape of the source zones) is a relatively unimportant parameter other than how it affects the choice of the seismicity parameters used for a given zone. The judgment of the adequacy of the zonation cannot be uncoupled from the assignment of seismicity parameters. The weights assigned seem a bit strange (0.2, 0.34, 0.23 and 0.23), and they are not justified in the report; but this is only a minor consideration, as they are nearly equally weighted.

A.2.4 Seismicity Parameters

Three parameters are required to define the earthquake recurrence model for each zone:

λ_o = number of earthquakes occurring larger than some minimum magnitude M_o.

b = slope of the relation logN = a - b(M or I)

M_u = largest earthquake that can occur in any given zone.

The hazard curve is relatively sensitive to changes in any of these parameters.

One of the important parameters is M_u. The text on page 5 of the D&M report suggests that M_u was taken as an MM Intensity of IX and a magnitude of 6.25. However, use of I_o = IX in Eq. A-1 would lead to a magnitude of 7.0. It would appear that a different relation was used to convert epicentral intensity into magnitude, but no explanation is provided.

Another problem is that the ground motion models used in the analysis are all in terms of magnitude. However the activity rates and the b parameter of Eq. A-2 are expressed in terms of intensity. It is not clear where and how the transformation to magnitude was made. A significant difference in the results can occur depending on when and/or where in the analysis the transformation is made.

No information is presented to allow an assessment of the activity rates presented in Table I of the D&M report. Our experience has shown us that estimating both the activity rate and the b parameters for any given zone is difficult because of differences in historical catalogs, and judgement as to how to correct for the incompleteness of the historical record.

Such factors can easily lead to differences of factors of 2 to 4 in the activity rates. Although not explicity stated, no uncertainty seems to have been assumed for the rate parameter in the analysis. This, in our view, is an unacceptable assumption.

A.2.5 Ground Motion Models

Only two ground motion models were used. The first model is attributed to Nuttli and Herrmann (Eq. 4.3 of the D&M report) and it appears to be in error. Because no Nuttli & Herrmann citation appears in the reference list, it is not possible to confirm this relative to the particular Nuttli & Herrmann ground motion model used. However, Nuttli consistently models the ground motion relation (Refs. A-6, A-7) in the form

$$A(R,f) = A_o(f)\ R^{-5/6} \exp(-\gamma R), \qquad \text{(A-3)}$$

which is consistent with accepted theoretical models. For the EUS this leads to values of γ on the order of 0.003. If Eq. 4-3 of the D&M report is converted to the form of Eq. A-3, the γ value would be 0.0074 - much higher (optimistic) than is generally accepted.

The text of the D&M report states that when R was less than 15 km, peak acceleration a_p was limited to a constant value equal to the smaller value obtained from D&M Eqs. 4-3 and 4-4. The problem with this is that for D&M Eq. 4-3, a_p scales as $\exp(1.15\ m_{bLg})$ and for D&M Eq. 4-4

$$a_p = \exp(.933\ m_{bLg}) \qquad \text{(A-4)}$$

Clearly, a major problem quickly arises in that a significant discontinuity would occur. Although the ground motion plot shown in Fig. 5 of the D&M report shows no such discontinuity, it is evident that the limiting R is much larger than 15 km. It is not clear what model was used and what the basis is for the model used. The D&M model, however, effectively reduces the seismic hazard computed for the Millstone site.

The other model used is the Campbell model. It is a reasonable model similar to the Nuttli & Herrmann model. However, neither the Nuttli-Herrmann model nor the Campbell model are directly based on EUS data. In fact, both were derived using the same set of semi-theoretical assumptions. We therefore find it surprising that none of the many other approaches to developing EUS ground motion models (Ref. A-1) were used. Fig. A-1 shows a comparison of the results from a wide variety of models that use various acceptable alternatives. By acceptable, we mean that the methodology/data used to arrive at the model is reasonable and (at least for the set of models compared in Fig. A-1) at least one member of a panel of experts in modeling of EUS ground motion deemed the model a possible alternative. See Ref. A-5 for further discussion. This figure, which shows peak ground acceleration versus epicentral distance for the magnitude values of 5 and 7, illustrates that there is considerable uncertainty in the ground motion modeling process and supports the point that the ±20% factor used in the D&M analysis is low. The models used in the D&M study are, in our opinion, two of the "better" EUS ground motion models. But as noted in Section A.3, one element of a probabilistic analysis is to ensure that the uncertainty has been bounded and included in the analysis. This has not been accomplished in the D&M selection of ground motion models.

There is also a question concerning the use of "sustained" acceleration as the appropriate measure of ground motion. We note that the study by Nuttli (Ref. A-6) which examined the concept of sustained acceleration, did not find that it improved the correlation between observed damage and the ground motion parameter used.

A.2.6 D&M Results

The final hazard curves used in the PSS analysis are based on 36 runs, 4 maps, 3 sets of $M_{u/b}$ values, and a variation of ±20% in the ground motion model. In our opinion, these 36 hazard curves do not adequately bound the uncertainty. Considerable variation should have been applied to the rate of earthquake occurrence in each zone, a much larger variation in the ground motion models should have been used, and additional zonations considered. In addition, there is some question about the "correctness" of the analysis, as it is not clear what equations were used.

The real problem does not lie in possible errors that have been made or in the particular choice of any one set of parameters of the hazard model. It is in the very limited set of models used. The results of the SEP study (Ref. A-1) show that there is a much larger uncertainty about the seismic hazard in New England than obtained by D&M. It is of some interest to note that the latest USGS study, Algermissen, et al. (Ref. A-8), would put the 2500-year return period peak ground acceleration at about 0.25g, or 0.2g sustained. Although this estimate of the hazard is at the upper bound of the D&M hazard curves shown in Fig. 1.2.1-1 of the PSS, it is in reasonable agreement with the results of the SEP study, as described below.

A.2.7 Comparison to the SEP Results

Because of the deficiencies of the D&M analysis outlined above, the median seismic hazard curve obtained from the D&M analysis is significantly lower than the seismic hazard estimate obtained in the USGS's most recent study. In order to evaluate these differences, it was necessary to perform a limited seismic hazard analysis for the Millstone site. We used the zonations and seismicity parameters provided by the SEP/EUS seismicity panel and a "correct" version of D&M's Eq. 3 for sustained acceleration:

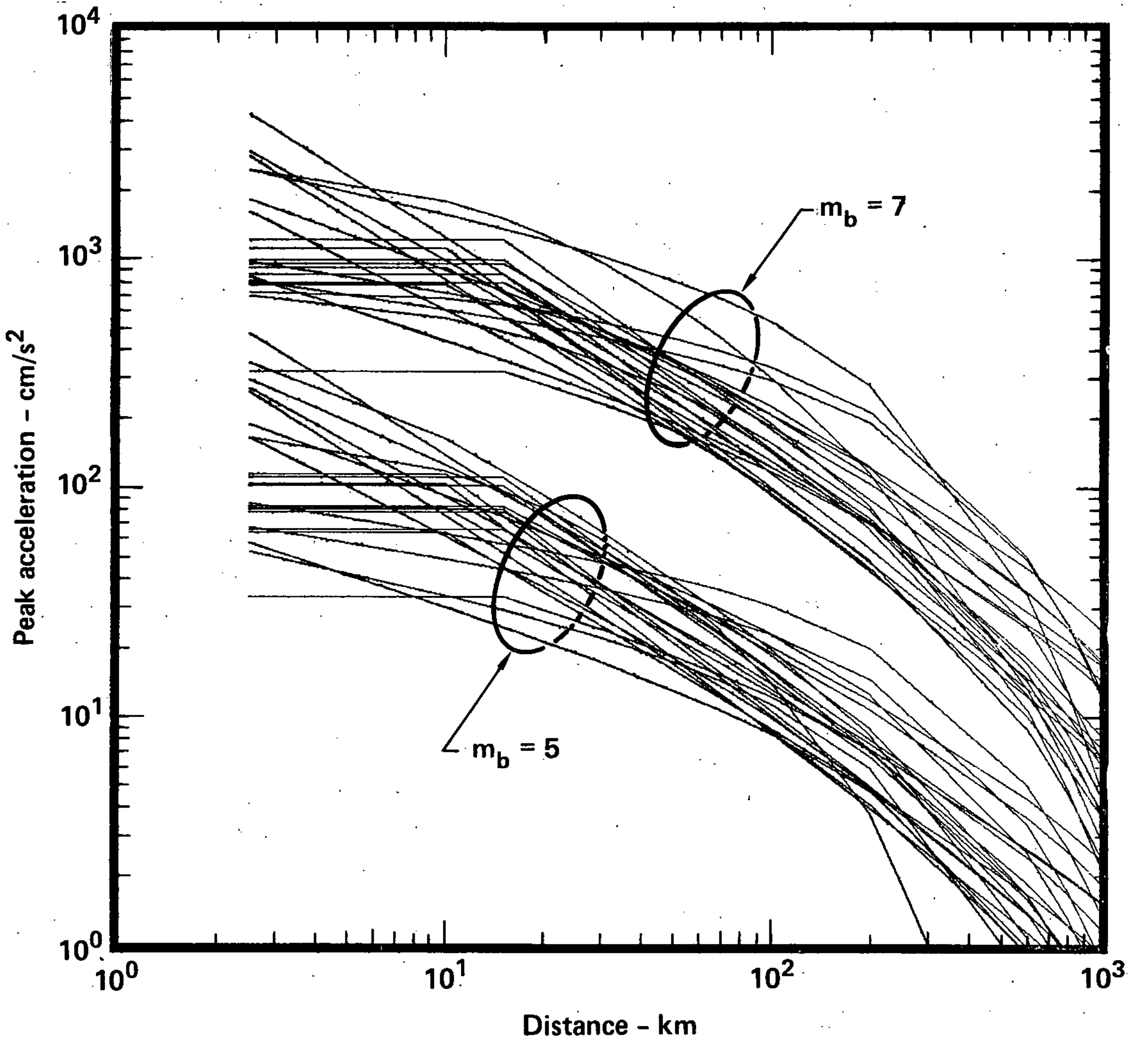


Fig. A-1 Possible ground motion models for the Eastern United States.

$$\ln a_s = 1.06 + 1.15\ m_b - 0.8333\ln R - 0.005R \quad R > 10 \text{ km} \tag{A-5}$$

and for R less than 10km

$$a_s(m_b,R) = a_s(m_b,10)$$

Some members of the SEP panel provided their models in terms of intensity. We replaced m_b with I_o in these models using the relation

$$I_o = 2\ m_b - 3.5 \tag{A-6}$$

Figure A-2 is a plot of the resulting hazard curves for all the SEP seismicity experts. This figure also shows two points for approximate "sustained" acceleration estimated from the maps in the USGS report by Algermissen, et al. It is seen that the USGS results are in reasonable agreement with the results obtained using the SEP seismicity experts' models. It must be noted that the USGS study used a significantly different ground motion model. It is difficult to assess exactly what hazard curve would be obtained from the USGS study if they had used the same ground motion model utilized in our study. It is most likely that the resulting hazard curve would be higher because no random uncertainty was used in the USGS model. In addition, (Ref. A-5), compares the preliminary results from a new panel of experts to the results obtained for the SEP study. The agreement between these two studies is excellent.

Figure A-3 shows the median curve from Fig. A-2 plotted on PSS Fig. 1.2.1-1. Also shown is the spread of our curves at 0.6g from Fig. A-2. It is seen from this figure that the D&M results are within the spread of the SEP results, but on the low side. It is not possible to determine exactly where the D&M median curve lies relative to the SEP and USGS results because the D&M curves are not equally weighted and the probabilities are not given on the various hazard curves. The D&M median appears to be about a factor of 5 low compared to the SEP median. A reasonably complete uncertainty analysis would spread out the scatter in the curves even more. However, this increase in uncertainty in the seismic hazard is considered unlikely to have much effect on the median curve. But it could have significant effect on the risk as it is generally found in such analyses that an increase in uncertainty increases the risk.

A.3 Seismic-Induced Initiating Events

The MP 3 PSS evaluated seismic-induced initiating events that were believed to be "credibly postulated to occur as a result of an earthquake within the acceleration range of interest (0.17g to 0.80g)." The set of these events is a subset of the two general classes of initiating events (LOCAs and transients) considered in the internal event analysis.

The events considered were of two types: those which occur as a result of seismic-induced failures of plant structures and equipment, i.e., large LOCA, small LOCA and ATWS; and transients induced by the seismic event as a result of ground motion or failure of nonseismically-qualified systems. These latter transients were modeled as a single "limiting" transient, which was assumed to occur if none of the other initiators occurred.

Initiators excluded from the analysis included SGTR, steamline break, and interfacing system LOCA, on the basis of high-seismic capacities associated

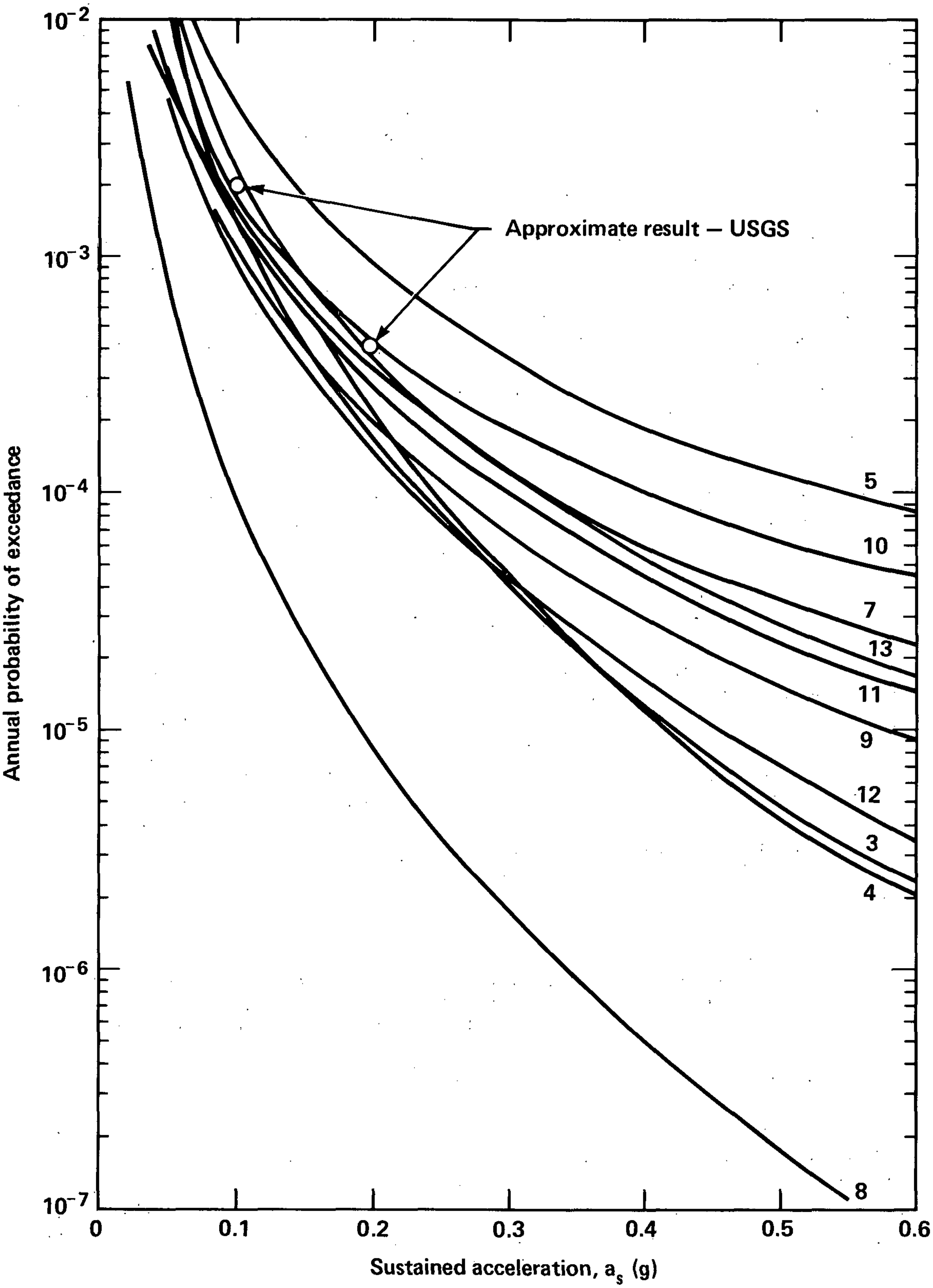


Fig. A-2 SEP experts sustained acceleration results based on "corrected" D&M ground motion model.

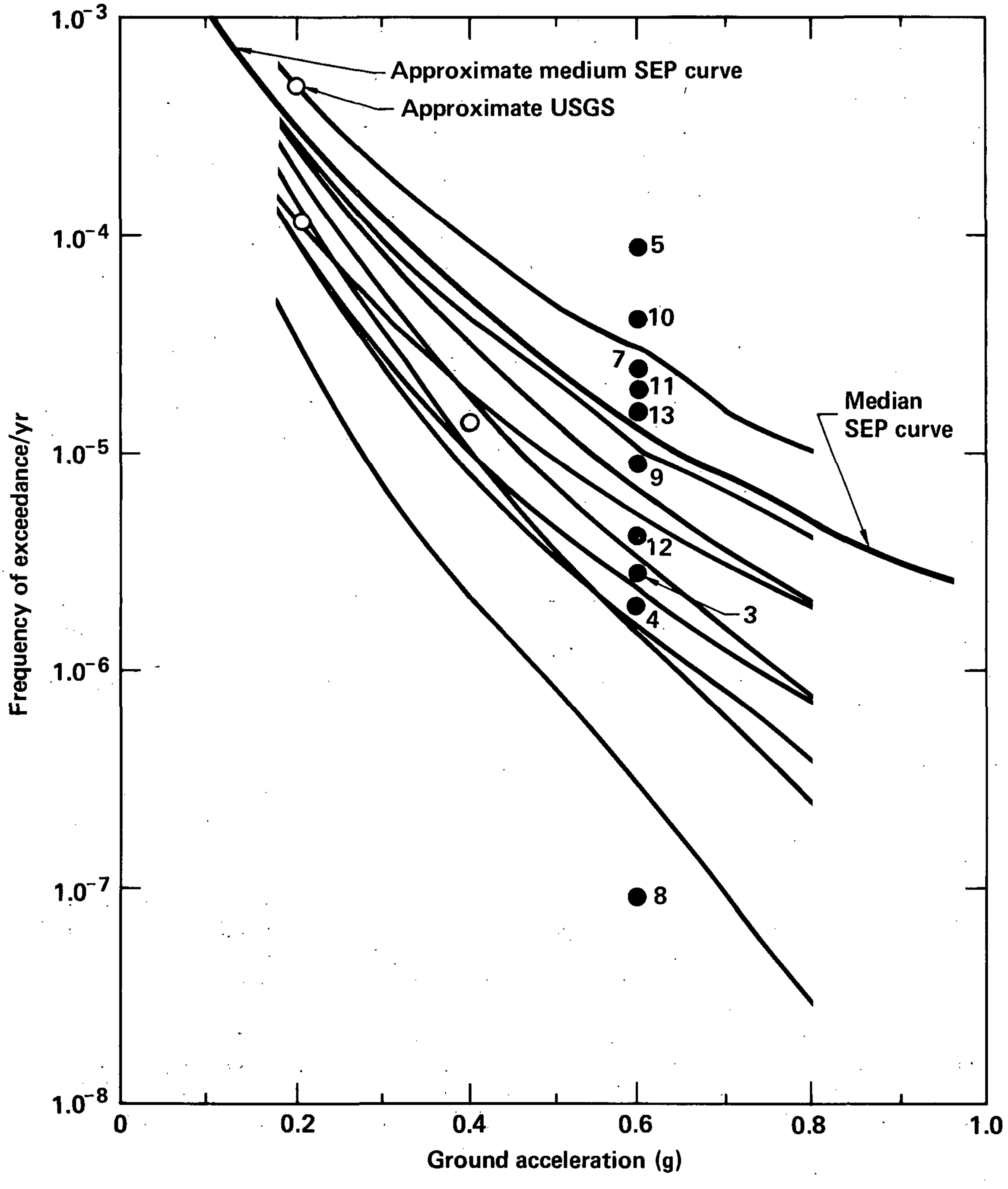


Fig. A-3 Comparison of hazard curves generated by SEP experts, D&M, and USGS approaches.

with items that would be required to fail in order to result in these initiators.

