U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

U.S. NRC Level 3 Probabilistic Risk Assessment (PRA) Project

Volume 3a: Reactor, At-Power, Level 1 PRA for Internal Events

Part 1 – Main Report

This report, though formatted as a NUREG report, is currently being released as a draft (non-NUREG) technical report for comment.

Office of Nuclear Regulatory Research

AVAILABILITY OF REFERENCE MATERIALS IN NRC PUBLICATIONS

NRC Reference Material

As of November 1999, you may electronically access NUREG-series publications and other NRC records at the NRC's Public Electronic Reading Room at http://www.nrc.gov/reading-rm.html. Publicly released records include, to name a few, NUREG-series publications; *Federal Register* notices; applicant, licensee, and vendor documents and correspondence; NRC correspondence and internal memoranda; bulletins and information notices; inspection and investigative reports; licensee event reports; and Commission papers and their attachments.

NRC publications in the NUREG series, NRC regulations, and Title 10, "Energy," in the *Code of Federal Regulations* may also be purchased from one of these two sources.

1. **The Superintendent of Documents**
   U.S. Government Publishing Office
   Mail Stop SSOP
   Washington, DC 20402-0001
   Internet: http://bookstore.gpo.gov
   Telephone: 1-866-512-1800
   Fax: (202) 512-2104

2. **The National Technical Information Service**
   5301 Shawnee Road
   Alexandria, VA 22161-0002
   http://www.ntis.gov
   1-800-553-6847 or, locally, (703) 605-6000

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

U.S. Nuclear Regulatory Commission
Office of Administration
Publications Branch
Washington, DC 20555-0001
E-mail: distribution.resource@nrc.gov
Facsimile: (301) 415-2289

Some publications in the NUREG series that are posted at the NRC's Web site address http://www.nrc.gov/reading-rm/doc-collections/nuregs are updated periodically and may differ from the last printed version. Although references to material found on a Web site bear the date the material was accessed, the material available on the date cited may subsequently be removed from the site.

Non-NRC Reference Material

Documents available from public and special technical libraries include all open literature items, such as books, journal articles, transactions, *Federal Register* notices, Federal and State legislation, and congressional reports. Such documents as theses, dissertations, foreign reports and translations, and non-NRC conference proceedings may be purchased from their sponsoring organization.

Copies of industry codes and standards used in a substantive manner in the NRC regulatory process are maintained at—

The NRC Technical Library
Two White Flint North
11545 Rockville Pike
Rockville, MD 20852-2738

These standards are available in the library for reference use by the public. Codes and standards are usually copyrighted and may be purchased from the originating organization or, if they are American National Standards, from—

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

Legally binding regulatory requirements are stated only in laws; NRC regulations; licenses, including technical specifications; or orders, not in NUREG-series publications. The views expressed in contractor-prepared publications in this series are not necessarily those of the NRC.

The NUREG series comprises (1) technical and administrative reports and books prepared by the staff (NUREG-XXXX) or agency contractors (NUREG/CR-XXXX), (2) proceedings of conferences (NUREG/CP-XXXX), (3) reports resulting from international agreements (NUREG/IA-XXXX), (4) brochures (NUREG/BR-XXXX), and (5) compilations of legal decisions and orders of the Commission and Atomic and Safety Licensing Boards and of Directors' decisions under Section 2.206 of NRC's regulations (NUREG-0750).

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

U.S. NRC Level 3 Probabilistic Risk Assessment (PRA) Project

Volume 3a: Reactor, At-Power, Level 1 PRA for Internal Events

Part 1 – Main Report

Manuscript Completed: March 2022
Date Published: April 2022

Prepared by:
C. Hunter[1]
J. Schroeder (retired)[2]
D. Helton[1]
S. Cooper[1]
S. Shen[1]
A. Kuritzky[1]
M. Drouin[1]
K. Coyne[1]
J. Nakoski[1]

[1]U.S. Nuclear Regulatory Commission

[2]Idaho National Laboratory
Idaho Falls, ID 83415

A. Kuritzky, NRC Level 3 PRA Project Program Manager

Office of Nuclear Regulatory Research

ABSTRACT

The U.S. Nuclear Regulatory Commission (NRC) performed a full-scope site Level 3 probabilistic risk analysis (PRA) project (L3PRA project) for a two-unit pressurized-water reactor reference plant, responding to Commission direction in the staff requirements memorandum (SRM) (Agencywide Documents and Management System [ADAMS] Accession No. ML112640419) resulting from SECY-11-0089, "Options for Proceeding with Future Level 3 Probabilistic Risk Assessment (PRA) Activities" (ADAMS Accession No. ML11090A039).

As described in SECY-11-0089, the objectives of the L3PRA project are to:

- Develop a Level 3 PRA, generally based on current state-of-practice methods, tools, and data,[1] that (1) reflects technical advances since the last NRC-sponsored Level 3 PRAs (NUREG-1150[2]), which were completed over 30 years ago, and (2) addresses scope considerations that were not previously considered (e.g., low power and shutdown [LPSD] risk, multi-unit risk, other radiological sources)

- Extract new insights to enhance regulatory decision making and to help focus limited NRC resources on issues most directly related to the agency's mission to protect public health and safety

- Enhance PRA staff capability and expertise and improve documentation practices to make PRA information more accessible, retrievable, and understandable

- Demonstrate technical feasibility and evaluate the realistic cost of developing new Level 3 PRAs

The scope of the L3PRA project encompasses all major radiological sources on the site (i.e., reactors, spent fuel pools, and dry cask storage), all internal and external hazards, and all modes of plant operation. Fresh nuclear fuel, radiological waste, and minor radiological sources (e.g., calibration devices) are not included as part of the scope. In addition, deliberate malevolent acts (e.g., terrorism and sabotage) are excluded from the scope of this study.

This report, one of a series of reports documenting the models and analyses supporting the L3PRA project, specifically addresses the reactor, at-power, Level 1 PRA model for internal events for a single unit. The analyses documented herein are based information for the reference plant as it was designed and operated as of 2012 and does not reflect the plant as it is currently designed, licensed, operated, or maintained.[3]

---

[1] "State-of-practice" methods, tools, and data refer to those that are routinely used by the NRC and industry or have acceptance in the PRA technical community. While the L3PRA project is intended to be a state-of-practice study, note that there are several technical areas within the project scope that necessitated advancements in the state-of-practice (e.g., modeling of multi-unit site risk, modeling of spent fuel in pools or casks, and of human reliability analysis for other than internal events and internal fires).

[2] NUREG-1150, "Severe Accident Risk: An Assessment for Five U.S. Nuclear Power Plants," December 1990.

[3] An overview report, which covers all three PRA levels, has been created for each major element of the L3PRA project scope (e.g., for the combined internal event and internal flood PRAs for a single reactor unit operating at full power). These overview reports include a reevaluation of plant risk based on a set of updated plant equipment and PRA model assumptions (e.g., incorporation of the current reactor coolant pump shutdown seal design at the

A full-scope site Level 3 PRA for a nuclear power plant site can provide valuable insights into the importance of various risk contributors by assessing accidents involving one or more reactor cores as well as other site radiological sources. Furthermore, some future advanced light water reactor (ALWR) and advanced non-light water reactor (NLWR) applicants may rely heavily on results of analyses similar to those used in the L3PRA project to establish their licensing basis and design basis by using the Licensing Modernization Project (LMP) (NEI 18-04, Rev. 1) which was recently endorsed via RG 1.233. Licensees who use the LMP framework are required to perform Level 3 PRA analyses. Therefore, another potential use of the methodology and insights generated from this study is to inform regulatory, policy, and technical issues pertaining to ALWRs and NLWRs.

CAUTION: While the L3PRA project is intended to be a state-of-practice study, due to limitations in time, resources, and plant information, some technical aspects of the study were subjected to simplifications or were not fully addressed. As such, inclusion of approaches in the L3PRA project documentation should not be viewed as an endorsement of these approaches for regulatory purposes.

reference plant and the potential impact of the U.S. nuclear power industry's proposed safety strategy, called Diverse and Flexible Mitigation Capability [FLEX], both of which reduce the risk to the public).