The following paragraphs describe several concerns regarding the initiating event selection process in the PSS.

A.3.1 Steam Generator U-tube Rupture[a]

The initiating event of steam generator U-tube rupture is discussed in PSS Section 2.5.1.2.1. It is stated there that the mean conditional probability of seismic-induced U-tube rupture is about 0.01 at 0.75g, and considering the low probability of a 0.75g earthquake, the conclusion was reached that detailed modeling of steam generator U-tube rupture is unwarranted. Although we have not seen detailed stress analysis results (and thus cannot be entirely sure of some of our assumptions), we nevertheless suggest that this conclusion be re-examined.

The basis for this suggestion is as follows. We do not know the number of U-tubes in the four steam generators at MP 3 but for the purpose of our discussion, we will assume there are 24,000. The conditional probability of 0.01 referred to above can then have two interpretations:

(1) Each of the 24,000 U-tubes has a failure probability of 0.01.

(2) Two hundred forty of the 24,000 U-tubes fail (24,000 x 0.01 = 240).

Using the second interpretation, fewer than 240 U-tubes would fail at lower accelerations than 0.75g. We understand that if as few as 20 U-tubes fail, then HPIS and LPIS may not be effective, if at the same time a LOCA occurs, and a core melt could occur. Since these failures occur during an earthquake, at the same time that we expect a transient to be in progress.

We believe that: (1) the U-tube initiator should be included in the PSS, (2) the fragility values for U-tubes should include any effects of degraded capacity due to corrosion, denting, radiation, etc.; and (3) a justification should be provided for not combining U-tube rupture with LOCAs.

If we use the analysis in PSS Section 5.2, but assume FCEE = 1.0 to account for U-tube degradation, we obtain a conditional failure probability of U-tubes of about 0.002 at the SSE acceleration. (As noted elsewhere in our review, we do not accept the argument in the PSS that seismic-induced failures are impossible at or below the SSE acceleration.) This analysis suggests that 0.002 x 24,000 = 48 U-tubes might fail at the SSE acceleration. Since U-tube failures from normal operation have been a common problem, it does not appear to be unreasonable to expect that failures due to the effects of earthquakes could also occur. This crude analysis suggests that a more careful analysis of the possibility and implications of seismic-initiated, U-tube rupture should be performed.

[a] This section addresses the SGTR analysis presented in the original PSS, i.e., prior to the revision of the fragility analysis.

Finally, we do not agree with the analysis of the probability of failure for U-tube rupture in PSS Section 2.5.1.2.1. These calculations should use total variability rather than just random variability. By doing so, the conditional probability of failure at 0.75g becomes about 0.04 rather than 0.01, for example. (Here, we used the total variability of 0.64 from Table 2-2B of PSS Appendix 2-I.)

A.3.2 Direct and Indirect Reactor Vessel Rupture (RVR)

Seismic-initiated RVR was not included in the analysis or discussed in the PSS. This failure could occur due to direct causes such as stress in the primary piping, as well as indirect causes like support failure (Ref. A-9).

The PSS should provide justification for not including this initiator in their analysis.

A.3.3 Loss-of-Coolant Accidents (LOCA)

The PSS does not clearly describe the process used to estimate LOCA initiating event probabilities. This is a difficult problem because of the large amount of piping in the primary system. It is also difficult because, for example, the simultaneous failure of a number of small pipes can be equivalent to a large LOCA. This manner of having the equivalent of a large or medium LOCA does not appear to have been included in the PSS.

The manner of estimating LOCA initiating events was not explicitly described in the PSS. The logical descriptions and probability estimates should include the various ways that multiple failures might lead to medium and large LOCAs as well as RVR.

A.3.4 General

A special effort should be placed on seismic initiating events in the PSS. This effort would seek to identify all the possible specific and unique ways that an earthquake might initiate an accident. More effort in this area may result in the conclusion that the initiating event conditional probabilities are larger than presently estimated in the PSS.

The key consideration is the capability of an earthquake to cause the simultaneous upset or failure of a large number of components. For example, what are the recovery steps required if a large number of relays, etc. need to be manually reset, even assuming they are not damaged? The data observed from the performance of operators at conventional power plants that experienced an earthquake is that in some cases it took a few hours to restart an undamaged plant while in other cases, only a few minutes were required (Ref. A-10).

A.4 Seismic Fragility

The review of seismic fragilities was performed by an LLNL subcontractor, Jack R. Benjamin & Associates. During the course of this review, we learned that NU had concluded their fragility assessment was unsatisfactory and that they were conducting a complete reassessment of these fragilities. Their submittal of a completely new fragility assessment to NRC in March 1984 made a new review necessary, which was completed in early May 1984.

Our review's results of the new fragility assessment, which are generally favorable, appear in Appendix C.

The results of our review of the original fragility assessment, generally not favorable, are contained in Appendix B. They are provided here only to complete the documentation of the review effort that was performed.

Additional observations and comments provided in the discussion below are primarily applicable to the original fragility assessment.

A.4.1 General Comments

Our overall impression of the seismic fragility analysis is that many of the median fragility values are conservative. However, numerous conceptual and philosophical errors were encountered and this led us to develop a lack of confidence that the fragility analysis was properly performed. Although there was evidence of considerable effort, the final fragility results are not consistent with the state-of-the-art.

If a number of median fragilities are found to be conservative and if these conservatisms exist for key components in dominant accident sequences, then we might expect that the removal of these conservatisms would lead to a downward revision of the estimates of the core melt probability in the PSS. Even if we had revised fragility estimates, it would be a significant calculational effort to follow these revisions through the analysis. (This is beyond the scope of our review.)

We will make a crude estimate of the possible effects of conservatism in the PSS fragility estimates. Our starting point is the median core melt acceleration that we estimate from Table A-1.

Table A-1 Mean core melt fragility.

Acceleration	Conditional probability of core melt
0.185	0.087
0.25	0.354
0.35	0.706
0.45	0.886
0.55	0.994[a]
0.65	0.993
0.75	0.999
0.80	1.0

[a] This is the PSS value, but it is an error.

Table A-1 was obtained from PSS Table 7.5.1-2. The median core melt value from Table A-1 is about 0.3g. The median of 0.3g intersects the second-highest seismicity curve in PSS Fig. 1.2.1-1 at about the median core melt probability in the PSS. We assume that the conservatisms in fragility lead to a factor of 2 on the median core melt we estimated from Table A-1. That is, we assume that the median core melt occurs at 0.6g, or at about three times the SSE g-level. Following the second-highest curve in PSS Fig. 1.2.1-1 from 0.3g to 0.6g, we find less than an order of magnitude difference in probability. We estimate that the median annual probability of core melt in the PSS will be reduced by about a factor of 5 when conservatisms in fragility are removed.

Although the variabilities (randomness and uncertainty) of the PSS estimates of fragility were obtained in an incorrect manner, the final numerical values are consistent with results from other commercial PRA studies. However, we believe that the uncertainty values in the PSS and other commercial PRA studies are too low.

One effect of an increase in uncertainty in fragility estimates is an increase of uncertainty in estimates of the probabilty of core melt.

We will use available results from the SSMRP (Ref. A-11) to estimate the effect of an increase in uncertainty in fragility estimates. Table A-2 summarizes key results on uncertainties.

Table A-2 Summary of results on annual probability of seismic-induced core melt.

Quantity	MP 3 PSS	SSMRP
95% confidence level	1.5E-4	2E-3
Mean	9.4E-5	2E-4
Median	9.1E-5	3E-5
5% confidence level	5.1E-5	1E-7

As shown in Table A-2, the difference between the high and the low value is about a factor of 3 in the PSS and 20,000 in the SSMRP. Note that the SSMRP results include the effects of uncertainty in the seismic hazard as well as fragility (as do the PSS results). These results are used in Section A.4.2 below to provide guidance on estimates of uncertainty.

Another effect of an increase in uncertainty in estimates of fragility is to increase the estimated median probability of core melt. We assume that this increase in core melt probability is relatively small in the PSS and is included in our estimates in other areas.

A.4.2 Specific Comments

PSS Appendix 2-J states that since structures and components were designed deterministically to withstand the SSE; (1) there is a cutoff value below which failure will not occur under seismic conditions, and (2) this value is the SSE acceleration of 0.17g.

No justification is provided for either of these assumptions and there are a number of reasons to question them. For example:

- Design and construction errors are not explicitly included in the PSS.
- The spectra used to design MP 3 are not an envelope of all possible spectra and have a probability of being exceeded.
- Some components (but not all) are seismically qualified by testing. There is a possibility that a weak component exists in the plant.

PSS Appendix 2-I states that "...this review is confined to plant elements having safety related functions..." Justification for this restrictive assumption is considered necessary in view of the pervasive effect of an earthquake.

The fragility values in the PSS are based on the concept of "sustained peak" rather than "instrumental peak" acceleration. The sustained peak concept is used to modify the hazard curves. While we do not disagree with the basic idea behind this concept, we do question the practice of applying a single factor at the level of the hazard curves. The factor is applied to the fragility of every component regardless of whether the component is a structure, mechanical system or component, or item of electrical equipment, or whether the anticipated failure mode is brittle, ductile, functional, or structural. The use of sustained peak acceleration in the PSS should be justified.

The discussion of uncertainty in PSS estimates of fragility is focussed primarily on developing the uncertainty values. There is relatively little discussion concerning interpretation of the uncertainties developed or the use of uncertainties in calculations. For example, there is no discussion of possible correlation of uncertainty or how correlation might affect the estimates of core melt in the PSS. It may be reasonable to assume that correlation exists between uncertainties in estimates of structural fragilities or between uncertainties in estimates of electrical fragilities. A thorough discussion of the meaning, interpretation, and use of uncertainty in estimates of fragility would be useful.

Correlation is discussed in the PSS at another level, see PSS Section 2.5.1.2.1, for example. There it is stated that the assumption of perfect correlation is made for seismic-induced failures of identically manufactured and physically proximate components and that this is recognized to be a conservative approach. We note that correlation may also exist in estimates of fragility through the estimates of dynamic response and that this can occur for components which are not in physical proximity. This aspect of correlation, discussed further in Section A.5, should be included in the PSS.

The uncertainty in estimates of fragility that are developed appear to address only uncertainty for the specific component. For example, this uncertainty would be used to describe the uncertainty in estimates of the probability of failure of the specific component. However, the primary intended use of fragilities in the PSS is in event tree-fault tree models of accident sequences in order to estimate the probability of these sequences. In such a case there is an additional uncertainty in how well these models estimate these probabilities. This uncertainty has been called modeling uncertainty (Ref. A-12). One way to include modeling uncertainty is to introduce it into the uncertainty in fragility. This issue is not addressed in the PSS. The PSS should describe how this modeling uncertainty is included. It is not included at this time and should be included in future estimates of seismic-induced core melt.

The fragilities in the PSS do not appear to include the effects of seismic-induced environmental conditions. For example, if an earthquake induces a LOCA or other failure, the resulting steam, internal flooding, temperature, or fire environment may induce failures in components that were not damaged directly by the earthquake vibrations. We recognize that this is a complex issue for which there is no simple solution. However, it is common for an earthquake to start a fire, for example. At a minimum, this issue should be addressed through a close examination of the initiating events and accident sequences and by modification of fragilities as appropriate. This examination should be thoroughly documented. In addition, initiating sequences should be identified that specifically account for seismic-induced environmental conditions. These sequences should also be thoroughly documented and discussed and the rationale provided for not quantifying any that are not included in the calculations. Conversely, the fragilities should also reflect any degradation due to environmental effects that exist prior to the earthquake.

On PSS page 2-I-58 the failure mode of electrical relay unrecoverable chatter or circuit breaker trip is identified. The circumstances under which relay chatter, for example, leads to an unrecoverable state, need to be much more carefully described. For example, conventional power plants that experienced an earthquake appear to have encountered some difficulty with relay chatter or breaker trip at accelerations of about 0.35g (Ref. A-10), which is a lower value than any of the MGACs in Table 2-2B of PSS Appendix 2-I, except for offsite power.

A.5 Seismic Core Melt Models

The modeling of seismic-induced accident sequences was performed through the use of logic diagrams and construction of a plant-level fault tree. An approach was taken in which perfect correlation among identical components in close proximity to one another was assumed. The PSS acknowledges, and we agree, that this approach is conservative. The consideration of random failures in the seismic sequences was performed in a simplified fashion, whereby two criteria were used to screen random failures to identify those with potential significant impact. The first criterion requires that the random failure must be significant relative to all relevant seismic-induced failures; the second criterion requires that the random failure contribute to a core melt accident progression that also involves at least one seismic-induced failure beyond the seismic-induced initiating event. The application of these criteria resulted in limiting consideration of random failures to pressurizer relief and safety valves and to operations requiring human action (e.g., feed and bleed).

There is a striking difference in the PSS in that the event tree-fault tree models used for seismic initiators are much coarser than the models used for internal (random) initiators. This difference raises the question as to whether model (in)completeness has any effect on the estimates of seismic-initiated core melt in the PSS. This issue is of particular concern for seismic initiators since the possibility exists for simultaneous failure of large numbers of components when an earthquake simultaneously threatens the entire plant. This consideration affects logical descriptions of initiating events and accident sequences as well as their quantification.

Explicit, direct quantification of the effects of model completeness would require substantial effort and is outside the scope of our review; however, it is possible to obtain insight on the effects of model completeness from two independent evaluations of Zion Unit 1. These results are available because:

- Seismic PRAs were performed on this plant as part of the SSMRP and as part of a PRA sponsored by the utility.

- The event tree-fault tree models used in the SSMRP are much more detailed than those used in the study sponsored by the utility. (This difference in level of detail is similar to the difference between the internal and external event models for MP 3 in the PSS.)

The major differences in the SSMRP and utility studies of Zion are

- differences in the level of detail of seismic analysis

- differences in fragility curves

- differences in hazard curves

- differences in the level of detail in event tree-fault tree models

While both the SSMRP and utility studies found essentially the same dominant accident sequences, there is nevertheless more than an order of magnitude difference in the median annual core melt probability; 3E-5 for the SSMRP and 2E-6 for the utility study, or a factor of 15. There is a factor of 40 on the means. We will now use (1) this difference (the SSMRP found that the median annual core melt probability for Zion Unit 1 was 15 times larger than was found in the utility study), (2) available SSMRP results, and (3) the above list of the four factors that might have contributed to the difference in (1) above,to provide an estimate of the effect of model completeness on the estimates of seismic-induced core melt in the PSS.

For Zion Unit 1, it is relatively easy to provide some insight on the effect of model completeness because only the fragility for the service water pumps contributed in any significant way to core melt in the utility-sponsored study. This means that if we use SSMRP inputs (seismic analysis, fragility, and hazard curves) to estimate the probability of failure of the service water pumps (that is, the probability of core melt in the utility study) and compare this with the SSMRP probability of core melt, we will obtain some measure of the effect of model completeness.

A minor complication in this comparison is that the two studies used fragilities for two different components to reflect loss of service water pumps. In the utility study, the fragility of the service water pumps was used. In the SSMRP, the fragility used was for the crib house pump enclosure roof - the collapse of which was assumed to result in failure of the service water pumps.

Using SSMRP inputs, the median annual probability of roof-induced failure of the service water pumps was found to be 2E-6. For the reasons described above, this is interpreted to mean that the utility study of Zion would have found the median annual probability of core melt to be about 2E-6 if SSMRP inputs were used in all areas except the level of detail in event tree-fault tree models. Coincidentally, this is the same value that was found in the utility study.

The difference between the two median probabilities of core melt (2E-6 for the utility study versus 3E-5 for the SSMRP) is thus found to be due to model completeness. That is, if more detailed models were used in the utility study of Zion, the median annual probability of core melt would be larger than the 2E-6 that was found - by as much as a factor of 15. Since we have not performed a detailed comparison of the SSMRP and utility seismic PRA studies on Zion, the factor of 15 should thus be considered preliminary and a result of crude estimates and gross simplifications. It is our best estimate at this time.

Since PRAs are highly plant- and site-specific, we should also not discount the possibility that even if 15 is the appropriate factor for Zion Unit 1, it may not be the appropriate factor for MP 3 because the utility studies on Zion and Millstone may be based on different assumptions and conservatisms whose effects may be significant enough to make the applicability of the above factor of 15 questionable. For example, in the utility study on Zion, the issue of model completeness is coupled with the assumed truncation of the hazard curves at the upper acceleration levels. Explicit direct quantification of the effects of this issue on the PSS estimates of core melt probability would require substantial effort and is outside the scope of our review.

Nevertheless, we estimate that the effect of model incompleteness in the PSS is an increase in the median annual probability of core melt by an order of magnitude.

As discussed elsewhere in our review, other issues lead us to both increase and decrease the estimates of core melt probability in the PSS. This order-of-magnitude estimate should thus be specifically noted to apply only to the model completeness issue addressed in this Section and not overall.

The model completeness issue in the PSS should have been addressed in the following explicit way.

The calculations should have been organized to demonstrate that the figure of merit (core melt, risk, etc.) does not change significantly if additional components, sequences, etc. are included in the calculations. The effects of uncertainties should be included in these calculations, but a complete uncertainty analysis is not required.

One relatively simple way to do this is to base the calculational demonstration on the mean figure of merit. In these calculations the random and uncertainty variabilities are combined in the hazard and fragility inputs to the calculation. Thus, a single hazard curve is developed where it combines the variabilities associated with the hazard. Similarly, a single fragility curve is developed for each component and it also combines the variabilities. Combining the two types of variabilities in this way has a number of advantages:

- The issue of uncertainty is explicitly addressed.
- The calculations are relatively simple.
- The growth of the figure of merit is based on a statistic (the mean) that has an easily interpreted and relatively stable meaning.

As a final check, the mean figure of merit obtained in the above manner should be compared with the mean obtained when the random and uncertainty variabilities are entered into the calculations separately.

A separate demonstration calculation may be required for each figure of merit. This is because the sequences that dominate core melt may not be the same ones that dominate risk, for example.

The model completeness issue is also directly related to the issue of estimates of uncertainty because crude models may lead to underestimation of the uncertainty. This may partially explain why the uncertainties in core melt probability in PSS Section 2.5.1.3 are so low (see Table A-2). As described on PSS page 7.5-4, uncertainties are propagated only through the dominant external risk sequences.

The model completeness issue is addressed in PSS Section 2.5.1.2.1. Model completeness is also coupled with another issue - the manner in which correlation is introduced into the calculations.

In PSS Section 2.5.1.2.1 the following statement is made on correlation (on page 2.5-4):

> ...the assumption of perfect correlation among the seismic-induced failures of identically manufactured and physically proximate components permits condensation of the system fault trees to reflect these dependencies.

On page 2.5-8 this statement is modified to exclude physical proximity, but this may be an oversight and it is not important to our point here.

The major problem with the above-quoted definition of how correlation was treated in the PSS is that this treatment does not go far enough. We could find no further discussion of correlation and thus we assume that this definition is a complete description of the approach to correlation in the PSS.

The aspect of correlation that is apparently omitted is the fact that correlation also arises as a result of the common dynamic response environment that occurs because an earthquake simultaneously excites all components of a plant. While this source of correlation will be observed for components that are in physical proximity, it will also be observed for other conditions, see Fig. 9.2 of (Ref. A-11).

In the PSS the primary way that correlation was used was in construction (condensation) of the system fault trees. The primary way that response correlation enters into the results is in the quantification of fault trees (and event trees if they exist).

This quantification is discussed in Chapter 9 of (Ref. A-11). Briefly, the major error probably arises in those logic expressions that contain a "logic AND" (see PSS Section 2.5.1.2.2). The problem is that ignoring the response correlation can lead to underestimation in the quantification of logical expressions.

Explicit, direct quantification of the effects of response correlation would require substantial effort and is outside the scope of our review. This quantification should be explicitly described in detail and included in the PSS.

However, for the purposes of this review, we will estimate the effects of response correlation in Section A.6. As noted above, this issue is coupled with our estimates of the effects of model completeness. We assume that the quantitative effects of response correlation are included in our above estimate of an order-of-magnitude increase in median annual probability of core melt.

A.6 Sensitivity Studies

The PSS is incomplete because it does not include the results of sufficiently deep sensitivity studies. Sensitivity studies are required to (1) provide an understanding of which elements of the analysis and the plant are important to the analysis results, (2) assess whether it is reasonable that these elements are the important ones and thus assess the reasonableness of the analysis, (3) refine the analysis of the important elements and provide a convincing demonstration of the robustness of the initial results or a revision of them, (4) identify any inconsistencies in the analysis, and (5) identify where design, construction, maintenance, etc., errors would be most important.

PSS Section 7.5.1 presents some results of sensitivity or dominance studies; however, these results may be of limited use because they are so-called mean results. This means that they are based on a mean hazard curve and presumably on median fragilities or on fragilities with only random variabilities included (the analysis is not clear on this point). As discussed in Section A.5 of our review, the dominance studies should be based on analyses that include the total (random plus uncertainty) variability. However, even this approach is not a completely satisfactory solution to the problem.

The basic problem is that the true value of the probability of core melt is unknown, as shown in Table A-2. The meaning of the SSMRP results in Table A-2 is something like the following: "We do not know what the annual probability of seismic-induced core melt is, but we have approximately 90% confidence that it is between 1E-7 and 2E-3. Its median value is approximately 3E-5 and its mean value is approximately 2E-4."

Since we do not know the true value of the annual probability of core melt we must be very careful when we make statements like "...26% of the core melt frequency is attributable to the TE damage states." (See PSS page 7.5-2.) The fundamental issue is: How do we confidently make quantitative statements of how much something (the TE damage states in the example) contributes to a quantity (the annual frequency of core melt in the example) whose value is unknown?

The Millstone PSS needs to be expanded to include a much more thoughtful and complete study of dominance, importance, and sensitivity.

A.7 Overall Quantitative Assessment

This section provides an overall quantitative assessment of our findings on core melt probability in the previous sections.

We summarize our findings as follows:

- In Section A.2 we found that the median seismic hazard was low by a factor of about 5.

- In Section A.3 we found apparent deficiencies in initiating events in the PSS but did not estimate their possible effect on core melt.

- In Section A.4 we found apparent conservatisms in the fragilities and estimated that their removal would reduce the median annual probability of core melt by a factor of about 5.

- In Section A.5 we found deficiencies in the treatment of model detail and response correlation and estimated that their combined effect would lead to an increase in the median annual probability of core melt by a factor of about 10.

- In Section A.6 we found deficiencies in the sensitivity studies in the PSS but did not find that they would lead to a significant change in core melt probability.

If we assume that the above factors are multiplicative we obtain the following result:

$$9.1E-5 \times (5) \times (1/5) \times (10) = 1E-3. \qquad (A-7)$$

That is, given the multiplicative assumption, we find that the median annual probability of seismic-induced core melt for MP 3 is about 1E-3. This is about 30 times the SSMRP median of 3E-5 on Zion Unit 1. At about 0.6g (the approximate acceleration that is assumed to dominate core melt) the SSMRP hazard curve has a median value of about 4E-5. The results from Section 4.A indicate that at about 0.6g the median hazard at MP 3 has a probability of about 2E-5. The closeness of these two hazard probabilities suggests that the factor of 30 is not a result of differences in the hazard at the two sites. This suggests that the factor of 30 is a result of differences in the two plants (Millstone Unit 3 and Zion Unit 1). The structures at Zion are founded on soil while most of the structures at MP 3 are founded on rock. Although the effects of soil-structure interaction might be expected to result in a lower probability of core melt at Zion compared to MP 3, our opinion is that it would not lead to a factor of 30 on the medians. Since MP 3 is a newer plant than Zion, our first reaction is that it is not reasonable that there should be a factor of 30 as we have estimated. However, we are not entirely sure that our reaction is valid. For example, this may simply be a reflection of the true uncertainties. That is, the medians are only estimates. As another example, the utility and SSMRP studies on Zion Unit 1 found a difference in medians of a factor of 15. There are, therefore, three possible conclusions:

(1) The median annual probability of core melt at MP 3 is greater than the value of 9.1E-5 found in the PSS and the true value may be about 1E-3.

(2) The multiplicative assumption is not valid. That is, it is not valid to multiply the factors as we have done. A more comprehensive and refined approach is required to assess the combined overall effect of the identified issues and thereby provide a valid estimate of the median annual probability of core melt at MP 3.

(3) The analyses that led to the individual factors are too crude and simplified and, as a result, the factors are in error.

Although we do not know which one or combination of these conclusions is correct, we are more confident in our estimates of the uncertainty in the annual core melt frequency. The SSMRP results from Table A-2 lead us to estimate that if the median annual core melt frequency is found to be on the order of 1E-5, then the 90% confidence interval is about 1E-3 to 1E-7. Note that this confidence interval is specifically stated to apply only to a median that is on the order of 1E-5.

A.8 References for Appendix A

A-1 D. L. Bernreuter, "Seismic Hazard Analysis: Application of Methodology, Results and Sensitivity Studies," USNRC Report NUREG/CR-1582, Vol. 4, 1981.

A-2 R. K. McGuire, "Fortran Computer Program for Seismic Risk Analysis," U.S. Geological Survey File Report 76-67, 1976.

A-3 D. L. Bernreuter, "Seismic Hazard Analysis: Review Panel, Ground Motion Panel, and Feedback Results," USNRC Report NUREG/CR-1582, Vol. 5, 1981.

A-4 TERA Corporation, "Seismic Hazard Analysis: Solicitation of Expert Opinion," USNRC Report NUREG/CR-1592, Vol. 3, 1980.

A.5 D. L. Bernreuter, J. Savy, R. Mensing and D. Chung, "Seismic Hazard Characterization of the EUS: Methodology and Interim Results for Ten Sites," USNRC Report NUREG/CR-3756, 1984.

A-6 O. W. Nuttli, "The Relation of Sustained Maximum Ground Acceleration and Velocity to Earthquake Intensity and Magnitude," Report 16 of State-of-the-Art for Assessing Earthquake Hazards in the United States, U.S. Army Corps of Engineers Waterways Experiment Stations, Vicksburg, Miss., Misc. Paper S-73-1, November 1979.

A-7 O. W. Nuttli, "Similarities and Differences Between Western and Eastern U.S. Earthquakes, and Their Consequences for Earthquake Engineering," to be published in Earthquakes and Earthquake Engineering: The Eastern U.S., Knoxville, Tenn., 1981.

A-8 S. T. Algermissen, D. M. Perkins, P. C. Theuhaus, S. L. Hanson and B. L. Bender, "Probabilistic Estimates of Maximum Acceleration and Velocity in the Contiguous United States," USGS, Open File Report 82-1033, 1982.

A-9 M. K. Ravindra, R. D. Campbell, R. P. Kennedy, H. Banon, "Probability of Seismic-Induced DEGB in RCL Piping," Proceedings of the 4th ASCE Specialty Conference on Probabilistic Mechanics and Structural Reliability, Berkeley, California, January 11-13, 1984.

A-10 P. E. Yanev, S. W. Swan, "Program for the Development of an Alternative Approach to Seismic Equipment Qualification, Volume 1: Pilot Program Report, Volume 2: Pilot Program Appendices," EQE, Inc., San Francisco, California, 1982.

A-11 M. P. Bohn, L. C. Shieh, J. E. Wells, L. C. Cover, D. L. Bernreuter, J. C. Chen, J. J. Johnson, S. E. Bumpus, R. W. Mensing, W. J. O'Connell, D. A. Lappa, "Application of the SSMRP Methodology to the Seismic Risk at the Zion Nuclear Power Plant," USNRC Report NUREG/CR-3428, May 1983.

A-12 P. D. Smith, R. G. Dong, "Seismic Safety Margins Research Program (Phase I) Interim Definition of Terms," Lawrence Livermore National Laboratory, Livermore, California, UCRL-53001, December 1980.

APPENDIX B

REVIEW OF THE
MILLSTONE UNIT 3 PROBABILISTIC SAFETY STUDY
SEISMIC FRAGILITY, WIND AND EXTERNAL FLOODING

by

John W. Reed

Prepared for

Lawrence Livermore National Laboratory

Livermore, California

December 22, 1983

TABLE OF CONTENTS

Page

1.0 INTRODUCTION.. 1-1

1.1 Scope.. 1-1

1.2 Overall Methodology.. 1-3

1.2.1 Seismic Fragility.. 1-3

1.2.2 Wind.. 1-5

1.2.3 External Flooding.. 1-5

2.0 SEISMIC FRAGILITY.. 2-1

2.1 Report Sections.. 2-1

2.2 Calculations.. 2-8

2.3 Closure.. 2-26

3.0 WIND.. 3-1

4.0 EXTERNAL FLOODING.. 4-1

5.0 CONCLUSIONS AND RECOMMENDATIONS.. 5-1

5.1 Seismic.. 5-1

5.2 Wind.. 5-2

5.3 External Flooding.. 5-2

REFERENCES.. R-1

1.0 INTRODUCTION

Jack R. Benjamin and Associates, Inc. (JBA) was retained by Lawrence Livermore National Laboratories (LLNL) to perform a review of the Millstone Unit 3 Probabilistic Safety Study (referred to as the Millstone PSS), which was prepared by Northeast Utilities Service Company (NUSCO), August 1983. The areas reviewed included seismic fragility, wind, and external flooding. The scope of the review is discussed in the next section. The final section in this chapter discusses the overall methodology used to develop the seismic fragility data and the bases for excluding wind and external flooding. Chapters 2, 3, and 4 present the review of seismic fragility, wind, and external flooding, respectively. Finally, Chapter 5 gives conclusions and recommendations based on the review.

1.1 SCOPE

The review of the Millstone PSS focused on the following report sections which document the seismic fragility, wind, and external flooding analyses:

• Section 1.2.3	External Flooding
• Section 1.2.5	Wind
• Section 2.5.1	External Event Analysis
• Appendix 2-I	Millstone Unit 3 Seismic Analysis--Structures and Equipment
• Appendix 2-J	Millstone Unit 3 Probabilistic Analysis of Structural and Component Fragilities

Jack R. Benjamin and Associates, Inc. has performed similar reviews of the Indian Point Probabilistic Safety Study (IPPSS) (Ref. 1) and the Zion Probabilistic Safety Study (ZPSS) (Ref. 2). (See Reference 3 for the IPPSS review. The Zion review has not been published.) Based on experience gained from the IPPSS and ZPSS reviews, the review of the Millstone PSS was conducted in a short time period in order to quickly evaluate the adequacy and accuracy of the results and to make recommendations based on the findings. In contrast to the previous reviews which consisted of an in-depth evaluation of each section and subsection of the PRA report, this review focused on critical areas which impact the results.

Dr. John W. Reed performed the review of the Millstone PSS. Dr. Martin W. McCann, Jr. assisted in the review of the external flooding hazard. One man-month of effort was devoted to the review with approximately two days each spent on the wind and flood sections with the remaining time devoted to the seismic fragility analysis.

During the review, a meeting was held with NUSCO to discuss the findings. It was learned that a reanalysis of the seismic hazard and fragility parts of the Millstone PSS is currently being conducted. The reanalysis has not been reviewed and comments in this report are made only for the information given in the Millstone PSS which was submitted in August 1983. A tour of the plant site was conducted at the end of the review. In comparison with other plants, the Millstone 3 structures and components appear to be properly constructed and supported from a structural viewpoint. The construction details and appearance of the plant, support the comments and conclusions made in this report.

It was assumed in the review that LLNL would be responsible for evaluating the seismic hazard analysis and the systems analysis (i.e., event trees, fault trees, and hazard/fragility integration). Since the overall seismic analysis was not reviewed, the impact of the findings are discussed in terms of the various component seismic fragilities. Note that it was concluded in the Millstone PSS that wind and external flooding are not significant hazards, hence no formal probabilistic analysis was conducted.

1.2 OVERALL METHODOLOGY

The overall methodology used to develop the seismic fragility data and the bases for excluding wind and external flooding are discussed below.

1.2.1 Seismic Fragility

The methodology used in the Millstone PSS to develop seismic fragility data is appropriate and adequate to obtain a rational measure of the probability distribution on the frequency of failure. However, the application of the methodology is a concern. It is stated in the calculations and Appendix 2-I that References 4 and 5 were used as the basis for the seismic fragility analysis. The approach used in the Millstone PSS is referred to in the PRA Procedures Guide as the "Zion" method (Ref. 6). However, the method used was not named or justified as appropriate in the Millstone PSS.

The Zion method has two important features. First, the methodology is based on a double lognormal distribution model. Both the distribution on the median and the random variation of frequency of failure are assumed to be lognormal. Secondly, the probabilistic analyses use the results from the original design analysis as the basis for the seismic fragility estimate. The median fragility values are obtained using the responses and capacities from the design analyses which are scaled to eliminate conservatisms and variabilities (i.e., randomness and uncertainty) and are estimated based on some data, but mostly on engineering judgment.

It is interesting to note that nowhere in the Millstone PSS report sections pertaining to the seismic fragility analysis was the word "lognormal" used. Thus, no defense is given why the lognormal model is appropriate. As discussed in Chapter 2 of this report, there is considerable confusion since the logarithmic standard deviations reported in Appendix 2-I (note they are referred to as randomness and uncertainty variabilities or beta values) for structures and equipment are incorrectly interpreted as standard deviations. Also, the lognormal distribution is converted to a Weibull distribution with a lower bound cutoff at 0.17g. This is philosophically inconsistent since the fragility analysis incorrectly assumed that the variabilities of the various capacity and response parameters are lognormal. It is also not clear that 0.17g is the proper cutoff point. Since potential design and construction discrepancies were not considered in the analysis, the use of a lower-bound cutoff is difficult to defend.

As discussed in Chapter 2, many errors in the seismic fragility analysis were found. In general, the assumptions which were made are on the conservative side. The final conclusion is that the analysis is not rational and the frequencies of failure are too conservative. This is part of the reason why the mean frequency of core melt is 9.4×10^{-5}, which is high relative to the results from other PRAs.

From Section 7.5 (i.e., Table 7.5.1-2) of the Millstone PSS, the mean systems fragility values for core melt were obtained and listed in Table 1-1. As can be seen from Table 1-1, the frequency of failure is very high with a median value approximately equal to 0.3g. Even close to the SSE value of 0.17g, the frequency of failure is on the order of 1 in 10. This is not reasonable since Millstone is a newer plant, which has been designed to comply with more recent regulations.

In contrast to other PRAs submitted to the USNRC to date, the Millstone PSS reflects new response analyses based on simple single-degree-of-freedom (SDOF) models for the buildings. This was done to rationally evaluate the conservatisms in the floor response spectrum used in the design analyses. This is commendable; however, it is not clear from the calculations whether the effects of the higher frequency building modes have been properly accounted for in the SDOF analyses.

A troublesome concern is the question of secondary nonsafety-related components failing and falling on safety-related equipment.

This issue is not addressed. Also, it is not clear why the Main Steam Valve building was not considered in the fragility analysis, since it is a safety-related structure.

The same general philosophical concerns from past PRA studies, which were based on the Zion method, also apply to the Millstone PSS. Reference 3 discusses these issues in depth based on the review ot the IPPSS. The reader is directed to Section 2 of Appendix A of Reference 3 for a general discussion of these issues.

1.2.2 Wind

It is concluded in the Millstone PSS that wind effects do not contribute significantly to the risk. As discussed in Chapter 3.0, this conclusion is reasonable. The argument for excluding wind is based on the hazard at the site and the protection provided by the two-foot-thick concrete walls and roof elements which form the safety-related structures. No fragility curves were developed and a systems analysis was not performed.

1.2.3 External Flooding

Similar to wind, it is argued in the Millstone PSS that external flooding is not a significant hazard to the risk at Millstone. As discussed in Chapter 4, the arguments given do not provide a rational basis for excluding flood. Since external flooding was eliminated, no fragility curves were developed and a systems analysis was not performed.

Table 1-1. Mean Core Melt Systems Fragility Values

Ground Acceleration	Mean Frequency of Failure
0.185	0.087
0.25	0.354
0.35	0.706
0.45	0.886
0.55	0.958
0.65	0.993
0.75	0.999
0.80	1.000

2.0 SEISMIC FRAGILITY

The review of the seismic PRA analysis focused on the following sections of the Millstone PSS report:

Section 2.5.1	Seismic Risk Analysis
Appendix 2-I	Millstone Unit 3 Seismic Analysis--Structures and Equipment
Appendix 2-J	Millstone Unit 3 Probabilistic Analysis of Structural and Component Fragilities

In addition to the review of these sections, the calculations for selected structures and components which are significant contributors to the frequency of core melt were evaluated. The steam generator was also included in the review since it was given as a representative example in Appendix 2-I.

Section 2.1 presents comments on specific sections of the report pertaining to the seismic fragility analysis. Section 2.2 gives the results of the review of the fragility calculations for selected items. Finally, Section 2.3 closes the seismic review and gives an estimate of the general level of conservatism which is contained in the Millstone PSS fragility analysis.

2.1 REPORT SECTIONS

The following comments are directed to specific sections of the PSS. Page numbers precede each comment to help the reader locate the area of concern. Specific comments on the calculations of structure or component fragility data are given in the next section.

Section 2.5.1 Seismic Risk Analysis

Page 2.5-2: It is stated that failure is assumed to occur if allowable load limits established by design codes or functional tests are exceeded. This is an overly conservative assumption; however, the fragility calculations in Appendix 2-I did not adhere to this constraint, but rather included the energy-absorption capacity beyond the yield limit, if appropriate.

Page 2.5-3: β_R and β_U are described as being standard deviations. In fact, they are logarithmic standard deviations. This philosophical error is discussed in more detail below (see comments on Appendix 2-J).

Page 2.5-5: It is assumed that the safety-related components designed to the SSE level will not fail (i.e., probably equal to 1.0) for accelerations below 0.17g. As concluded below, the fragility curves are conservative, and the equivalent median frequency of the safety-related systems, which is between 0.25g and 0.35g, should be roughly a factor of two to three higher. For higher capacities, this cutoff assumption is not critical. However, for the analyses documented in the PSS, accelerations below 0.17g will contribute noticeably to the mean frequency of core melt. As discussed in Section 1.2, the lower bound cutoff value of 0.17g has not been justified.

Page 2.5-6: Components above 1.11g were excluded from the fault tree since their capacity is sufficiently high such that they do not contribute significantly to the results. However, if higher capacities are justified as discussed below, then some of the excluded components may become significant contributors.

Page 2.5-10. Terminating the analysis at 0.8g is inconsequential for the low structural capacities developed in the PSS since the mean system fragility curve corresponds to a frequency of failure of 1.0 at 0.8g (see Table 1-1 in Chapter 1). However, if higher capacities are used as discussed below, then the upper bound acceleration cutoff should be justified on the basis of the maximum earthquake intensities which can occur.

Page 2.5-11: The assumption that incipient sliding leads directly to failure of interconnecting piping is very conservative.

Page 2.5-12: The basis for the comment that structural sliding does not affect interconnecting piping and cabling is not true. However, the incipient sliding condition assumed in the PRA is very conservative (see comment directly above).

Appendix 2-I - Millstone Unit 3 Seismic Analysis--Structures and Equipment

Page 2-I-6: It is not clear why the variabilities were reduced on a selected basic at the end of the project.

Page 2-I-24: It is stated that as part of the inelastic energy absorption capacity, the redistribution of forces among structural elements was considered. For the component calculations reviewed (see Section 2.2), no allowance for force redistribution was found.

Page 2-I-26: The definition of seismic fragility as ". . .level of effective median peak ground acceleration at which the structure would cease (fail) . . ." is incorrect. The median value is a parameter of the lognormal distribution on capacity, not the entire fragility curve of a structure.

Page 2-I-26: The sliding capacity as calculated is the incipient sliding capacity and is conservative. As discussed below (see Section 2.2), the amount of sliding displacement and its effects on interconnecting equipment is the critical issue, not the level of ground motion at which sliding begins.

Page 2-I-28: FCSM should be the ratio of the strength, computed with the actual material properties, divided by the strength, computed with the specified material properties.

Page 2-I-30: The simple inelastic energy model used in the PRA analysis is applicable to structures which can be modeled as single-degree-of-freedom systems. This model has not been shown to apply to complex structures. At best the uncertainty is a function of the complexity of the system being analyzed.