FOREWORD

The U.S. Nuclear Regulatory Commission (NRC) performed a full-scope site Level 3 probabilistic risk analysis (PRA) project (L3PRA project) for a two-unit pressurized-water reactor reference plant, responding to Commission direction in the staff requirements memorandum (SRM) (Agencywide Documents and Management System [ADAMS] Accession No. ML112640419) resulting from SECY-11-0089, "Options for Proceeding with Future Level 3 Probabilistic Risk Assessment (PRA) Activities" (ADAMS Accession No. ML11090A039).

Licensee information used in performing the Level 3 PRA project was voluntarily provided based on a licensed, operating nuclear power plant. The information provided reflects the plant as it was designed and operated as of 2012 and does not reflect the plant as it is currently designed, licensed, operated, or maintained. In addition, the information provided for the reference plant was changed based on additional information, assumptions, practices, methods, and conventions used by the NRC in the development of plant-specific PRA models used in its regulatory decisionmaking. **As such, use of L3PRA project reports to assess the risk from the reference plant is not appropriate and these reports will not be the basis for any regulatory decision associated with the reference plant.**

Each set of L3PRA project reports covering the Level 1, 2, and 3 PRAs for a specific site radiological source, plant operating state, and hazard group is accompanied by an overview report. The overview reports summarize the results and insights from all three PRA levels.

In order to provide results and insights better aligned with the current design and operation of the reference plant, the overview reports also provide a reevaluation of the plant risk based on a set of new plant equipment and PRA model assumptions and compare the results of the reevaluation to the original study results. This reevaluation reflects the current reactor coolant pump (RCP) shutdown seal design at the reference plant, as well as the potential impact of FLEX strategies,[4] both of which reduce the risk to the public.

A full-scope site Level 3 PRA for a nuclear power plant site can provide valuable insights into the importance of various risk contributors by assessing accidents involving one or more reactor cores as well as other site radiological sources (i.e., spent fuel in pools and dry storage casks). These insights may be used to further enhance the regulatory framework and decisionmaking and to help focus limited agency resources on issues most directly related to the agency's mission to protect public health and safety. More specifically, potential future uses of the Level 3 PRA project can be categorized as follows (a more detailed list is provided in SECY-12-0123, "Update on Staff Plans to Apply the Full-Scope Site Level 3 PRA Project Results to the NRC's Regulatory Framework," dated September 13, 2012):

- enhancing the technical basis for the use of risk information (e.g., obtaining updated and enhanced understanding of plant risk as compared to the Commission's safety goals)

- improving the PRA state-of-practice (e.g., demonstrating new methods for site risk assessments, which may be particularly advantageous in addressing the risk from

[4] FLEX refers to the U.S. nuclear power industry's proposed safety strategy, called Diverse and Flexible Mitigation Capability. FLEX is intended to maintain long-term core and spent fuel cooling and containment integrity with installed plant equipment that is protected from natural hazards, as well as backup portable onsite equipment. If necessary, similar equipment can be brought from offsite.

advanced reactor designs, or in supporting the evaluation of the potential impact that a multi-unit accident, or an accident involving spent fuel, may have on the efficacy of the emergency planning zone in protecting public health and safety)

- identifying safety and regulatory improvements (e.g., identifying potential safety improvements that may lead to either regulatory improvements or voluntary implementation by licensees)

- supporting knowledge management (e.g., developing or enhancing in-house PRA technical capabilities)

In addition, the overall Level 3 PRA project model can be exercised to provide insights with regard to other issues not explicitly included in the current project scope (e.g., security-related events or the use of accident tolerant fuel). Furthermore, some future advanced light water reactor (ALWR) and advanced non-light water reactor (NLWR) applicants may rely heavily on the results of analyses similar to those used in the L3PRA project to establish their licensing basis and design basis by using the Licensing Modernization Project (LMP) (NEI 18-04, Rev. 1) which was recently endorsed via RG 1.233. Licensees who use the LMP framework are required to perform Level 3 PRA analyses. Therefore, another potential use of the methodology and insights generated from this study is to inform regulatory, policy, and technical issues pertaining to ALWRs and NLWRs.