Page 2-I-30: The average factor of safety due to earthquake combination (i.e., 1.3) where the responses from the three directions were combined using an absolute sum, is a gross approximation. A specific value should be determined for each structure. For example, using data from the FSAR it can be shown that values of 1.2 and 1.4 are more appropriate for the interior concrete and exterior shell of the containment building, respectively. However, it was later determined that the seismic forces were actually combined by the SRSS method in the PRA calculations for the Containment internal structure. See discussion in Section 2.2 for the Containment crane wall failure.

Page 2-I-35: The use of different soil-structure interaction safety factors for the EGEB (i.e., for sliding and strength failure modes) is inconsistent. The values should be the same.

Page 2-I-36: The variability in the ultimate strength prediction is also due to uncertainty in the simple models used in the PRA analysis.

Page 2-I-37: The variability for the design capacity factor should be based on the strength equation which generally is different for each structure. A range of ±20 percent (COV) is a gross approximation, which should be determined specifically for each structure.

Page 2-I-37: The material strength factor variability is not equal to the variability in material strength. It is equal to the variability of the strength model due to variability in the parameters in the model such as material properties.

Page 2-I-39: The statement: "The randomness also was considered to contain the uncertainty of the mean" is philosophically wrong. By definition, randomness and uncertainty are mutually exclusive.

Page 2-I-39: The modeling factor variability should be based on variability of the modal frequencies and mode shapes. The frequency effect should be obtained using the median ground response spectrum at the median damping value. Variability in frequency should be transformed using the response spectrum to variability in response. The use of ±15 percent (COV) is a gross approximation and should be determined specifically for each structure.

Page 2-I-40: The basis for establishing the earthquake combination factor variability is not rational. Some simple calculations for the Limerick PRA (Ref. 7) show that the randomness logarithmic standard deviation varies from 0 to 0.16 depending on the relative responses from the three components and the coupling between the responses. Thus the value of 0.22 is on the high side.

Pages 2-I-41 to 44: See Section 2.2 for a discussion of the calculations performed for selected structures.

Page 2-I-58: It is assumed that electrical relay unrecoverable chatter is a failure. It is not clear how this was used in the PRA analysis. Also, using incipient sliding of the connecting buildings as a failure mode for buried piping is very conservative.

Page 2-I-61: Single-degree-of-freedom models were used to obtain the modified ARS for median damping values (i.e., 10 percent for structure and 5 percent for equipment). It is not clear whether the effect of higher frequency modes was properly included in the modified floor response spectra.

Page 2-I-63: The report states that the variability for the equipment design capacity factor for piping was based on the ratio of design pressure to operating pressure calculated for each representative pipe element. This is not rational. The variability should be calculated from the strength equation using the variabilities for the model parameters (i.e., material properties).

Page 2-I-64: Equation 4-4 is for a lognormal distribution, not a normal distribution as stated. This is an example of the misunderstanding of what was calculated and reported in Appendix 2-I.

Page 2-I-65: The generic damping factor variability value of 0.09 may be low for equipment with natural frequencies close to the lower frequencies of the supporting structure. When the frequencies of the equipment and structure coincide, small differences in equipment damping can cause large differences in response.

Page 2-I-65: Modeling factor variability includes contributions from mode shape and frequency. The latter effect is sensitive to the proximity of the equipment frequency value to the peak of the floor response spectra. Component-specific values for this parameter should be developed.

Page 2-I-65: The earthquake component combination variability is a function of the relative contributions from the three earthquake components and the degree of coupling which exists. The frequency of the equipment (i.e., flexible versus rigid) is not a significant variable for this type of variability. The logarithmic standard deviation values are typically between 0 and 0.16.

Page 2-I-66: It is assumed that the earthquake component combination factor variability is the same as the structural response factor variability for the structure in which the component is located. This is not rational. This factor should be based on the characteristics of the equipment, not the structure as discussed above.

Page 2-I-72: The modal combination factor, FRSC, should not be included in the structure response factor when determining the fragility for an equipment item, since the floor response spectra were obtained from a time history analysis (i.e., since the phasing information is properly incorporated). Also, the earthquake combination factor, FRSE, should not be included since the effects of random phasing between the earthquake components should only be included in the equipment response factor.

Page 2-I-76: The illustrative example given in Appendix 2-I, Section 5.2 is discussed as part of the review of the calculations for significant components in Section 2.2, below.

Page 2-I(A)-2: As discussed above for page 2-I-61, it is not clear that the higher frequency modes of the buildings were properly reflected in the modified ARS development.

From the calculations it appears that the equipment spectral shape factor was calculated properly. The safety factor for equipment damping was obtained from a ratio of the relative floor responses (i.e., the median level case vs. the design level case) where the relative floor responses for each case were obtained as the spectral ordinate divided by the zero period acceleration value. This approach is reasonable; however, it is not clear that the effect of higher frequency modes of the structures was properly incorporated.

Also, as discussed below in Section 2.2, the approach used for scaling the structure response factor with height is incorrect.

Appendix 2-J - Millstone Unit 3 Probabilistic Analysis of Structural and Component Fragilities

Page 2-J-2: It is obvious from the use of the fragility parameters produced in Appendix 2-J that the authors of this appendix did not realize that a median value and two logarithmic standard deviations were developed for each structure or component in Appendix 2-I. It was erroneously assumed that β_R and β_U are standard deviations (in fact, they are logarithmic standard deviations). The conversion from a lognormal distribution to a Weibull distribution is incorrectly performed. By assuming that the betas from Appendix 2-I are standard deviations the variabilities are increased substantially. The final result is that the fragility curves used in the analysis are overly conservative.

2.2 CALCULATIONS

The calculations for a select group of structures and components were reviewed. The following items were chosen because they are significant contributions to the frequency of core melt. The steam generator was also reviewed since it is the single illustrative example that is presented in Appendix 2-I of the Millstone PSS report.

Structure/Component	Median Capacity (g)*
Steam Generator	2.28
Auxiliary Building (collapse)	0.55
125 VDC Distribution Panel	0.64
Demineralized Water Storage Tank	0.68
Reactor Core Geometry	0.68
Service Water Piping	0.74
ESF Building (sliding)	0.74
Emergency Generator Enclosure (sliding)	0.75
Containment (crane wall failure)	0.87

*Listed in Table 2.5.1-3 of the Millstone PSS report.

A discussion of the calculations for each item is given below.

Steam Generator (Millstone PSS Report Section 5.2 - ILLUSTRATIVE EXAMPLE)

Numerous discrepancies were found in the illustrative example of the steam generator. The following is a discussion of the problems which were encountered.

The structure earthquake combination factor, FRSE, should be 1.0, not 1.3, since the equipment was designed using the SRSS procedure. Also, the structural response factor should not be scaled to different elevations, since as first approximation all points in the building above the base are equally affected by changes in the structural response parameters (i.e., spectral shape, damping, modeling, etc.). Hence the structural response factor should be just 1.5.

In developing the variability for the spectral shape safety factor, it was assumed that the uncertainty component was zero, which is similar to what was done in past seismic PRA studies. As discussed in Reference 3, it is believed that if this were true, there would be no motivation to ever conduct site studies to develop site-specific spectra.

The variability for modeling is assumed to be all uncertainty with a logarithmic standard deviation of 0.15. This value is consistent with other PRA studies; however, it is more rational to compute this parameter for each building considering variability in the mode shape and fundamental frequency. In the Zion and Indian Point PRA studies, the logarithm of the ratio of the spectral ordinates of the median spectrum at the median and median minus one standard deviation frequency was used to compute the uncertainty value.

The variability for structure modal combination (i.e., 0.17) should not be included since the floor response spectra were obtained using a time history analysis where all significant modes and the phasing between the modes were retained. The variability for structure earthquake component combination (i.e., 0.22) should be eliminated for the structural response factor and a smaller value included in the equipment response factor. Based on a study conducted as part of the Limerick PRA (Ref. 7), the randomness due to earthquake components is a function of the number of components which contribute to the response and the degree of coupling between the components. Values for the logarithmic standard deviations varied in the study from 0 to 0.16. Also, a small randomness component for damping would be more reasonable than assuming zero.

The safety factor for equipment response, FRE, was assumed to be 1.0. The spectral shape factor, FRES, was inappropriately assumed to be 1.0. The value for this factor is actually included as part of the capacity factor (i.e., third equipment factor equal to 1.5). However, this factor was not computed correctly since it is based on the ratio of the design ZPA value to the median ZPA value. Since the steam generators are flexible, the factor should be based on the ratio of spectral ordinates corresponding to the fundamental frequency of the component.

The variability for equipment spectral shape factor was assumed equal to the same value as for the structure spectral shape factor. The variability should have been based on the floor response spectra from the median analysis and split into randomness and uncertainty components corresponding to single mode variability and higher mode contributions, respectively. Similarly, the equipment damping variability should have been based on floor response spectra from the median analysis. The value of 0.09 in the report is equal to the variability in damping. It should be equal to the variability in response due to the variability in damping. Also, the equipment damping variability should be split into randomness and uncertainty components.

The equipment modeling variability should reflect variability in mode shape and frequency. Both of these factors are affected by uncertainty in boundary conditions and randomness of material properties. The frequency variability can be used to directly obtain response variability using the median floor response spectrum at the location of the steam generators.

The randomness of the capacity factor due to material property variability is equal to 0.14. According to the calculations, this was obtained by the following expression:

$$\ln (1.25)/1.65 = 0.14$$

where 1.25 is the lower bound capacity factor and 1.65 corresponds to the 95 percent probability level. This is incorrect. The logarithmic standard deviation should be based on the randomness in design capacity due to the randomness in the material properties. Although the value used (i.e., 0.14) is reasonable, the method for obtaining this number is not rational.

The variability in the inelastic energy absorption factor was incorrectly set equal to the variability in the ductility ratio. A more correct value is obtained by the following expression:

$$\ln \sqrt{\frac{2(3) - 1}{2(1.5) - 1}} / 2 = 0.23$$

In addition to the uncertainty in the ductility ratio, there is uncertainty in the inelastic energy absorption model, which should be included. Again, the value of 0.35 used is reasonable, but the method for obtaining this value is not rational.

In conclusion, the median acceleration value of 2.28g may be reasonable. The structural response factor should be 1.5, not 2.51, but the spectral shape factor (called the third design capacity factor in the report) should be based on the design versus the median spectral ordinates at the natural frequency of the steam generator. It is likely that the correct safety factor for spectral shape is greater than the 1.5 value used in the analysis. Thus, the two discrepancies tend to offset each other.

The total variability logarithmic standard deviation value of 0.62 tends to be on the high side. It is likely that a more careful analysis would reduce this value.

Auxiliary Building (Collapse)

The design capacity safety factory, FCSD, equal to 1.6 for the Auxiliary building collapse, is based on the strength of columns in the building. It is assumed that there is no significant margin beyond the design load; thus FCSD is equal to 1.1/0.7, where 1.1 is the SSE load factor and 0.7 is the code capacity reduction factor for tied columns. It is not clear why columns are controlling the capacity for seismic events since the Auxiliary building is a shear wall structure. In typical shear wall buildings the walls resist the lateral forces and the columns support vertical dead and live loads. For cases where lower story columns support upper story walls, axial forces due to seismically-induced overturning moments at the bottom of walls will be predicted by elastic analyses; however, if the columns begin to yield the lateral loads will redistribute through the floor diaphragms to walls which extend to the foundation. This safety factor is an important contribution to the median capacity and is low compared to similar factors for shear wall structures at other nuclear power plants.

The material strength safety factor, FCSM, equal to 1.35 is based on the ratio of the column axial strength using actual material properties to the strength using design properties. This is appropriate if column axial strength is the dominate strength contribution. Because an axial column failure is a brittle failure no inelastic energy absorption was assumed. As discussed above it may be unrealistically conservative to assume that the Auxiliary building will fail based on overstressing the building columns. Possible redistribution of forces should be considered.

The spectral shape factor, FRSS, was based on the ratio between the spectral ordinates of the design spectra and the median rock spectra from WASH-1255 (Ref. 8). The approach used is appropriate and is consistent with other PRA studies.

The damping safety factor was incorporated in the development of the spectral shape safety factor in that the design spectrum at 5 percent damping and the median rock spectrum at 10 percent damping were used. This is a consistent approach.

The modeling safety factor, FRSM, was assumed to be 1.0. It is stated in the calculations that modeling was accounted for in the spectral shape safety factor. Since the calculated frequency was assumed to be the median frequency, this is correct.

The SRSS combination of modal response was used; hence, the modal combination safety factor was assumed to be 1.0. This is reasonable.

The earthquake components were evidently combined using an SRSS combination for the Auxiliary building. This contrasts to other Millstone building analyses where the absolute sum of all three components was supposedly used. For the Auxiliary building, a safety of 1.0 is appropriate for this safety factor.

Since the Auxiliary building is on rock, the safety factor for soil-structure interaction is 1.0.

In conclusion, the total safety factor of 3.24 appears to be low. The assumption that the interior columns control the capacity of the Auxiliary building should be reexamined.

The uncertainty logarithmic standard deviation for strength failure of structures was assumed to be 0.20 for all buildings. It was not based on the uncertainty of the different strength prediction models, but was assumed based on values used in the Zion and Oyster Creek PRAs. Because of the possibility of load redistribution, this value is on the low side.

The randomness logarithmic standard deviation for material strength of the Auxiliary building was based on the variability of individual construction materials (i.e., steel and concrete). However, the variability of the strength equation should have been used rather than the variability of the individual material strengths. The value of 0.10 which was assumed is reasonable compared to results from other PRAs.

Because no inelastic energy absorption was assumed for the Auxiliary building, no variability was assumed. This is reasonable based on this premise; however, the assumption that there is no inelastic capacity is very conservative.

In developing the variability for the spectral shape safety factor, it was assumed that the uncertainty component is zero, which is similar to what was done in past seismic PRA studies. As discussed in Reference 3, it is believed that if this were true, there would be no motivation to ever conduct site studies to develop site-specific spectra. The approach used to develop the randomness component was based on the logarithm of the response spectral ordinates from the WASH-1255 spectra at the median and the median plus one standard deviation curves, which is a reasonable approach.

The variability for damping effects was assumed to be all uncertainty. The logarithmic standard deviation was based on the logarithm of the response spectral ordinate from the median curves at 7 percent and 10 percent, where it is assumed that the 7 percent value is at the minus one standard deviation level. The approach used is reasonable. However, there should be a small randomness component.

The variability for modeling is assumed to be all uncertainty with a logarithmic standard deviation of 0.15. This value is consistent with other PRA studies; however, it is more rational to compute this parameter for each building, considering variability in the mode shape and fundamental frequency. In the Zion and Indian Point studies, the logarithm of the ratio of the spectral ordinates of the median spectrum at the median and median minus one standard deviation frequencies was used to compute the uncertainty value.

The variability for modal combinations was assumed to be all randomness, and the logarithmic standard deviation value of 0.17 was assumed based on what was used in the Zion PRA. This is consistent with other PRA studies.

For the combination of earthquake components, the variability was assumed to be all randomness, which is appropriate. However, a value of 0.17 was assumed to be equal to the same value as used for modeling (see discussion above). The basis for this value is not rational and is probably on the high side. The results of a study conducted for the Limerick PRA (Ref. 7) were based on considering the possible response extremes to be at ±3 standard deviations. Different response coupling and phase relationships (i.e., in-phase and out-of-phase) were considered. The values for the logarithmic standard deviations ranged from 0 to 0.16. Although the assumption of ±3 standard deviation range is debatable, based on this study the 0.17 value seems high.

Since the Auxiliary building is on rock, there will be no significant soil structure interaction, hence the variability is essentially zero.

In conclusion, the logarithmic standard deviation for combined variability is 0.43, which is consistent with other studies. However, the approach used to obtain the value is not entirely rational as discussed above, and the final value of 0.43 is probably on the low side.

125 VDC Distribution Panel

The 125 VDC Distribution Panel contains switchgear and is located on the base mat of the Control building. The PRA calculations for this component are confusing, and it is difficult to systematically account for all the discrepancies that have occurred in the calculations. It is assumed in the analysis that electrical malfunctions will occur at a higher acceleration than failure of the external cabinet. Consequently, a static force computer analysis was performed using forces from transmissibility data obtained from dynamic tests of the cabinet.

In the development of the design capacity factor, the computer analysis was conservatively biased. Both horizontal direction earthquake loadings were applied simultaneously (which produced an absolute sum combination in the critical column). The maximum stress appears to be high for the applied loading. The energy absorption safety factor was based on a median ductility value of 1.5, which is low.

The randomness value of 0.14 assumed for the effect of material strength on design capacity is not rational. This is the same incorrect value as used for the steam generator (see discussion above). The variability for inelastic energy absorption is low. The median and median plus one standard deviation values for ductility were assumed to be 1.5 and 1.8, respectively. This is not a realistic range. Also, no uncertainty was assumed for the inelastic energy absorption model.

The equipment response safety factor was assumed to be 1.0 with a variability logarithmic standard deviation of 0.24. The latter value is different from the calculations (i.e., 0.15) and may be low because the variability value consists only of contributions from instrumentation and control errors, and modeling effects. The effect of response spectrum, frequency, damping, mode shape, mode combination, earthquake combination, general test input, and static model factors should also be systematically incorporated into the analysis.

The structural response safety factor also was assumed to be 1.0 with a variability of zero. This assumption was made because the equipment is supported on the base mat which was poured against the ground. According to the FSAR, there is some fill beneath the Control building, and a soil-structure interaction model was developed in the design of the building. The base mat floor response spectrum should be used in developing the equipment response factor and the ground response spectrum used to develop the structural response factor with the appropriate properties of the building (i.e., frequency, damping, mode shape, etc.). Even if the building were supported directly on rock, the equipment response factor should reflect the difference between the design and median ground response spectra.

Note that the analysis assumed a 0.25g peak base acceleration value rather than the SSE value of 0.17g. This discrepancy was encountered at several places in the calculations, which suggests that some of the analysts believed that the plant had been originally designed for an SSE ground acceleration value of 0.25g.

In summary, the median capacity of 0.64g and the combined logarithmic standard deviation value of 0.30 are both low. These values are considerably lower than values for similar components in the Zion and Indian Point PRAs.

Demineralization Water Storage Tank (sliding)

The design capacity factor, FCSD, for sliding is equal to 2.0, which is based on the incipient sliding friction failure between the bottom of the 10-foot thick base mat and the fill concrete placed against the rock foundation. The calculation is based on a sliding coefficient of friction of 1.0 and resistance provided by the compacted earth fill against the base mat. The value of 1.0 is conservative even for incipient sliding. Apparently the applied force due to the SSE earthquake is an absolute sum combination of the two horizontal components. A traditional-type incipient sliding analysis was performed; however, it is unlikely that the tank foundation will slide very far, even for an earthquake with accelerations greater than the median capacity.

The variability logarithmic standard deviation value of 0.1 for capacity is low. It is based on the assumption that a coefficient of friction value of 1.0 is 1.65 standard deviation below the mean value in the logarithmic domain (i.e., median equals 1.2). This is apparently an error because FCSD was based on a median value of 1.0. A more realistic value could be obtained from multiple nonlinear sliding analyses where uncertainty in the dynamic coefficient of friction is used to determine the uncertainty in response. The randomness component was included in the spectral shape randomness logarithmic standard deviation.

The uncertainty for the spectral shape was assumed to be zero. As discussed above for the Auxiliary building, this is not reasonable.

If the absolute sum of the two horizontal earthquake components was used as stated, then the earthquake combination safety factor appears to be correct. The logarithmic standard deviation value for randomness equal to 0.22 appears to be high as discussed above for the Auxiliary building.

In summary, the median capacity value of 0.68g is low, because the design capacity factor was based on a conservative incipient sliding analysis. A more realistic definition of failure should be used to correspond to actual failure conditions of interconnecting equipment. The combined variability logarithmic standard deviation value of 0.38 is low. Because of the uncertainties which are present, a higher value would be more reasonable.

Reactor Core Geometry

The seismic PRA analysis for the reactor core geometry was based on the Westinghouse stress analysis of the upper and lower reactor pressure vessel internals. The development of the equipment capacity safety factor, FCE, is conceptually correct; however, the Westinghouse stress analysis results were not available and the interpretation of these results and use in the seismic PRA analysis were not reviewed. However, the assumed median ductility value of 1.5 used in the analysis appears to be on the conservative side.

The reported equipment capacity factor variability value is 0.36. The corresponding value given in the calculations is 0.20, which does not agree with the report. The difference is probably due to the variability in ductility (0.35 was used for other components) which is not included in the calculations, but somehow was included in the report (however, a value closer to 0.40 in the report, rather than 0.36, would be more consistent with this explanation). The randomness values for material strength and ductility are incorrectly calculated (see discussion above for the steam generator example). The approach for determining the equipment capacity factor variability should be based on the variability in the models, material properties, and ductility ratios and their effect on the equipment capacity safety factor. The first item contributes to uncertainty and the last two to both uncertainty and randomness.

The equipment response factor, FRE, is assumed to be 1.0, since the final stresses were scaled to plant-specific spectral values in the Westinghouse calculation. The value of 1.0 is not correct. The value should be larger due to the difference between the envelope floor response spectra and assumed equipment damping values, and the corresponding median properties. It is likely that FRE is much larger than 1.0 because of these effects.

The reported equipment response factor variability is 0.41. The corresponding value given in the calculations is 0.26, which does not agree with the value of 0.41 given in the report. The uncertainty component was derived generically to include 0.09 for damping and 0.10 for the effect of material properties on dynamic response. The damping term should be obtained specifically for this component since this factor is sensitive to the frequency of the component and the corresponding floor response spectra (i.e., greater variability occurs near spectral peaks).

Also, it is not clear whether the uncertainty value of 0.09 is due to damping or due to the effects of damping variability on response (see discussion above for the Steam Generator). The randomness component is based on a value of 0.22 for spectral shape and 0.05 for the effects of material properties on dynamic response. The latter value was assumed generically, and the basis for the former value is not known, but probably is the same as the corresponding spectral shape value for the building. In addition, there should be randomness included for damping and combination of earthquake components. Also, modeling errors (i.e., frequency and mode shape) and modal combination effects are apparently not included.

The structural response safety factor, FRS, is reported to be 2.00. This value can be separated into the contribution from spectral shape (i.e., 1.5) and combination of earthquake components (i.e., 1.3). The latter factor is incorrect and should be 1.0, since the equipment was designed based on an SRSS combination of earthquake components.

The reported structure response factor variability is 0.42, which agrees with the value in the calculations. A logarithmic standard deviation value of zero was assumed for the effect of damping randomness, which is low; however, the corresponding value of 0.22 used for combination of earthquake components is both high and not appropriate since this variability should be included only in the equipment response contributions. Also, the 0.17 value for modal contribution should not be used since the floor response spectra were probably obtained by a direct integration time-history analysis.

In summary, the median capacity of 0.68g is low primarily due to the unrealistically low value for the equipment response factor. The total variability logarithmic standard deviation reported is 0.67; however, the value in the calculations is 0.54. The latter value is more consistent with previous seismic PRAs, but it is not clear which is the better estimate.

Service Water Piping

The failure of the service water piping is assumed to be the same as the failure of the Engineering Safety Features (ESF) building. However, it is stated in the calculations that compressible material has been provided between the ESF building and the pipe line. No compressible material apparently has been provided between the Emergency Generator Enclosure (EGE) and the service water line. It is concluded in the calculations that the failure of the service water line is represented by the sliding fragility of the EGE (not the ESF building). Apparently there is a discrepancy between the calculations and the report; however, the difference is small.

As discussed above for the sliding failures of the various structures, incipient sliding does not imply immediate failure of the interconnecting components (e.g., service water line). The failure capacity is higher. Because these structures are embedded, it is unlikely that the relative sliding displacements will be significant at the median capacities which are given in the report.

Rocking of a structure such as a containment building can lead to problems for interconnecting piping (e.g., Zion seismic PRA). This is a more likely condition than a sliding-induced failure. This potential failure mode should have been considered in the fragility analysis of structures.

Engineered Safety Features Building (sliding)

The design capacity safety factor, FCSD, for sliding is equal to 2.4, which is based on the capacity of the ring girder in bending where it is assumed that the reinforcement is designed to allowable values. Based on this assumption, FCSD is equal to 2(1.1/0.9), where 2 is the ductility factor, 1.1 is the SSE load factor, and 0.9 is the code capacity reduction factor for bending. Note that the ductility factor was included in FCSD and not in the inelastic energy safety factor, as done for other structures.

It appears that a conservative approach was taken in the development of FCSD. First, it is likely that there is extra capacity in the ring girder which was neglected in the analysis. Second, sliding is also resisted by the contact between the foundation and the rock base. The dynamic coefficient of friction may be large due to irregularities at the foundation/rock interface. Even if the structure starts to slide, the amount of displacement and its effects on interconnected equipment is the important consideration for determining the median capacity value.

The uncertainty logarithmic standard deviation value of 0.20 for the capacity factor was determined generically as discussed above for the Auxiliary building. This value seems low for the sliding failure of the ESF building. Also, since the failure is controlled by the ring girder, randomness for the effect of variability in material properties and ductility should be included.

In developing the variability for the spectral shape safety factor, it was assumed that the uncertainty component is zero, which is similar to what was done in past seismic PRA studies. As discussed above for the Auxiliary building, this value is not reasonable.

The median safety factor for earthquake combination is equal to 1.3. As discussed below for the Emergency Generator Enclosure, this generic value should not be used. Instead a building-specific value should be developed. The logarithmic standard deviation value for randomness equal to 0.22 appears to be high.

In summary, both the median capacity of 0.74g and the combined logarithmic standard deviation of 0.39 appear to be low.

Emergency Generator Enclosure (sliding)

The design capacity safety factor, FCSD, for sliding is equal to 1.8, which is based on the incipient shear failure of the Basil till beneath the building. The capacity was obtained by conservatively reducing the normal force by the vertical earthquake component (corresponding to 0.17g) and multiplying this reduced force by the tangent of 40°, where 40° is the internal friction angle of the till. A small additional capacity was added to this result for the frictional force along the outside walls. This capacity was divided by the base shear due to the horizontal earthquake (probably due to only one component) to obtain the value of 1.8 for FCSD.

This is a conservative capacity factor corresponding to incipient sliding. Because the building is embedded approximately 15 feet, it is unlikely that it will slide very far even for an earthquake with accelerations greater than the calculated median capacity.

The basis for the uncertainty logarithmic standard deviation value of 0.1 for capacity is unknown. It may have been selected to be the same as the value used for the Demineralized Water Storage Tank. See discussion for this component above. This value seems very low.

The uncertainty for spectral shape was assumed to be zero. As discussed above for other buildings, this is not reasonable.

The combined earthquake safety factor, FRSE, value of 1.3 probably is incorrect since it appears that only one earthquake component was used to develop the capacity factor. The logarithmic standard deviation value for randomness equal to 0.22 appears to be high (see discussion for Auxiliary building).

In summary, the median capacity value of 0.75g is low, because the design capacity factor was based on incipient sliding. A more realistic definition of failure should be used to correspond to actual failure conditions of interconnecting equipment. The combined variability logarithmic standard deviation value of 0.37 is low. Because of the uncertainties which are present, a higher value would be more reasonable.

<u>Containment</u> (crane wall failure)

The design capacity safety factor, FCSD, for the containment is equal to 1.75 which is based on an analysis of the columns which support the crane wall (these columns are really wall segments 10 feet by 3 feet in plan and 25 feet high). The calculations which are provided are difficult to follow. The following inconsistencies were noted:

- The axial forces in the columns due to overturning moments were based on plane sections remaining plane. This may not be true.

- The interior walls at the center were neglected which biased the results to the conservative side.

- The maximum moment in the critical column was based on single curvature. Because of the relative dimensions, a fixed boundary condition at the top and bottom would be a more reasonable assumption. This would decrease the applied moment by a factor of 2.

- Because the critical column will be braced by other wall segments, the slenderness effects can be neglected.

- The analysis was performed using code-required strength reduction factors which biased the results to the conservative side.

Also, as the critical walls begin to fail the loads will be transferred to other walls. It is concluded that the FCSD value of 1.75 is overly conservative. A more detailed analysis should be conducted.

The uncertainty logarithmic standard deviation for strength failure of structures was assumed to be 0.20 for all buildings. It was not based on the uncertainty of the different strength prediction models, but was assumed based on values used for Zion and Oyster Creek PRAs (Refs. 1 and 2). Because of the possibility of load redistribution, this value is on the low side.

The randomness logarithmic standard deviation for material strength of the Containment building was based on the variability of individual materials (i.e., steel and concrete). The variability of the strength equation should have been used rather than the variability of the individual material strengths. However, the value of 0.14 which was assumed is reasonable.

The inelastic energy safety factor, FCSE, was assumed to be 1.0 since the column failure would be a compression failure. As discussed above, the analysis is overly conservative, and the failure mode may be tension or shear. It is likely that there is ductile capacity and FCSE should be greater than 1.0.

In developing the variability for the spectral shape safety factor, it was assumed that the uncertainty is zero, which is similar to what was done in past seismic PRA studies. As discussed above for the Auxiliary building, this value is not reasonable.

The analysis conducted for the Containment internal structure for the PRA combined the seismic effects by the SRSS method. Thus the earthquake components safety factor, FRSE, value of 1.3 is not appropriate. A value of 1.0 should have been used. As discussed above for the Auxiliary building analysis, the randomness logarithmic standard deviation for this safety factor is high (i.e., 0.22 was used).

In summary, the median capacity of 0.87g appears to be low. The combined logarithmic standard deviation of 0.47 may also be on the low side.

2.3 CLOSURE

The overall impression of the seismic fragility analysis is that the results are very conservative. The numerous conceptual and philosophical errors encountered produce a lack of confidence that the fragility analysis was properly performed. Although the amount of computations, as evidenced by the thickness of the calculation file (approximately eight inches thick), and the additional response spectra analyses performed for the seismic PRA indicate that considerable resources were expended; however, the final results are not consistent with the state-of-the-art.

Based on comparing the fragility results of the Millstone PSS with similar data from the Indian Point and Zion PRAs, it is judged that the median fragility estimates are a factor of 2 to 3 low. This estimate is speculative since an independent analysis has not been performed to confirm the reasonableness of the higher structure and equipment capacity values.

Although the variabilities (i.e., randomness and uncertainty) were obtained in an incorrect manner, the final results are consistent with results from other PRA studies. However, the uncertainty values for Millstone and other PRA studies are generally on the low side.

3.0 WIND

In Section 1.2.5 of the Millstone 3 PSS, it is concluded that wind does not contribute significantly to plant risk. The governing wind event at the Millstone site is the occurrence of severe tornados. In general, the effects of tornados, hurricanes, and extratropical cyclones (i.e., normal winter storms and thunderstorms) should be considered in the wind risk analysis. As discussed below, it is agreed that tornado effects, which potentially create much larger loads, do not contribute significantly to plant risk; thus, the effects of other wind loads are implicitly included.

It is stated that all Millstone Unit 3 safety-related structures are of reinforced concrete construction with wall thicknesses of at least two feet. Except for some of the Quench Spray system components, all other safety-related components are contained in safety-related structures (Ref. 9, Table 3.2-1).

Based on the analysis described in Section 1.2.5.1.1 of the Millstone 3 PSS, it is stated that the frequency of exceeding the design tornado wind speed of 360 mph is approximately 5.4x10^{-6} per year. It is believed that this value is very conservative as discussed below.

At the Indian Point site, which is approximately 100 miles away and which is in an area with higher tornado activity based on historic data, the mean maximum tornado wind speed at the 10^{-7} per year frequency level is 230 mph with an 80 percent confidence range of 170 to 340 mph (Ref. 1). Other independent point estimates for the Indian Point site at this frequency level are 236 mph and 200 mph (Ref. 3). Note that these results are significant since the reported mean rate of tornado occurrence in the Millstone Unit 3 PSS is 1.87x10^{-4} per square mile per year, which is lower than the value of 2.4x10^{-4} per square mile per year used in the Indian Point study (Ref. 1).

A recent technical paper by Twisdale gives velocity/frequency curves for four regions of the contiguous U.S. (Ref. 10). None of the curves extend beyond 300 mph. Finally, using an approach developed by Reinhold (Ref. 11), the mean frequency using a tornado occurrence rate of 1.87×10^{-4} per square mile per year was found to be less than 10^{-8} per year. It is concluded that the mean frequency of occurrence of tornados with maximum wind speeds equal to or greater than 360 mph is less than 10^{-8} per year.

On the capacity side of the problem, all safety-related structures are designed, using code procedures and allowable strength values, to resist wind speeds of 360 mph and associated tornado missiles. From a probabilistic viewpoint, the frequency of structural failure or missile-induced damage given a 360 mph tornado would be one to two orders of magnitude lower than the frequency of the tornado occurrence.

Because of the extremely low mean frequencies of failure (i.e., on the order of 10^{-9} to 10^{-10} per year), it can be safely concluded that tornado (and hence other lesser wind types) effects are not significant. Even considering the contribution of uncertainty it is unlikely that the effects of wind would contribute significantly to the plant risk.

4.0 EXTERNAL FLOODING

In Section 1.2.3 of the Millstone PSS, it is concluded that external flooding is an insignificant contributor to plant risk. Only two sources of external flooding are considered to potentially impact the Millstone site: tidal flooding and intense precipitation. Since there are no major rivers or streams in the vicinity of Millstone Point, river flooding and dam failure are not considered applicable to the site. Tsunamis are also excluded since there is an extremely low probability that these events will occur along the North Atlantic coast line.

The justification for excluding external flooding from the formal risk analysis is made on a qualitative basis. No formal probabilistic analysis was performed. Tidal flooding and intense precipitation are based on the effects of the Probable Maximum Hurricane (PMH) and the Probable Maximum Precipitation (PMP), respectively. No probability values are given; however, these events are judged to have a point estimate frequence of occurrence between 10^{-6} to 10^{-4} per year. This estimate is based on an approximate analysis using available hurricane hazard data in the vicinity of the Millstone site (Refs. 1 and 12).

The description of the calculations, which were conducted to obtain the maximum wave runup and standing wave height due to the PMH and the flood depth due to the PMP, are contained in the FSAR (Ref. 9). It is apparent from the description given that conservatisms were included in the calculations (e.g., the most severe combination of hurricane parameters were used to represent the PMH and the site yard drains were considered ineffective in the PMP analysis). However, the amount of additional conservatism is not known. It is not necessarily true that single extreme events are the only circumstances that contribute to the risk. Also, the PMH and PMP may be correlated since the PMP could be caused by the PMH.

In contrast to the seismic analysis, the external flooding analysis did not explicitly consider the uncertainty (which is large) in the underlying parameters and models. Even at the 100-year storm level, the coefficient of variation on water depth is expected to be approximately 0.2 to 0.3. Thus, the conclusion that external flooding has a very low frequency of occurrence is not convincing without some formal quantification of the hazard.

By including the effect of uncertainties in the external flood analysis, a distribution on the frequency of occurrence can be obtained. The present analysis implies that the frequency of flooding above the protected elevation is small. However, the margin of safety above the PMH and PMP design elevation is also small (less than 1 foot for the PMH and less than an inch for the PMP).

As an example, the point estimate for the PMH might be 10^{-5} per year; however, because of the large uncertainties that are present, there is a small but finite probability that the frequency of the PMH is 10^{-4} per year or larger. Similarly, it can be argued that there is a potential hurricane bigger than the PMH which could produce a wave runup which exceeds the water-tight elevation of 25.5 feet msl. The point estimate for this event might be on the order of 10^{-6} per year; however, due to uncertainty there also is a small but finite probability that it is 10^{-5} per year or larger. Proceeding in this manner, it can be shown that including uncertainty will result in a family of hazard curves which may increase the mean frequency of water depth above the value obtained using only a single point estimate value (i.e., the PMH). In order to evaluate the implications of a water level greater than 25.5 feet msl, it is necessary to either conservatively assume core melt or to develop event trees, fault trees, and equipment fragilities to systematically incorporate the unique features of the plant into the uncertainty analysis.

In summary, a formal analysis should be conducted which provides frequencies of occurrence and includes uncertainty in the external flood models and parameters. Because of the large uncertainties which exist for external flood, there is the possibility that the mean frequency of core melt is larger than 10^{-6}. In order to conclude that the contribution from external flooding is insignificant relative to other hazards, a complete statement of the probability distribution on frequency of occurrence should be provided.

5.0 CONCLUSIONS AND RECOMMENDATIONS

The following are conclusions based on the review of the Millstone PSS and recommendations for additional work which should be conducted. The information is given below for seismic, wind, and external flood hazards.

5.1 SEISMIC

Because of the very conservative assumptions and numerous errors which have been made, the fragility parameter values do not represent the results of a state-of-the-art analysis. The median ground acceleration values for the components which are significant contributors to the frequency of core melt are judged to be a factor of 2 to 3 low compared to similar components from other recent PRA studies. This estimate is speculative and was not confirmed in detail for the specific components. In contrast, the logarithmic standard deviations for randomness and uncertainty are generally consistent with results obtained from other PRA studies; although numerous errors (many which are compensating) were made in calculating the variabilities. The logarithmic standard deviations for uncertainty are on the low side; however, the effect of this bias is probably small on the final risk results.

Based on the findings of the review, the fragility parameters should be recalculated to eliminate the excessive conservatisms and to correct the errors which have occurred. The new fragility curves should be incorporated in the systems analysis and combined with the seismic hazard curves to produce more realistic distributions on frequency for core melt and other consequences.

Also, after the plant is completed a review should be conducted to determine if any non-safety related structures or components could fail, fall, and impact the safety-related items in the plant.

5.2 WIND

The conclusion in the Millstone PSS that wind effects do not contribute significantly to the risk of radiological consequences is reasonable. Because all safety-related structures have been designed to resist tornado loads and resultant missiles for wind speeds up to 360 mph, the minimum thickness of concrete walls and roofs is two feet. A point estimate frequency for this speed is on the order of 10^{-8} per year at the Millstone site. Failure of the concrete structures would be one to two orders of magnitude lower. Even incorporating the effects of uncertainties, wind hazard will not become a significant external event.

5.3 EXTERNAL FLOODING

The exclusion of external flooding as a significant event is based on qualitative arguments. No formal probabilistic analysis or even point estimate values are offered in defense of this conclusion.

An approximate analysis indicates that the PMH has a frequency of occurrence between 10^{-6} and 10^{-4} per year. If uncertainties are included, the risk of flood waters exceeding critical elevations may be significant. No information is given regarding the consequences (i.e., flooding-induced equipment fragilities or systems analysis) if the protected elevations are exceeded. In conclusion, there is no quantitative basis to conclude that external flooding is not a problem.

In order to provide a rational basis for judging whether external flooding is a significant contributor to off-site consequences, a formal probabilistic hazard analysis should be conducted which incorporates the uncertainties of the methods and parameters. If the probabilities of the frequencies of exceeding the protected elevations are significant, then fragility and systems analyses for flooding may be required.

REFERENCES

1. Pickard, Lowe, and Garrick, "Indian Point Probabilistic Safety Study," Prepared for Consolidated Edison Company of New York, Inc., and Power Authority of the State of New York, Copyright 1982.

2. Pickard, Lowe, and Garrick, "Zion Probabilistic Safety Study," Prepared for Commonwealth Edison Company, not dated.

3. Kolb, G. J., et al., "Review and Evaluation of the Indian Point Probabilistic Safety Study," Prepared for U.S. Nuclear Regulatory Commission, NUREG/CR-2934, December 1982.

4. Kennedy, R. P., C. A. Cornell, R. D. Campbell, S. Kaplan, and H. F. Perla, "Probabilistic Seismic Safety Study of an Existing Nuclear Power Plant," Nuclear Engineering and Design, North-Holland Publishing Company, 1980.

5. Wesley, D. A., R. D. Campbell, P. S. Hashimoto, G. S. Hardy, and R. P. Kennedy, "Conditional Probabilities of Seismic Induced Failures for Structures and Components for the Zion Nuclear Generating Station," Structural Mechanics Associates, Prepared for Pickard, Lowe, and Garrick, Inc., Irvine, California, 1980.