The results and perspectives from this report, as well as all other reports prepared in support of the Level 3 PRA project, will be incorporated into a summary report to be published after all technical work for the Level 3 PRA project has been completed.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ABBREVIATIONS AND ACRONYMS

AC	alternating current
ACC	accumulator
ACCW	auxiliary component cooling water
ACRS	Advisory Committee on Reactor Safeguards
ADAMS	Agencywide Documents Access and Management System
AFW	auxiliary feedwater
AMSAC	anticipated transient without scram mitigation system actuation circuitry
ANS	American Nuclear Society
AOP	abnormal operating procedure
ARV	atmospheric relief valve
ASEP	Accident Sequence Evaluation Program
ASME	American Society of Mechanical Engineers
ATWS	anticipated transient without scram
CBDT	Cause-Based Decision Tree
CCCG	common cause component group
CCF	common-cause failure
CCP	centrifugal charging pump
CCU	containment cooling unit
CCW	component cooling water
CDF	core damage frequency
CSFST	critical safety function status tree
CST	condensate storage tank
CVCS	chemical and volume control system
DC	direct current
EB	Empirical Bayes
ECCS	emergency core cooling system
EDG	emergency diesel generator
EDMG	extensive damage mitigation guidance
EF	error factor
EOP	emergency operating procedure
EPRI	Electric Power Research Institute
ESF	engineered safety features
ESFAS	engineered safety features actuation system
FTLR	fail to load/run
FTR	fail to run
FTS	fail to start
FV	Fussell-Vesely
gpm	gallons per minute
HCR	Human Cognitive Reliability

HEP	human error probability
HFE	human failure event
HLR	hot-leg recirculation
HPI	high-pressure injection
HPR	high-pressure recirculation
HRA	human reliability analysis
HVAC	heating, ventilation and air conditioning
IA	instrument air
IEEE	Institute of Electrical and Electronic Engineers
INPO	Institute of Nuclear Power Operations
ICES	INPO Consolidated Events Database
ISLOCA	interfacing system loss-of-coolant accident
kV	kilovolt
L3PRA	Level 3 probabilistic risk assessment (project)
LLOCA	large loss-of-coolant accident
LOCA	loss-of-coolant accident
LOOP	loss of offsite power
LPI	low-pressure injection
LPR	low-pressure recirculation
MDP	motor-driven pump
MOV	motor-operated valve
MCC	motor control center
MFIV	main feedwater isolation valves
MFW	main feedwater
MLOCA	medium loss-of-coolant accident
MSIV	main steam isolation valve
MSPI	mitigating systems performance index
NCP	normal charging pump
NIS	nuclear instrumentation system
NPSH	net positive suction head
NRC	Nuclear Regulatory Commission
NSCW	nuclear service cooling water
ORE	Operator Reliability Experiments
PORV	power-operated relief valve
PRA	probabilistic risk assessment
psi	pounds per square inch
PWR	pressurized water reactor
RAT	reserve auxiliary transformer
RADS	Reliability and Availability Data System
RAW	risk achievement worth
RCP	reactor coolant pump

RCS	reactor coolant system
RCY	reactor-critical year
RHR	residual heat removal
ROP	Reactor Oversight Process
RPS	reactor protection system
RTB	reactor trip breaker
RWST	refueling water storage tank
SBO	station blackout
SG	steam generator
SGTR	steam generator tube rupture
SI	safety injection
SLOCA	small loss-of-coolant accident
SORV	stuck-open relief valve
SPAR	standardized plant analysis risk
SRM	staff requirements memorandum
SRV	safety relief valve
SSB	secondary side break
SSC	structure, system, and component
SSIE	support system initiating event
SSPS	solid state protection system
SSU	safety system unavailability
TBV	turbine bypass valve
TDP	turbine-driven pump
THERP	Technique for Human Error Rate Prediction
TPCCW	turbine plant closed cooling water
TPCW	turbine plant cooling water system
TS	technical specifications
UAT	unit auxiliary transformer
UET	unfavorable exposure time
V	volt
VCT	volume control tank
WOG	Westinghouse Owner’s Group

1 INTRODUCTION

This report documents a description and results for the reactor, at-power, Level 1 probabilistic risk assessment (PRA) model for internal events that supports the U.S. Nuclear Regulatory Commission (NRC) full-scope site Level 3 PRA project (L3PRA project) for a two-unit pressurized-water reactor (PWR) reference plant. The results provided in this report are for a single unit—a subsequent report in this series addresses multi-unit risk.

Licensee information used in performing the L3PRA project was voluntarily provided based on a licensed, operating nuclear power plant. The information provided reflects the plant as it was designed and operated as of 2012 and does not reflect the plant as it is currently designed, licensed, operated, or maintained. In addition, the information provided for the reference plant was changed based on additional information, assumptions, practices, methods, and conventions used by the NRC in the development of plant-specific PRA models used in its regulatory decisionmaking. **As such, use of this report to assess the risk from the reference plant is not appropriate and this report will not be the basis for any regulatory decision associated with the reference plant.**

Since the L3PRA project involves multiple PRA models, each of these models should be considered a "living PRA" until the entire project is complete. It is anticipated that the models and results of the L3PRA project are likely to evolve over time, as other parts of the project are developed, or as other technical issues are identified. As such, the final models and results of the project (which will be documented in a summary report to be published after all technical work for the L3PRA project has been completed) may differ in some ways from the models and results provided in the current report.

The series of reports for the L3PRA project are organized as follows:

Volume 1: Summary (to be published last)

Volume 2: Background, site and plant description, and technical approach

Volume 3: Reactor, at-power, internal event and flood PRA
- Volume 3x: Overview
- Volume 3a: Level 1 PRA for internal events (Part 1 – Main Report; Part 2 – Appendices)
- Volume 3b: Level 1 PRA for internal floods
- Volume 3c: Level 2 PRA for internal events and floods
- Volume 3d: Level 3 PRA for internal events and floods

Volume 4: Reactor, at-power, internal fire and external event PRA
- Volume 4x: Overview
- Volume 4a: Level 1 PRA for internal fires
- Volume 4b: Level 1 PRA for seismic events
- Volume 4c: Level 1 PRA for high wind events and other hazards evaluation
- Volume 4d: Level 2 PRA for internal fires and seismic and wind-related events
- Volume 4e: Level 3 PRA for internal fires and seismic and wind-related events

Volume 5: Reactor, low power and shutdown, internal event PRA
- Volume 5x: Overview

Volume 5a: Level 1 PRA for internal events
Volume 5b: Level 2 PRA for internal events
Volume 5c: Level 3 PRA for internal events

Volume 6: Spent fuel pool all hazards PRA
Volume 6x: Overview
Volume 6a: Level 1 and Level 2 PRA
Volume 6b: Level 3 PRA

Volume 7: Dry cask storage, all hazards, Level 1, Level 2, and Level 3 PRA

Volume 8: Integrated site risk, all hazards, Level 1, Level 2, and Level 3 PRA

Part 1 of the current report is organized in 11 sections:

- Section 1 provides an overview of the development of the L3PRA project Level 1 model for reactor, at power, internal events.
- Section 2 provides a description of the initiating event identification/grouping and Level 1 model initiating event frequency calculations.
- Section 3 includes descriptions of the modeling of the events trees.
- Section 4 provides an overview of the success criteria analyses.
- Section 5 provides descriptions of the modeling of the fault trees for the event tree top events and key support systems.
- Section 6 provides descriptions of the human reliability analysis (HRA) elements for the L3PRA Level 1 model development.
- Section 7 provides an overview of the basic event unreliability and unavailability analysis and data-supported recovery failure analysis.
- Section 8 provides a discussion of several key modeling issues, and associated analyses identified in the development of the L3PRA Level 1 model.
- Section 9 provides the baseline core damage frequency results, uncertainty analysis, and basic event importance measures.
- Section 10 provides an overview of the sources of model uncertainty and applicable sensitivity analyses.
- Section 11 provides the references used in this report.

Part 2 of this report includes four appendices:

- Appendix A provides the data tables as described in Section 7 (e.g., template events, CCF parameters, other basic events).
- Appendix B provides an overview of the significant L3PRA Level 1 model cut sets.