6. American Nuclear Society and the Institute of Electrical and Electronics Engineers, "PRA Procedures Guide," Vol. 1 and 2, U.S. Nuclear Regulatory Commission, NUREG/CR-2300, 1983.

7. Philadelphia Electric Company, "Limerick Generating Station Final Safety Analysis Report," 1983.

8. Nathan M. Newmark Consulting Engineering Services, "A Study of Vertical and Horizontal Earthquake Spectra," WASH-1255, Prepared for the U.S. Atomic Energy Commission.

9. Northeast Utilities Service Company, "Final Safety Analysis Report, Millstone Nuclear Power Station Unit 3," 1983.

10. Twisdale, L. A., and W. L. Dunn, "Probabilistic Analysis of Tornado Wind Risks," Journal of the Structural Division, ASCE, Vol. 109, No. 2, February 1983.

11. Reinhold, T. A., and B. Ellingwood, "Tornado Damage Risk Assessment," NUREG/CR-2944, Brookhaven National Laboratory, September 1982.

12. Batts, M. E. et al., "Hurricane Wind Speeds in the United States," NBS Building Science Series 124, National Bureau of Standards, May 1980.

APPENDIX C

REVIEW OF THE ORIGINAL
MILLSTONE UNIT 3 PROBABILISTIC SAFETY STUDY
SEISMIC FRAGILITY

by

John W. Reed

Martin W. McCann, Jr.

Prepared for

Lawrence Livermore National Laboratory

Livermore, California

May 4, 1984

TABLE OF CONTENTS

Page

1.0 INTRODUCTION.. 1-1

1.1 Scope.. 1-1

1.2 Overall Methodology.. 1-3

2.0 EARTHQUAKE CHARACTERISTICS EFFECTS ON FRAGILITY.................. 2-1

2.1 Effect of Earthquake Magnitude and Duration................ 2-1

2.2 Response Spectrum Shape.................................. 2-10

2.3 Velocity/Acceleration Relationship........................ 2-11

3.0 FRAGILITY ANALYSIS.. 3-1

3.1 General Comments.. 3-1

3.2 Review of Structure Fragilities............................ 3-5

3.3 Review of Component Fragilities............................ 3-10

4.0 CONCLUSIONS AND RECOMMENDATIONS.................................. 4-1

REFERENCES.. R-1

1. INTRODUCTION

Jack R. Benjamin and Associates, Inc. (JBA) was retained by Lawrence Livermore National Laboratory (LLNL) to perform a review of the fragility analysis of the structures and components at the Millstone Unit 3 Nuclear Power Station. The fragility analysis was performed by Structural Mechanics Associates (SMA) for Northeast Utilities Service Company (NUSCO) (Ref. 1). A previous review by JBA of the fragility analysis originally used in the Millstone Unit 3 Probabilistic Safety Study (referred to as the Millstone PSS) is documented in Reference 2. In regards to the original seismic fragility analysis, JBA recommended that the fragility parameters should be recalculated to eliminate excessive conservatisms and to correct errors which had occurred. In addition, it was recommended that after the plant is completed, a review should be conducted to determine if any non-safety related structures or components could fail, fall, and impact the safety-related items in the plant.

In response to the first recommendation, NUSCO retained SMA to perform a reanalysis of the seismic fragilities, which are documented in Reference 1. This report presents our review of the revised analysis.

1.1 SCOPE

Jack R. Benjamin and Associates, Inc. has performed similar reviews of the Indian Point Probabilistic Safety Study (IPPSS) (Ref. 3) and the Zion Probabilistic Safety Study (ZPSS) (Ref. 4). (See Reference 5 for the IPPSS review. The ZPSS has not been published.) Based on experience gained from the initial review of the Millstone PSS and the IPPSS and ZPSS reviews, the evaluation of Reference 1 was conducted in a short time period in order to quickly determine the adequacy and accuracy of the results and to make recommendations based on the findings. In contrast to the previous reviews of the IPPSS and ZPSS which consisted of an in-depth evaluation of each section and subsection, this review focused only on critical components and issues which may impact the results.

This review consisted of reviewing Reference 1 and studying the calculations provided by NUSCO which document the development of the fragility parameter values. The new fragilities were developed only for the safety-related structures and for components with median ground motion capacities less than 1.5g. Note that all capacities cited in this report are referenced at the free-field ground surface level. The results of the original analysis were used to screen the components and only the low capacity ones were selected for reanalysis. We agree that this is a reasonable approach since the original analysis is excessively conservative. However, it is implicitly assumed that components with median capacities greater than 1.5g do not contribute significantly to core melt or risk.

The revised hazard and systems analyses were not reviewed. It is assumed that the NRC will evaluate these analyses in their entirety. Because of the overlap between the fragility analysis and the hazard and systems analyses, Amendment 2 to the Millstone PSS was quickly read. Based on this reading, we question whether the 5.3 to 6.3 range on earthquake magnitude that is assumed in the fragility analysis in Reference 1 is realistic. The implications of a higher range is discussed in Chapter 2. Also, we do not believe that the systems fragility curves and the hazard curves have been properly integrated. The mean annual frequency of core melt value of 1.7×10^{-5} seems high. This concern was communicated to the NRC in a telephone conference call on April 19, 1984.

In Chapter 2, the effect of earthquake characteristics on fragility calculations is discussed. In this chapter, the effect of earthquake duration and magnitude are considered. This has been a troublesome philosophical (and practical) problem in previous PRA studies. The approach used in Reference 1 is different from other PRAs. An evaluation of the current approach in relationship to previous procedures for handling this issue is given. Also, the effect of using a site-specific response spectrum shape and the relationship between peak ground velocity and peak ground acceleration are discussed in Chapter 2. This latter issue is important to the structure sliding analyses and the resulting median capacities. In Chapter 3, the fragility analysis is addressed. General comments are given and the results of our review of specific structure and component fragilities are provided. Finally, Chapter 4 gives conclusions and recommendations based on the findings of our review.

1.2 OVERALL METHODOLOGY

The methodology used in Reference 1 to develop seismic fragility data is appropriate and adequate to obtain a realistic estimate of structure and component fragility. In general, we believe that more representative capacity values have been developed in the revised analysis as compared to the original fragility analysis. We have some specific concerns as discussed subsequently in this report.

As discussed in Chapter 3, some revisions to the methods have been made, which has improved the analysis approach. The following three issues have been considered in Reference 1 in a different manner as compared to past seismic fragility analyses. Comments concerning these issues are given below.

- Design and construction errors
- Lower-bound fragility cut-off
- Correlation between failure modes

Design and Construction Errors

The issue of design and construction errors is discussed in Reference 1. As in other PRAs, this type of error is not generally included in the fragility calculations. However, in contrast to other PRA reports, it is stated that there is the possibility that unidentified design and construction errors may exist which can affect the seismic capacity. This recognition is important, although not much data is available to explicitly incorporate this effect in the analysis. This is an important area which is in urgent need of research.

Lower-Bound Fragility Cut-Off

A mathematical procedure for establishing a lower-bound cut-off on fragility curves is given in Reference 1. The method is reasonable, but is based on engineering judgment without any data to support the values used. In Amendment 2 to the Millstone PSS, it is stated that components were eliminated from the systems analysis if the acceleration capacity at two standard deviations below the median capacity is greater than 0.8g. In Table 2.5.1-1A in Amendment 2 to the Millstone PSS, the 37th (last) component listed (i.e., the steam generator tubes rupture) is the only component which satisfies this criteria and hence could be eliminated. For the Millstone 3 reanalysis, this cut-off issue is not of any practical significance, since it appears not to have affected the analysis.

Correlation Between Failure Modes

The issue of correlation between failure modes is discussed in Reference 1. We have raised this issue in our review of past PRAs. Although correlation has been treated conservatively in the past, it is important not to ignore potential unconservative situations which may arise in future PRAs. It is stated in Reference 1 that consideration should be given to possible correlation between controlling seismically-induced failure modes. In a quick reading of Amendment 2 to the Millstone PSS, we saw no evidence that this issue had been considered. We trust that the NRC will investigate this concern as part of their review of the systems analysis.

These concerns and other general philosophical concerns from past PRA studies also apply to the Millstone PSS. Reference 5 discusses these issues in depth based on the review of the IPPSS. The reader is directed to Section 2 of Appendix A of Reference 5 for a general discussion of these concerns.

2. EARTHQUAKE CHARACTERISTICS EFFECTS ON FRAGILITY

2.1 EFFECT OF EARTHQUAKE MAGNITUDE AND DURATION

It has been generally recognized that the use of instrumental peak ground acceleration is an ineffective basis to predict the damage potential of earthquake ground motion. Other factors, such as the number of cycles and frequency content of ground motion are also important. As a result, an effort has been made by SMA to account for these additional factors in the development of seismic fragility curves for structures and equipment. As new PRAs are performed, SMA has attempted to improve the procedure to do this. The Millstone PSS is the most recent attempt to do this.

Background

As background to the review of the Millstone fragility analysis, a brief review is given of previous attempts to develop a damage effective ground motion parameter. This is an area of ongoing development, that is at times troublesome and difficult to understand.

The Zion (ZPSS) and Indian Point (IPPSS) PRAs (Refs. 3, 4) were the first attempt to define a damage effective ground acceleration which was applied in a seismic risk analysis of a nuclear power plant. In developing a damage effective acceleration, two steps were taken. First, an effective peak acceleration (EPA) was defined which was an acceleration value that could be used to scale a broad-band response spectrum (e.g,. WASH 1255 spectrum (Ref. 6)) such that the predicted spectral accelerations in the frequency range 2 to 10 Hz are consistent, in a median sense, with spectral levels of real earthquakes in the earthquake magnitude range of interest. As indicated in Reference 4, the EPA value is dependent on earthquake size. For small magnitude events, the EPA is significantly less than the instrumentally recorded peak acceleration (IPA). This is due partially to the fact that smaller magnitude earthquakes have narrow, peaked response spectra and short durations. For large magnitude events, which have a broad response spectrum shape, the effective peak acceleration would equal the IPA. Anchoring a broad-band response spectrum shape to an EPA provides an elastic response spectrum that is median centered in the 2 to 10 Hz frequency range.

To determine a median-centered, broad-band spectrum, SMA recommended in the Zion and Indian Point PRAs that the EPA be equal to

$$EPA = 1.25 * A_{3F} \tag{2.1}$$

where A_{3F} is the third-highest peak acceleration or sustained acceleration in a low-pass filtered acceleration record. Frequencies beyond 9 Hz were eliminated. Implied in equation 2.1 is the assumption that earthquakes that contribute to failure are small to moderate size events (i.e., $5.3 < M \leq 6.3$).

In the next step, the elastic response spectrum is modified to reflect its potential to damage structures or equipment with natural frequencies in the 2 to 10 Hz range. The basis for this second step is the fact that in order for damage to occur, a structure or equipment item must experience multiple cycles of response. Consequently, for small magnitude earthquakes that have relatively short durations, the expected amount of damage is small, and thus the elastic response level would be significantly reduced. For large magnitude events, which last longer, little or no modification is required, according to the Zion method.

In order to estimate the damage potential of earthquake ground motion, a damage effective acceleration was defined as,

$$A_D = \frac{EPA}{F}$$

$$= \frac{1.25}{F} * A_{3F} \tag{2.2}$$

where the factor F is a function of earthquake magnitude and duration, and the level or type of damage. The intent of the F factor is to account for the less damaging effects of small earthquakes by effectively reducing the intensity of ground motion that is input to a structure. At the time the Zion and Indian Point studies were done, only limited information on the possible values of F was available. It was felt by SMA that F would lie in the range of 1 to 3. Thus, a single value of 1.25, reported to be conservative, was used. This resulted in $A_D = A_{3F}$, and the need to shift the seismic hazard curves by a factor 1/1.25 to sustained acceleration values where they had been defined in terms of sustained peak accelerations.

With respect to the approach used in the ZPSS and IPPSS, a number of comments are given. First, the definition of effective peak acceleration is based on the use of a broad-band response spectral shape, which when anchored to the EPA gives the median spectral acceleration in the 2 to 10 Hz frequency range. For Zion and Indian Point, the median spectral shape in Reference 6 was used by SMA. As a result, the definition of EPA is strongly dependent on these factors, and would presumably change, if a different broad-band spectrum was used, or a different frequency range were considered. Estimates of EPA are therefore relative to these factors. If a magnitude-dependent spectral shape is used, the estimate of an EPA would be different. This is discussed later in this section.

In support of equation 2.1, SMA has reported the results of a study where the response spectra for twelve earthquakes were compared to WASH 1255 broad-band response spectra anchored to an EPA as defined in equation 2.1 (Ref. 7). Although the visual comparisons in Reference 7 appear convincing, statistical analyses were not conducted to empirically define an appropriate EPA relationship. There is an implied modeling uncertainty in this approach, since more realistic approaches could have been used to determine a definition of effective peak acceleration.

In comparing actual earthquake response spectra to broad-band spectra scaled by an EPA, the mean plus one standard deviation WASH 1255 amplification spectrum was used by SMA in their analysis (Ref. 7). It would have been more appropriate, in our opinion, to have used the median-centered amplification spectrum. As a result, there is some doubt in our minds as to the appropriateness of equation 2.1 to estimate an EPA, and thus there may be a bias in the 1.25 factor. The arguments given by SMA are less convincing without the benefit of a statistical analysis to support their conclusions.

From Reference 7 we note that the estimate of effective peak acceleration is explicitly defined for frequencies less than 8 Hz, while the Zion and Indian Point studies assume an applicable range of 2 to 10 Hz. This appears to be inconsistent.

Following the Zion and Indian Point studies, the Limerick Severe Accident Risk Assessment (Limerick SARA) was published (Ref. 8). In this study, the results of research work were used to revise the seismic risk model. Ground motion intensity was expressed in terms of effective peak acceleration and a broad-band response spectrum (Ref. 6). However, in performing the seismic risk calculations, the seismic hazard curves were shifted to convert from EPA to $A_D = A_{3F}$. Thus, an adjustment identical to that in the ZPSS and IPPSS was made, suggesting the F factor in equation 2.2 was again taken as 1.25.

However, in the Limerick SARA an Earthquake Duration factor of 1.4 was incorporated in the fragility analysis to account for the less damaging effects of small magnitude earthquakes. The earthquake duration factor has the effect of increasing structure capacities, when the size of the expected earthquakes is small, as opposed to decreasing the hazard, by the 1/F factor given in equation 2.2. It was concluded in our review (Ref. 9) with concurrence by SMA, that the F factor in equation 2.2 and the earthquake duration factor included in the fragility analysis accounted for the same phenomena, and therefore only one factor should be used. On this basis we conclude that for the methodology used in the Limerick SARA, the earthquake ground motion hazard is more appropriately characterized by the EPA as defined by equation 2.1, keeping in mind that the factor on A_{3F} is still a function of earthquake magnitude.

In summary, the F factor previously used to shift the accelerations in the seismic hazard analysis, was incorporated in the seismic fragility analysis for Limerick, as an earthquake duration factor. When the earthquakes that contribute to risk are small, then the duration factor serves to increase the capacity of structures, because of the less damaging effects of smaller, shorter duration earthquakes. The median value of this factor as used by SMA was 1.40 based on work reported in Reference 10. This represented an increase from the previous value of 1.25 used in ZPSS and IPPSS. In our review of the Limerick study (Ref. 9), we generally agreed with this approach, but felt the factor of 1.40 may be too high.

Generally speaking, the Limerick SARA study represented an improvement in the seismic risk analysis. Detailed comments on this method are provided in Reference 9.

Millstone PSS

The latest effort by SMA to establish a realistic ground motion characterization and seismic fragility model was performed for the Millstone PSS (Ref. 1). This approach is summarized below, followed by review comments. Based on the work reported in Reference 10, a procedure somewhat different from that used in previous PRAs was developed. In terms of the seismic hazard, peak ground acceleration was used to characterize the intensity of ground motion. In addition, a magnitude-dependent response spectrum shape, developed by LLNL (Ref. 11) was used, rather than the WASH 1255 broad-band spectrum. Discussion of the magnitude-dependent spectrum is given in the next section. A response spectrum shape corresponding to earthquakes with magnitudes 5.3 to 6.3 was selected, which according to the seismic hazard analysis in Appendix 1-B to Amendment 2 to the Millstone PSS was the range of earthquake magnitudes that contributed to accelerations around 0.17g, the SSE level. This is troublesome, since the accelerations that contribute to the mean frequency of core melt appear to be much higher. Whether it can be assumed that earthquakes of this size are the dominant contributors to failure, is discussed later.

As discussed above in regards to the ZPSS and IPPSS, the characterization of effective ground acceleration was defined relative to the frequency range of interest, a WASH 1255 broad-band spectra, and earthquake magnitude. In the case of Millstone, rather than using a broad-band spectrum, a magnitude-dependent spectrum was selected. As a result, the definition of effective peak acceleration used in ZPSS and IPPSS no longer applies. Instead, the effective peak acceleration for a median-centered, magnitude-dependent response spectrum is the instrumental peak acceleration. To understand this, recall that in the case where a broad-band spectrum is used, if large earthquakes are dominant contributors to risk, then the EPA used to scale the spectrum shape is equivalent to the IPA. This will be the case since the response spectra of large magnitude events are also broad-band. The same analogy can be made when a magnitude-dependent spectrum is used. We therefore agree that peak ground acceleration is the appropriate parameter to characterize strong ground motion for the Millstone seismic analysis.

In previous PRAs the effect on seismic capacity of earthquake magnitude and duration was accounted for by shifting the seismic hazard curve (e.g., ZPSS and IPPSS) or increasing the seismic capacity relative to an EPA value (e.g., Limerick SARA). Based on research conducted by SMA (Ref. 10), larger magnitude earthquakes that have longer durations and thus produce many cycles of structure response, will exhibit less ductility at failure than smaller events with short durations, and lower levels of ground shaking intensity. In Reference 10, the available or effective ductility in single-degree-of-freedom systems of various frequencies subjected to earthquake ground shaking was calculated. The results of this study provided the basis to estimate an Inelastic Energy Absorption factor of safety, based on an effective ductility and the Riddell-Newmark formula. The effective ductility, μ^*, is estimated to account for the influence of earthquake magnitude and duration. In this approach, the following formulation was used by SMA:

$$\mu^* = 1.0 + C_D \, (\mu - 1.0) \tag{2.3}$$

where the factor C_D is a function of earthquake magnitude and   is the structure ductility ratio. For earthquakes in the range 4.5 to 6.0, C_D was given as 1.4, suggesting the effective ductility is higher for small magnitude events. For large earthquakes, C_D = 0.70, which gives a lower effective ductility.

As indicated earlier, the magnitude range 5.3 to 6.3 was assumed to make the greatest contribution to risk, thus a C_D value of 1.3 was assumed. This value was subjectively selected to reflect the slightly higher magnitudes that are expected. A quantitative basis was not given to support this value.

A brief review was conducted to assess the adequacy of the analysis procedure used in Reference 1, and to evaluate the parameters used in the analysis. Overall, the approach used in the Millstone PSS represents an improvement over past PRAs. Based on a preliminary review of the Inelastic Energy Absorption factor, F , with the incorporation of magnitude/duration effects, a number of questions or concerns are raised. In addition to Sections 4.1.2 and 4.1.2.1 of the fragility analysis report (Ref. 1), we also reviewed SMA's supporting calculations and Reference 10.

The C_D factor in equation 2.3 was developed from data reported in Reference 10 for two magnitude ranges: 4.5 to 6.0 and 6.5 to 7.5. In addition, two structure ductilities of 1.85 and 4.27 were considered. SMA calculated C_D equal to 1.40 for the lower magnitude earthquakes and 0.70 for the larger events. We attempted to reproduce the C_D values SMA calculated for each magnitude range/ductility pair and were unable to do so. In one case, our estimate of C_D varied considerably from that of SMA, while in other cases small differences occurred. From the four estimates of C_D, a value for each magnitude range was used in the report. It is not clear from the calculations how the final values of C_D of 1.40 and 0.70 were determined. They are not strict averages within each magnitude range, but appear to be subjectively chosen.