- Appendix C provides a table of significant basic events that have risk-achievement worth (RAW) importances greater than or equal to 2.0.

- Appendix D identifies potential future modeling improvement and errors that were identified late in the documentation phase are listed in Appendix D. These modeling improvements should be implemented to maximize the value of the insights obtained from the study.

Simplified diagrams for key systems are provided in Volume 2 of this NUREG series (see Agencywide Documents Access and Management System Accession No. ML22067A232).

CAUTION: While the L3PRA project is intended to be a state-of-practice study, due to limitations in time, resources, and plant information, some technical aspects of the study were subjected to simplifications or were not fully addressed. As such, inclusion of approaches in the L3PRA project documentation should not be viewed as an endorsement of these approaches for regulatory purposes.

1.1 Initial Development of the L3PRA Project Level 1, At Power, Internal Events PRA Model

The L3PRA project Level 1 model incorporated various aspects of the Standardized Plant Analysis Risk (SPAR) model for the reference plant. Since the reference plant CAFTA-based PRA model did not use event trees, the event trees from the reference plant SPAR model were used as the starting point for developing the L3PRA project Level 1 event trees. Other examples of SPAR modeling conventions that were incorporated into the L3PRA project Level 1 model include naming conventions, support system initiating event (SSIE) fault tree methodology, common-cause failure (CCF) modeling, and loss of offsite power (LOOP) modeling. The SPAR model logic and structure was also modified to support planned model extensions (e.g., Level 2 PRA).

Some of the key aspects of the Level 1 model development associated with the SPAR model and NRC modeling approaches, are described below:

- Most basic events were named using the SPAR naming conventions, making sure the naming scheme included a distinction for unit 1 and unit 2 events. For those devices that the reference plant reported device reliability data to the Institute of Nuclear Power Operations (INPO) Consolidated Events (ICES) database, the basic events used plant-specific failure rate templates based on Bayesian updates of industry averaged failure rate data.[5] The original basic event probabilities were preserved in a change set.[6] The Bayesian update of industry-average values with the plant-specific operating experience used the published 2010 update to NUREG/CR-6928, “Industry-Average performance for Components and Initiating Events at U.S. Commercial Nuclear Power Plants” (NRC, 2007), for prior failure rate parameters. Plant specific evidence was used to update the priors for only those devices for which the reference plant reported device reliability through the ICES database.

[5] ICES is a proprietary database and it is not available to the public.

[6] A change set is a set of data modifications to be applied to basic events during fault tree or sequence analysis.

- The CCF events in the reference plant SPAR model were used so that all CCF events from the SPAR model were included in the L3PRA project Level 1 model. The CCF events from the SPAR model used SAPHIRE CCF computations derived from failure rate templates and industry average alpha factor events. However, the reference plant PRA model included many CCF events that could not easily be mapped to SAPHIRE common-cause computations (i.e., failure rate and alpha factor events). CCF events in the reference plant Level 1 PRA model that were not present in the reference plant SPAR model were retained as explicit basic events in the L3PRA project Level 1 model, using the reference plant model quantification. See Section 7.3 for additional information.

- The SSIE fault trees used in the Level 1 PRA were modeled to conform to Electric Power Research Institute (EPRI) Technical Report (TR)-1016741, "Support Systems Initiating Events [SSIE]" (EPRI, 2008), which is the approach used in the existing plant-specific SPAR model. Most of the modifications performed were related to CCF event representation. The NRC/EPRI SSIE practice used represents the basic parameter model events in a CCF group within both initiating event fault trees and mitigating fault trees. The fault tree modeling was arranged to accommodate the dual representation of these events.

- The reference plant SPAR event trees (and related assumptions) for LOOP/SBO were used in modeling with supporting information from the appropriate fault tree logic from the reference plant CAFTA-based PRA model. Some of the key elements of the plant-specific SPAR model that differed from the reference plant model and were incorporated in the L3PRA project Level 1 model include:

  – Event trees were included for each of the four LOOP initiators so that initiator-specific LOOP recovery curves could be used [based on NUREG/CR-6890, “Reevaluation of Station Blackout Risk at Nuclear Power Plants,” (NRC, 2005a) and updates on the NRC parameter estimation web site]. See Section 7.4 for additional information.