Of greater concern is the frequency dependence exhibited by the data in Reference 10. Based on a preliminary assessment, we observe that depending on the natural frequency of the structure, C_D will vary at low frequencies, from a value greater than 1.0, implying greater effective ductility, to less than 1, or less effective ductility, for higher frequency structures. This observation is independent of both magnitude and ductility ratio. Intuitively, this appears reasonable since we expect a structural system to respond in an oscillatory manner, consistent with its natural frequency, in an earthquake. As a result, it is reasonable to expect that high frequency structures and components will experience many more cycles of response than structures with lower natural frequencies for the same amplitude and duration of ground motion input. Consequently, lower effective ductilities for higher frequency structures are anticipated. This can have a significant impact on the estimate of the effective ductility. It should be noted that the total impact of this observation is dependent on magnitude and the ductility ratio. To illustrate this relationship we estimate that for structures with natural frequencies of 2.14 Hz and ductilities of 1.85 and 4.27, C_D should be greater than 1.0 for large magnitude earthquakes, as opposed to 0.70 as suggested by SMA.

As a general concern, only 10 earthquake records were used to estimate the C_D values in the Millstone PSS. This is a relatively small sample set to effectively estimate the magnitude/duration dependence of C_D. This is apparent in the fact that the entire magnitude range is not fully represented (i.e., magnitudes 6.0 to 6.5 are not included, and only two large magnitude ranges could be considered). In addition, for an earthquake of a given magnitude, there is considerable variability in the duration of ground motion that can be expected (Ref. 12). As a result, the true variability in C_D is large. Consequently, we feel the available data set provided in Reference 10 is not adequate to fully characterize an effective ductility.

To estimate the variability for the inelastic energy absorption factor, F , it was assumed that there is a 1% chance of F being less than 1 for C_D = 0.70. On this basis, an estimate of β_C, the composite variability was derived by SMA. In principal, we do not agree with this approach to estimating variabilities since it suggests that the assumed lognormal distribution is correct and can be used to prescribe what the variability <u>ought</u> to be. Furthermore, it tends to combine the notions of randomness and uncertainty, which in principal are different. However, we recognize the problems encountered in estimating variabilities, including a lack of data to estimate β_R and the concern that unreasonable frequencies of failure are estimated by the lognormal model at low ground accelerations. As a result, the analyst attempts to constrain the model by fixing the lower tail. In some ways, the engineer is forced to live with the lognormal model and the unrealistic values it predicts, particularly when there is large uncertainty, β_U, in his estimate. This is one example where the lognormal model breaks down by being overly conservative. In general we feel that the engineer should utilize the available data and his judgment to estimate β_R and β_U separately.

An important assumption made in the fragility analysis is that the earthquakes which are dominant contributors to core melt are in the magnitude range 5.3 to 6.3. It is reported in the seismic hazard analysis that accelerations around 0.17g are produced by earthquakes of about magnitude 5.6. However, the chance of core melt may be dominated by accelerations greater than 0.70g. Of greater importance is to know the size of earthquakes that contribute to these levels of ground shaking. Results for the Limerick PRA indicate that the average magnitude will consistently increase for increasing acceleration. As a result, we expect that the average earthquake magnitude that contributes to plant risk may be 6.0 or greater. This would suggest that the duration of ground shaking will be longer than is assumed in the fragility analysis. Thus, the available ductility will be less. Similarly, the magnitude-dependent response spectrum shape which is applicable in the 5.3 to 6.3 magnitude range may not be appropriate.

Conclusion

1. We agree that the magnitude-specific response spectrum should be anchored to IPA.

2. The effective ductility is an appropriate concept, but in addition to depending on magnitude it is also frequency-dependent. We recommend that the dependence of the effective ductility on the natural frequency of structures be taken into account. This influence may have a significant effect on the effective ductility for structures and components with h~~igh natural frequencies.~~

3. If the average magnitude of earthquakes which contribute to risk are greater than 6.3; then effective ductilities will be lower and a different response spectrum shape should be used.

2.2 RESPONSE SPECTRUM SHAPE

In the Millstone PRA, a magnitude-dependent response spectrum shape was used to characterize the intensity of ground motion. This step is a change from other PRAs where a broad-band spectral shape has been used. When using a magnitude-dependent response spectrum the definition of effective peak acceleration changes as a more realistic spectral shape is considered. In this section we review the response spectra and compare it to other spectra available for the site. An evaluation of the site spectra with respect to its influence on the fragility analysis was conducted. It is our understanding that the NRC is performing a critical review of the seismic hazard analysis, including the magnitude-dependent spectrum.

The response spectrum shape for earthquake magnitudes in the range 5.3 to 6.3 developed in Reference 11 for rock sites was used. Figure 2-1 shows this spectra with the Millstone design spectra for 10 percent damping. The procedure described in Reference 11 to convert the 5 percent damped spectrum to 10 percent damping was useo. Each spectrum in the figure is scaled to 0.17g, the SSE level. Also shown in the figure is the WASH 1255 broad-band response spectrum.

In addition to these spectra, LLNL (Ref. 13) has conducted a new seismic hazard analysis for the Millstone site. In Figure 2-1, the 1000 year return period spectral shape scaled to 0.17g is shown.

Based on the comparison in Figure 2-1 we find that the magnitude-dependent spectra are generally higher than the design spectra for frequencies greater than 5 Hz. Among these, the most recent spectra developed by LLNL has the highest spectral level. At frequencies less than 5 Hz, the design spectrum exceeds the site-specific spectrum, with the greatest variations occurring at frequencies less than 2 Hz.

In comparison to the WASH 1255 broad-band spectra, the LLNL site-specific spectra both have higher spectral levels at frequencies beyond 5 Hz. In the 2-5 Hz region, the WASH 1255 is higher.

The impact of these spectra on the fragility analysis are summarized in Table 2-1 in terms of their ratio to the Millstone design spectra, for frequencies corresponding to the Control Building, Auxiliary Building, the Containment Crane Wall, Emergency Generator Enclosure, and the Engineering Safety Features Building. These results indicate that the latest spectrum developed by LLNL has considerably higher spectral levels than the Millstone design spectra.

2.3 VELOCITY/ACCELERATION RELATIONSHIP

As part of the seismic fragility analysis for structures (e.g., Control Building) and equipment items (e.g., DWST), the resistance to sliding was evaluated. In predicting sliding displacements due to ground shaking an approximate approach developed by Newmark was used. In Chapter 3, comments are provided on the analysis technique itself. In this section, comments are given on the ground motion characterization aspects of the sliding analysis, as described in Sections 4.1.1.7 and 4.1.1.8 of the SMA fragility report (Ref. 1).

Briefly, the Newmark approach predicts the amount of sliding displacement due to a single acceleration pulse. Based on the relative displacement that is needed to cause failure of buried piping, a relationship was derived to estimate the capacity in terms of peak ground acceleration (e.g., equation 4-9 in the fragility analysis report). Equation 4-9 relates the sliding displacement to the coincident ground velocity and ground acceleration. Based on peak ground motion estimates made by Newmark (Ref. 6), a relationship between peak ground velocity (PGV) and peak ground acceleration of 28 in/sec/g was assumed. From this, the sliding displacement was expressed in terms of peak ground acceleration.

From a review of Reference 6, the 28 in/sec/g ratio was based on four horizontal ground motion records at two stations during the 1971 San Fernando earthquake. The use of only two stations from the same earthquake in our opinion is inadequate. Also, the use of the two horizontal components from a single station is inappropriate, since these acceleration traces are correlated. SMA used these four data points to estimate the variability of the PGV/g ratio and thus is equally inappropriate. To establish an estimate of the median acceleration capacity corresponding to a displacement limit, the peak ground velocity is assumed to occur in the same cycle as the peak acceleration. In general, this is not the case, although the PGV may occur near the PGA within a few cycles. In fact, the joint occurrence of ground accelerations and velocities is random, thus there is a distribution of possible velocity/acceleration pairs that can occur.

Because of the different ground motion attenuation properties between the eastern and western U.S. it is not clear that waveforms expected in the east will have the same characteristics as those in the west. This is particularly true for large magnitude, distant events that could produce high velocities and low accelerations.

As part of this review, data for rock sites in the western U.S. reported in Reference 13 were used as the basis to estimate a peak ground velocity to acceleration ratio. For a total of 15 data points, the estimated mean value was 24.6 in/sec/g with a corresponding logarithmic standard deviation of 0.39. This compares to the 28 in/sec/g mean value and 0.31 standard deviation used by SMA.

As a further comparison, the results of the LLNL probabilistic seismic hazard analysis for Millstone (Ref. 11) were used to estimate a PGV/PGA ratio for annual frequencies of $5\text{x}10^{-3}$, $1\text{x}10^{-3}$ and $2.5\text{x}10^{-4}$. For these three values, a mean value of 64.6 in/sec/g was obtained. Although this estimate is considerably higher than the value used in the PRA, it should be noted that this is not an entirely appropriate comparison. The hazard analysis for PGA and PGV were conducted independently, therefore the correlation between PGA and PGV was not preserved. However, this result indicates a possible upper bound.

In our opinion, the value of 28 in/sec/g used in the PRA is reasonably consistent with data recorded in the western U.S. However, it is recommended that this value be looked at from the perspective of the expected ground motion in the east. We also feel the variability in this factor is underestimated.

TABLE 2-1. SPECTRAL RATIOS (10 Percent Damping)

Building	Frequency (Hz)	WASH 1255 MDS	SS(OLD)* MDS	SS(NEW) MDS
Control Building	8.3	1.08	1.20	1.40
Auxiliary Building	8.8	1.08	1.25	1.46
Containment Crane Wall	5.5	0.90	0.97	1.19
Engineering Safety Features Building	12.8	1.18	1.29	1.82
Emergency Generator Enclosure	9.0	1.0	1.30	1.57

* SS = LLNL Magnitude-Specific Spectrum

MDS = Millstone Design Spectra

Note: SS(OLD) is the spectrum used in the fragility analysis.

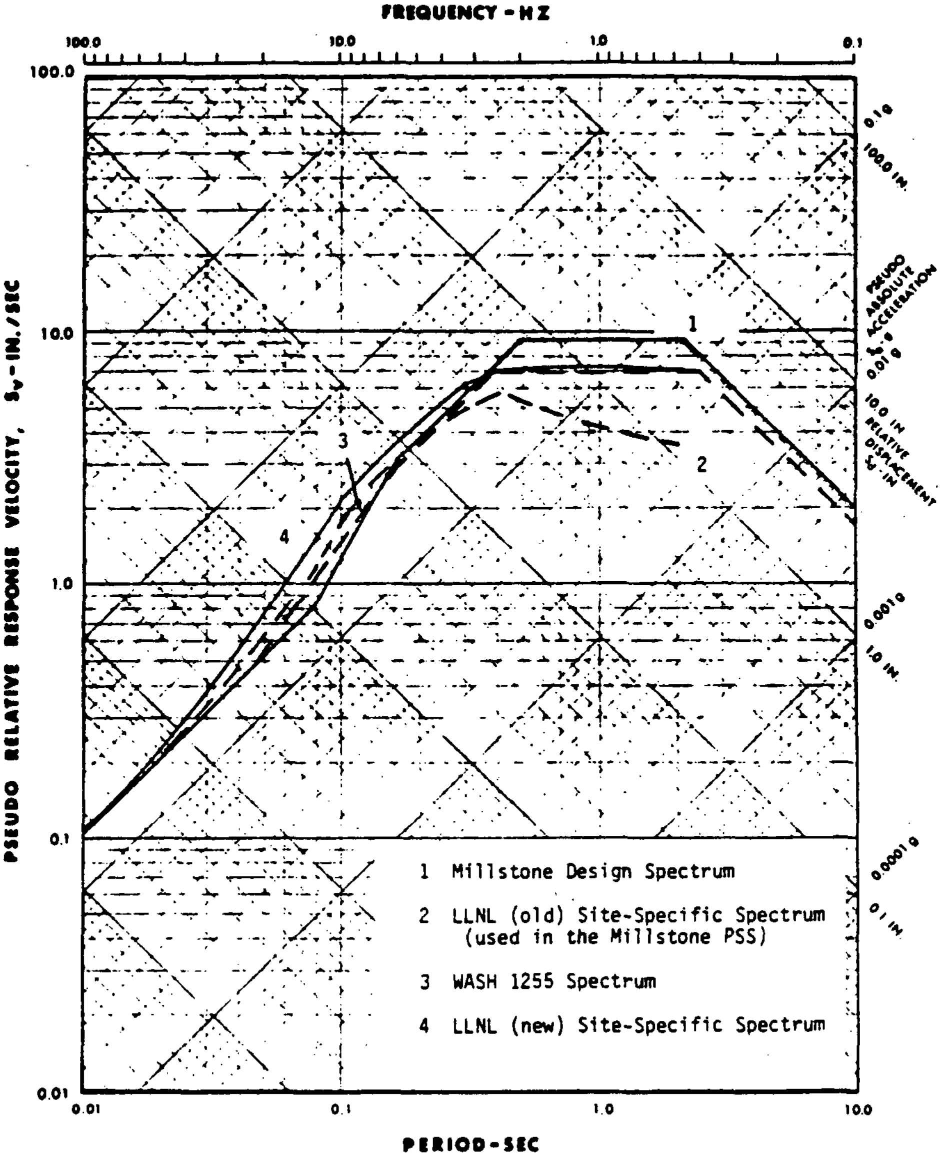


FIGURE 2-1. MILLSTONE RESPONSE SPECTRA FOR 10% DAMPING

3. FRAGILITY ANALYSIS

The focus of the review of the fragility analysis contained in Reference 1 was directed to the critical components which are significant contributors to the Millstone PSS. Based on information provided by the NRC and NUSCO, the following ten structures and components were reviewed.

Structures

- Emergency Generator Enclosure
- Pumphouse
- Control Building
- Engineering Safety Features Building
- Containment Crane Wall

Components

- 4160 V Switchgear
- Service Water Piping
- Emergency Diesel Generator
- RPV Core Geometry
- Control Rod Drive Mechanisms

The review of each of these structures and components is discussed in Sections 3.2 (structures) and 3.3 (components). Section 3.1 gives general comments on the fragility analysis.

3.1 GENERAL COMMENTS

The structure capacity calculations are generally more detailed than previous calculations performed for seismic PRA studies. Except for the Emergency Generator Enclosure, new response spectrum dynamic analyses of the major safety-related structures were performed for the seismic PRA study. The original models developed for the plant design were modified to reflect median properties. Based on a review of the PRA calculations, evidence of the model properties being checked was found. In some cases (discussed below) the models were changed to reflect the correct properties. The median response spectrum assumed in the seismic PRA was used as input to the models, which eliminated the uncertainty of extrapolating from the design analyses for the structures. Note that new floor response spectra were not developed; hence, the fragility analyses for components were performed similar to past PRAs.

Forces from the dynamic analysis were generally distributed to walls using the computer program WALLDI (SMA proprietary program) which is based on the stiffness characteristics and geometry of the structural elements. Both the new dynamic analysis and the force distribution step are improvements over previous PRA studies, where forces were generally obtained based only on the original design analysis results. This new approach reduces uncertainty and should lead to more realistic results (although the logarithmic standard deviations for uncertainty are as large or larger compared to corresponding values in previous PRAs).

In contrast to previous seismic PRAs, more systematic checking of structural elements (i.e., shear walls and diaphragms) was performed. This provides confidence that the critical strength sections have been found. Effects of soil pressure on buried walls was considered; although, the capacity of these walls was not found to be critical.

Sliding analyses were performed for the safety-related structures. In general, both incipient sliding and displacement sliding capacities were determined. It was assumed for cases where sliding is not restricted that a 4-inch displacement corresponds to failure of interconnecting piping. The basis for this criterion is not known. A reference to page DT-48 is given in the calculations for the Emergency Generator Enclosure; however, pages DT-39 through D-57 have been deleted from the Demineralized Water Storage Tank calculations. The basis for the 4-inch displacement value should be justified and reviewed.

An approximate procedure developed by Newmark was used to compute the sliding displacement capacity. Resistance to sliding includes friction between the base mat and foundation, shear keys, and side wall-to-soil friction. Reduction for the effects of the vertical earthquake component and buoyancy due to water were also included.

The Newmark approximate procedure is claimed to be conservative. A quick comparison of the approach with results from nonlinear time history sliding analyses indicates that it gives conservative results for a single sliding excursion. However, due to multiple sliding excursions, which may not be evenly balanced to each side of the starting position, a net drift displacement may occur. In some cases we have found that displacements using an "exact" approach exceed the values obtained from the Newmark procedure. The potential for drift is earthquake magnitude dependent. Since the sliding capacities were calculated to be larger than 1g median, the associated earthquakes are likely to come from large magnitude, long duration events, and hence there will be time for multiple excursions to occur.

An important assumption made in the sliding analysis is the relationship between peak ground acceleration and peak ground velocity. It was assumed in the seismic PRA that 1g corresponds to 28 in/sec. As discussed in Chapter 2, this value may not be appropriate for the Millstone site. Note that the sliding displacement is proportional to the velocity raised to a power between 1 and 2, depending on the size of the vertical earthquake component.

Table 1 lists the coefficients of friction assumed in the analysis. These values were not reviewed in detail, although they appear to be reasonable.

The inclusion of the vertical earthquake component likely produces conservative results. For the 4-inch displacement considered in the sliding analysis, the time during which sliding will occur is approximately 0.3 seconds. In this time period the vertical component may reverse direction several times and its effect on horizontal sliding would be minimal.

In conclusion, there appears to be conservatisms and unconservatisms which tend to balance out. However, we recommend that the velocity to acceleration ratio be verified by the NRC since this assumption will have a major impact on the sliding capacities. Also, justification should be given that a 4-inch sliding displacement corresponds to the median capacity for buried piping.

The calculations for the component fragility values appeared to be more organized and consistent (i.e., between components) compared to similar calculations in previous PRAs. Based on our review, we have differences of opinion on several aspects of the component fragility analysis as discussed below. As discussed in Section 3.3, we found several small errors.

Factors of safety for earthquake component combinations were developed generically and are listed in Table 5-3 of Reference 1. Development of these factors is a complicated task and other engineers are likely to produce values different from those given in Table 5-3. We attempted to develop these factors directly ourselves and found that we disagree only slightly. However, one exception is the F_{ECC} value of 1.25 for Case 4 for the second design condition in Table 5-3 (corresponding to the situation when the SRSS value of the responses from the two horizontal directions was combined absolutely with the vertical component in the original design). Note that this design condition apparently applies only to balance of plant piping since the median SRSS rule was used for all other components. We calculate a value of 1.15 for this factor which is about 10 percent lower than the value of 1.25 given in Table 5-3.

In regards to the multi-directional effects factor for testing, we obtain correction factors that are approximately 10 percent lower for bi-axial testing (i.e., 0.77 compared to 0.853) and 13 percent lower for uniaxial testing (0.64 compared to 0.735). This difference is statistically small since there is considerable uncertainty that the methods for computing these factors (i.e., ours and theirs) are exact.

In contrast to the development of fragility values for structures, the uncertainty in response due to uncertainty in frequency is treated generically with logarithmic standard deviation values (which also include uncertainty in the mode shape) that vary from 0.10 to 0.20. This parameter should be developed specifically for each component as is done for structures. In situations where the median component frequency is close to a structure's natural frequency, the variability in response can be large due to uncertainty in the relative relationship between the two frequencies.

The ductility adjustment factor discussed in Chapter 2 for structures also has been applied to components in Reference 1. This is the first time that capacities of components have been modified for the effects of a duration or a ductility factor. In general, the same comments given for structures also apply to components.

3.2 REVIEW OF STRUCTURE FRAGILITIES

The results of the review of the fragility calculations for the Emergency Generator Enclosure, Pumphouse, Control Building, Engineering Safety Features Building, and Containment Crane Wall are given below.

Emergency Generator Enclosure

The following elements were analyzed for the Emergency Generator Enclosure:

- Sliding of the entire building
- Wall footing
- Slab at elevation 24 feet
- Roof slab
- Shear walls (in-plane and out-of-plane)
- Diesel generator pedestal stability

The inertial forces used in the analysis were developed from the original design analysis which consisted of a soil-structure interaction model, and no new dynamic analyses were performed. Forces were distributed to walls using the program WALLDI developed by SMA. This structure is relatively stiff with a fundamental frequency near 9 Hz.

Sliding analyses were conducted to determine the incipient sliding capacity (i.e., 0.31g median) and the capacity corresponding to a 4-inch displacement (i.e., 1.30g median). The resistance against sliding included friction between the soil and the footings and side walls using a coefficient of friction equal to 0.55 (this is based on coarse grain soil containing no clay or silt) and the shear capacity of the soil enclosed between the buried walls. The effect of the vertical earthquake component was conservatively included in the analysis. The 4-inch displacement criterion corresponds to failure of buried piping as discussed above. The sliding analysis was based on the Newmark approximate approach and is subject to the limitations as also pointed out above.

The footings which support the EW direction walls span between the north wall footing and the vault base mat were the critical structural elements. Friction between the soil and footings was used to provide part of the resistance. Apparently a conservative coefficient of friction of 0.45 was used (compared to 0.55 used for sliding of the entire building). The footing capacity was found to be 0.88g, which appears to be on the conservative side.

Pumphouse

The following elements were analyzed for the Pumphouse:

- Sliding of the entire building
- Shear walls (in-plane and out-of-plane)
- Diaphragm (at elevation 14 feet)

A dynamic analysis of the Pumphouse using the basic properties developed in the original design (i.e., masses, stiffnesses, and geometry) was performed by SMA. Forces were distributed to the walls using the program WALLDI. This structure is relatively stiff with fundamental frequencies of 9.5 Hz and 14.8 Hz in the EW and NS directions, respectively.

Sliding analyses were conducted to determine the incipient sliding capacity (i.e., 0.48g median) and the capacity corresponding to a 4-inch displacement (i.e., 1.30g median). Only sliding in the westward direction is considered possible (in the other directions either the structure is keyed into or butts against rock). Only friction between the concrete mat and the foundation was assumed to resist sliding. A coefficient of friction equal to 1.1 was used, which was an average value for concrete on excavated rock or raked concrete fill (i.e., coefficient equal to 1.2) and concrete on intact rock (i.e., coefficient equal to 1.0). Similar to the sliding analysis for the Emergency Generator Enclosure, a 4-inch displacement criterion was assumed and the sliding capacity was calculated using the Newmark approximate approach. However, it was noted that a 1-inch displacement capacity was assumed at minus two standard deviations below the median, which is different from the corresponding value of 2 inches assumed in the sliding analysis for the Emergency Generator Enclosure. This is a minor inconsistency.

The exterior shear walls were analyzed for both in-plane loads and out-of-plane fluid and soil loads. The single north wall is the weakest wall corresponding to a median capacity of 1.6g. The diaphragm at the pump support level was also analyzed and found to have a median capacity of 1.5g. The critical section near the north wall contains numerous openings which controls the diaphragm capacity.

No mention of the capacity of the roof slab was found. This slab also has numerous openings. In contrast to the crib house roof slab at Zion, which was a critical component, the in-plane forces in the diaphragm at Millstone are resisted by buttresses on the intake side of the building. Thus it is unlikely that the roof slab will be a significant contributor.

Control Building

The following elements were analyzed for the Control Building:

- Sliding of the entire building
- Diaphragm

- Roof slab
- Shear walls
- Block walls

A dynamic analysis of the Control Building was performed by SMA. They found that the structural mass was about 30 percent larger than the mass used in the original design analysis. This was explained by construction changes made since the original analysis was conducted. Forces were distributed to the walls using the program WALLDI. This structure is relatively stiff with fundamental frequencies of 8.9 Hz and 8.3 Hz in the EW and NS directions, respectively.

Analyses were conducted to determine the incipient sliding capacity (i.e., 0.43g median) and the capacity corresponding to a 2-inch displacement (i.e., 1.2g median). A 2-inch displacement criterion was used because of potential impact with the turbine building. Shear keys add additional capacity, which explains in part the 1.2g capacity for only a 2-inch displacement. (Note that other structures have a 1.3g capacity for a 4-inch displacement criterion.)

The shear walls were analyzed for in-plane loads. Their capacities are higher than the 1.0g median capacity for the diaphragm at elevation 64'-6" which is controlled by a section with numerous openings adjacent to the west exterior wall. A systems ductility ratio of only 1.3 was assumed, which seems conservative.

The block walls adjacent to critical safety-related equipment were analyzed. These walls are reinforced and supported by a steel frame. A dynamic analysis of a critical panel was conducted by SMA and found to have a 2.0g median capacity.

Engineering Safety Features Building

The following elements were considered for the Engineering Safety Features Building:

- Sliding of the entire building
- Diaphragm
- Shear walls

A dynamic analysis of the Engineering Safety Features Building was performed by SMA using the basic properties developed in the original design (i.e., masses, stiffnesses, and geometry). Slight discrepancies were found by SMA regarding the center of rigidity and induced torsional forces. Modifications were made to the model. Forces were distributed to the walls using the program WALLDI. This structure is very stiff with a fundamental frequency of 12.8 Hz.

The strength of various shear walls and the critical diaphragm section were analyzed and the capacities were found to exceed 2.0g median ground acceleration for these failure modes.

The potential for sliding was considered for this building. In three of the four directions it was argued that sliding was not a realistic failure mode. In the west direction (i.e., toward the containment), an incipient sliding analysis was performed. Because of the high resulting capacity, only the shear key and support provided by the adjacent containment base mat were assumed to provide resistance. The high buoyant force and vertical acceleration component eliminated the friction capacity between the soil and base mat. This portion of the analysis appears to be on the conservative side.

Because the incipient sliding capacity was found to be high (i.e., 1.7g median), no sliding displacement analysis was performed.

Containment Crane Wall

A dynamic analysis of the Containment Building was performed by SMA using the basic properties developed in the original design. Median properties and seismic input were used to obtain gross forces acting on the internal structures. A refined model of the internal structures including the crane wall elements was developed by SMA. Forces from the dynamic analysis were applied statically to the model. As each element reached its yield capacity the model was modified, and an additional incremental load was applied until the maximum resistance was obtained. A system ductility ratio of 3 was assumed in the analysis.

The capacity of the crane wall was determined to be 2.2g median ground acceleration. This is considerably higher than the 0.87g capacity calculated in the original analysis. The revised value is more realistic.

3.3 REVIEW OF COMPONENT FRAGILITIES

The results of the review of the fragility calculations for the 4160 V Switchgear, Service Water Piping, Emergency Diesel Generator, RPV Core Geometry, and the Control Rod Drive Mechanisms are given below.

4160 V Switchgear

Both relay chatter and relay trip failure modes were developed for the 4160 V Switchgear, which is located on the base mat in the Control Building (i.e., elevation 4'-6"). The relay chatter median capacity of 0.88g is based on the assumption that chatter will occur at a level 20 percent higher than the qualification level (based on judgment). The uncertainty logarithmic standard deviation for this estimate is only 0.08. A value between 0.2 and 0.4 is probably more appropriate. We also disagree slightly with the median factors of safety assumed for earthquake components and building response spectral shape. In conclusion, we estimated the median relay chatter capacity to be 0.85 (compared to 0.88g) with logarithmic standard deviation for randomness and uncertainty to be 0.26 and 0.47, respectively (compared to 0.29 and 0.40, respectively in the SMA report).

The relay trip capacity is based on generic data developed from the Army Corps of Engineers shock tests. The extrapolation of this data to seismic fragility values has been recently questioned (Ref. 15). However, the capacity for this mode is relatively high (i.e., 3.09g median). In addition, a very large logarithmic standard deviation for uncertainty has been used (i.e, 0.81). It is unlikely that the median capacity for this failure mode is less than 1.5g; although, this conclusion is speculative and not based on any data.

Service Water Piping

The critical failure mode for the service water piping is displacement failure caused by sliding of the connecting buildings. Capacities of the piping within the buildings is relatively high and failure in the ground due to wave passage effects in the surrounding soil is unlikely at accelerations in the range of potential sliding failures. The analyses of the sliding failure mode for the various safety-related structures are discussed in Section 3.2.

It is our understanding that a concrete wall retains soil through which the service water piping pass between the pumphouse and the plant. Failure of this wall may lead to failure of the adjacent piping. A fragility analysis should be conducted for this wall.

Emergency Diesel Generator

The capacity of the Emergency Diesel Generator is controlled by the strength of the lube oil cooler anchor bolts. This component is located in the Emergency Generator Enclosure at elevation 24'-6". We are unable to confirm the reasonableness of the fragility calculations since the seismic stress report (Ref. 16) was not provided with the package of calculations. This reference is needed to verify the fragility parameter values.

The soil-structure interaction (SSI) factor of safety was assumed to be 1.3. The basis for this value is not given. Since the diesel generators are supported on their own foundations separate from the Emergency Generator Enclosure, a separate design analysis was performed for them. We speculate that SMA obtained a copy of this analysis and judged that the modeling of SSI resulted in a factor of safety of 1.3. We have no other basis to determine whether this value is reasonable.

RPV Core Geometry

The upper support plate was determined to be the weakest element in the RPV core. A total of seven potential failure modes were evaluated. It was assumed in the analysis that the code allowable stress corresponds to failure. This assumption acknowledges that the faulted design values allow significant inelastic deformation. Since deflection limits are not included, it is assumed by SMA that inelastic deformation does not constitute a functional failure and that Westinghouse has demonstrated satisfactory control rod insertion at the allowable loads. The only increase incorporated in the strength factor is the difference between median properties and nominal values used in the design (i.e., a factor between 1.20 and 1.25).

In developing the structural response factors a factor of safety is developed for the difference between the median ground response spectrum and the response spectrum used in the original design. A spectral value of 0.51g was used for the original design value (corresponding to 4.7 Hz at 5 percent damping). Based on Figure 3.7B-6 of the Millstone Nuclear Power Station Unit 3 FSAR the value is approximately 0.45g. This difference lowers the median ground acceleration capacity to 0.87g instead of 0.99g. No other significant differences were found for this component.

Control Rod Drive Mechanisms

Bending in the control rod was determined to be the weakest element in the Control Rod Drive Mechanisms. Similar to the upper support plate in the RPV, the allowable stress was assumed to be the failure stress. An increase of 25 percent was included to reflect the difference between median properties and the nominal values used in the design.

The same apparent mistake made in determining the structural response factor for the RPV Core Geometry (see discussion above) was also made for this component. If the spectral value is corrected, the median capacity is 0.88g instead of 1.00g.

TABLE 3-1. COEFFICIENTS OF SLIDING FRICTION ASSUMED IN THE SEISMIC AREA

Condition	Coefficient
Concrete against soil with silt and clay	0.45
Concrete against soil without silt and clay	0.55
Smooth concrete against smooth concrete	0.80
Concrete poured against rough concrete	1.00
Foundation against intact rock	1.00
Foundation against excavated rock or raked concrete	1.20

4. CONCLUSIONS AND RECOMMENDATIONS

Based on review of Reference 1 and the supporting calculations we generally believe that the revised fragility parameter values are realistic. However, we have found various problems which may affect the results of the risk analysis. We recommend that the NRC investigate the impact of these problems on the resulting frequency of core melt and other risk consequences. From the results of our review we recommend the following.

1. NUSCO should provide justification that a 4-inch displacement corresponds to the median capacity of buried piping. This justification should be reviewed by the NRC.

2. The NRC should determine if the range of earthquakes contributing to the risk analysis are greater than magnitude 5.3 to 6.3. If this is the case, then the effective ductility ratios will be lower and a different response spectrum shape should be used. This will result in lower median capacity values.

3. Because the structures at Millstone have high natural frequencies, the dependence of the Inelastic Energy Absorption factor on frequency should be incorporated into the analysis. NUSCO should revise their Inelastic Energy Absorption factor estimates to reflect the frequency characteristics of the structures. For estimation purposes, a lower bound on the Inelastic Energy Absorption factor is 1.0.

4. The NRC should determine if the site-specific spectrum used in the fragility analysis is appropriate. See Table 2-1 and Figure 2-1 for a comparison of different response spectra.

5. The NRC should investigate the correlation between failure modes to determine if it significantly affects the risk analysis.

6. The NRC should determine if the velocity to acceleration ratio of 28 in/sec/g is a representative median value for the Millstone site. If the value is significantly higher, then the structure sliding capacities should be reevaluated. A conservative bounding assumption is that the median capacity is inversely proportional to the square of the velocity to acceleration ratio.

7. Table 4-1 lists revised fragility values based on our review. The impact of these values on risk should be investigated by the NRC. These values do not include adjustment for the effects of larger earthquake magnitudes, the effects of the dependency of the Inelastic Energy Absorption factor on the frequency of structures, or the effects of site-specific spectra (see Nos. 2, 3, 4 above).

8. NUSCO should provide Reference 2 and the fragility analysis for the Emergency Diesel Generator should be reexamined in light of this information.

9. NUSCO should perform a fragility analysis for the concrete wall which retains soil through which the service water piping passes from the pumphouse to the rest of the plant.

10. As recommended in our first review (Ref. 2), a study should be conducted after the plant is completed to determine if any non-safety related structures or components could fail, fall, and impact the safety-related items in the plant.

TABLE 4-1. REVISED FRAGILITY PARAMETER VALUES

Component/Parameter	Revised Values	Reference 1 Values
4160 V Switchgear (Chatter Failure Mode)		
Median	0.85g	0.88g
β_r	0.26	0.29
β_u	0.47	0.40
RPV Geometry		
Median	0.87g	0.99g
Control Rod Drive Mechanism		
Median	0.88g	1.00g

REFERENCES

1. Wesley, D. A., et al., "Seismic Fragilities of Structures and Components at the Millstone 3 Nuclear Power Station," Prepared for Northeast Utilities, Structural Mechanics Associates Report No. SMA 20601.01-R1-0, March 1984.

2. Reed, J. W., "Review of the Millstone Unit 3 Probabilistic Safety Study--Seismic Fragility, Wind, and External Flooding," Prepared for Lawrence Livermore National Laboratory, December 22, 1983.

3. Power Authority of the State of New York and Consolidated Edison Company of New York, Inc., "Indian Point Probabilistic Safety Study, Units 2 and 3," Dockets 50-247 (Unit 2) and 50-286 (Unit 3), March 5, 1982.

4. Commonwealth Edison Company, "Zion Nuclear Plant Units 1 and 2 Probabilistic Safety Study," Dockets 50-295 (Unit 1) and 50-304 (Unit 2), September 8, 1981.

5. Kolb, G. J., et al., "Review and Evaluation of the Indian Point Probabilistic Safety Study," Prepared for U.S. Nuclear Regulatory Commission, NUREG/CR-2934, December 1982.

6. Newmark, N. M., "A Study of Vertical and Horizontal Earthquake Spectra," WASH 1255, Nathan M. Newmark Consulting Engineering Services, prepared for U.S. Atomic Energy Commission, April 1973.

7. Kennedy, R. P., W. H. Tong, S. A. Short, "Earthquake Design Ground Acceleration Versus Instrumental Peak Ground Acceleration," prepared for Nathan M. Newmark Consulting Engineering Services, Structural Mechanics Associates Report No. SMA 12501.01R, December 1980.

8. Philadelphia Electric Company, Limerick Generating Station Severe Accident Risk Assessment, 1983.

9. M. A. Azarm, et al., "A Preliminary Review of the Limerick Generating Station Severe Accident Risk Assessment, Volume I: Core Melt Frequency," Engineering and Risk Assessment Division, Department of Nuclear Energy, Brookhaven National Laboratory, 1984.

10. R. P. Kennedy, et al., "Engineering Characterization of Ground Motion Effects of Characteristics of Free-Field Motion on Structural Response," SMA 12702.01, prepared for Woodward-Clyde Consultants, 1983.

11. Bernreuter, D. L., "Seismic Hazard Analysis Application Methodology, Results and Sensitivity Studies," U.S. Nuclear Regulatory Commission, NUREG/CR-1582, UCRL-53030, Vol. 4, October 1981.

12. McGuire, R. K., and T. P. Barnhard, "The Usefulness of Ground Motion Duration in Predicting the Severity of Seismic Shaking," Proceedings of the 2nd U.S. National Conference on Earthquake Engineering, Stanford University, August 22-24, 1979.

13. Bernreuter, D. L., J. B. Savy, R. W. Mensing, D. H. Chung, "Seismic Hazard Characterization of the Eastern United States: Methodology and Interim Results for Ten Sites," U.S. Nuclear Regulatory Commission, NUREG/CR-3756, UCRL-53527, Draft, April 1984.

14. Joyner, W. B. and D. M. Boore, "Peak Horizontal Acceleration and Velocity from Strong Motion Records Including Records from the 1979 Imperial Valley California Earthquake," Bulletin of the Seismological Society of America 71, December 1981.

15. Kana, D. D, and D. J. Pomerening, "The Use of Fragility in Seismic Design of Nuclear Plant Equipment," Prepared for U.S. Nuclear Regulatory Commission, Southwest Research Institute Report No. SWRI-6582-004, March 1984.

16. Colt Industries Operating Corporation, "Seismic Analysis For Emergency Diesel Generator Systems, Millstone Unit No. 3 of NUSCO," Fairbanks Morse Engine Div., Analytical Engineering Dept., Approved by Stone & Webster Engineering, B. A. Bolton, February 14, 1979.

NRC FORM 335
(2-84)
NRCM 1102,
3201, 3202

U.S. NUCLEAR REGULATORY COMMISSION

BIBLIOGRAPHIC DATA SHEET

SEE INSTRUCTIONS ON THE REVERSE.

1. REPORT NUMBER *(Assigned by TIDC, add Vol. No., if any)*

NUREG/CR-4142

2. TITLE AND SUBTITLE

A Review of the Millstone 3 Probabilistic
Safety Study

3. LEAVE BLANK

4. DATE REPORT COMPLETED

MONTH	YEAR
December	1985

5. AUTHOR(S) A. Garcia, D. Bernreuter, T. McKone, P. Smith (LLNL), P. Amico (Applied Risk Technology Corporation), J. Reed, M. McCann, Jr (Jack R. Benjamin & Associates Inc.), P. Davis and G. Apostolakis (Consultants).

6. DATE REPORT ISSUED

MONTH	YEAR
April	1986

7. PERFORMING ORGANIZATION NAME AND MAILING ADDRESS *(Include Zip Code)*

Lawrence Livermore National Laboratory
7000 East Avenue
Livermore, CA 94550

8. PROJECT/TASK/WORK UNIT NUMBER

9. FIN OR GRANT NUMBER

FIN A-0447

10. SPONSORING ORGANIZATION NAME AND MAILING ADDRESS *(Include Zip Code)*

Division of Safety Technology
Office of Nuclear Reactor Regulation
U. S. Nuclear Regulatory Commission
Washington, D. C. 20555

11a. TYPE OF REPORT

Final

b. PERIOD COVERED *(Inclusive dates)*

12. SUPPLEMENTARY NOTES

13. ABSTRACT *(200 words or less)*

Lawrence Livermore National Laboratory (LLNL) has conducted a review of the Millstone Unit 3 (MP 3) Probabilistic Safety Study (PSS) for the Office of Nuclear Reactor Regulation, U.S. Nuclear Regulatory Commission (NRC). This probabilistic safety study was performed by Northeast Utilities (NU) in response to a 1981 request from the NRC. The objective of LLNL's review was to review those aspects of the MP 3 PSS leading to estimates of the plant core damage frequency. LLNL estimated core damage frequency from internal events at MP 3 to be about 1×10^{-4} per year. LLNL reviewed major areas of the PSS, including initiating events, event trees, success criteria, fault trees, human factors, component and operating experience data, and treatment of uncertainty. The review of external events included earthquakes, fires, external and internal flooding, extreme winds, aircraft accidents, hazardous materials, and turbine missiles. The MP 3 PSS treated external events, other than seismic and fire, in a cursory manner. LLNL's seismic review effort was curtailed by the staff because of ongoing seismic analysis revisions by NU.

14. DOCUMENT ANALYSIS – a. KEYWORDS/DESCRIPTORS

PRA, Probabilistic Risk Assessment, Probabilistic Safety Study, Core melt frequency, Millstone 3, Small Break LOCA, RHR LOCA, Internal Events.

b. IDENTIFIERS/OPEN-ENDED TERMS

15. AVAILABILITY STATEMENT

unlimited

16. SECURITY CLASSIFICATION

(This page)
unclassified

(This report)
unclassified

17. NUMBER OF PAGES

18. PRICE

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555

OFFICIAL BUSINESS
PENALTY FOR PRIVATE USE, $300

260