  – The potential for a consequential LOOP following a reactor trip (with and without an SI actuation) is explicitly modeled in the safety-related 4.16 kilovolt (kV) alternating current (AC) fault trees. See Section 8.2 for additional information.

  – Convolution corrections were included for emergency diesel fail-to-run events and recovery of offsite power. See Section 7.4.2 for additional information.

  – Credit for aligning offsite power from an alternate switchyard via the station auxiliary transformer (SAT) was included in SBO sequences for plant-centered and switchyard-related LOOPs using a different approach than that used in the reference plant model. The alternate switchyard is not expected to be available during grid- and weather-related LOOPs; therefore, no credit for the alternate switchyard is provided for these LOOP types. See Section 8.1.3 for additional information.

  – No credit was allowed for recovery of offsite power following depletion of the most limiting plant batteries required to realign offsite power to a safety-related bus, which are the turbine building batteries (assumed 2-hour depletion time). See Section 8.1.1 for additional information.

- Reference plant-specific MELCOR thermal-hydraulic calculations, as well as previous MELCOR calculations for a similar plant, were used to confirm selected system success criteria from the reference plant PRA model.

- For the L3PRA project Level 1 model, recovery of hardware failures is not credited. However, recovery of AC power given a LOOP (initiating event or consequential) and subsequent SBO was credited (either explicitly in the fault tree logic for LOOP initiating events or via post-processing rules for consequential LOOPs). The following criteria were used to determine if AC power recovery should be applied (see Section 8.1 for additional information):

  – No recovery credit should be applied to SBO cut sets that imply core damage irrespective of the status of offsite power. Examples involve failure or unavailability of NSCW trains, failure of RAT feeder circuit breakers to the safety-related 4.16 kV AC buses to open, sequencer failures, and battery unavailabilities.

  – Credit for offsite power recovery and for the alignment of power from an alternate switchyard (for applicable LOOP types) should be applied to cut sets that involve actual EDG failures (failure to run, failure to start, or unavailability due to test or maintenance) or EDG-related failures outside the component boundary (e.g., fuel transfer pump), but not to support system components that can lead to the unavailability of the EDGs (e.g., NSCW components).

- The reference plant model included logic for eliminating technical specifications (TS) disallowed maintenance events, applying some very limited recoveries, and applying human error event dependency adjustments. SAPHIRE recovery rules were developed that were equivalent to the reference plant model logic.

After the model development was completed, checks were performed to ensure that the initial version of the L3PRA project Level 1 model yielded results consistent with the reference plant model and any differences were explored. These checks focused on comparison of the importance measures and CDFs/conditional core damage probabilities (CCDPs) for initiating events between the two models.

1.2 Key Changes Subsequent to Initial Model Development

Based on internal reviews by NRC staff, feedback provided by the Advisory Committee on Reactor Safeguards (ACRS), and results of the American Society of Mechanical Engineers/American Nuclear Society (ASME/ANS) PRA standard self-assessment and peer review, the current version of the L3PRA project Level 1 PRA model underwent substantial changes since the model was initially developed. While a significant portion of the L3PRA Level 1 model still aligns with the reference plant model, especially in systems' fault tree logic, some significant changes were made that include:

- The structure of most event trees was modified:

- The transient event trees were modified to allow for a consistent structure and to account for additional modeling assumptions (e.g., 72-hour safe/stable end state,[7] stuck-open secondary-side valves) in the L3PRA project Level 1 model. See Section 3.1 for additional information.

- The potential for pressurizer power-operated relief valves (PORVs) and safety relief valves (SRVs) to be demanded and then failing to reclose was included for all applicable initiating events. See Section 3.1 for additional information.

- The RCP seal injection and cooling functions were separated into different top event fault trees to account for different RCP seal leakage rates. See Section 3.1 for additional information.

- The secondary-side break (SSB) event trees (including consequential SSB) were modified to include the potential for a consequential steam generator tube rupture (SGTR) due to high-pressure differential across the steam generator (SG) tubes. In addition, a consequential SSB upstream of the MSIVs (main steam isolation valves) event tree was created for a stuck-open SG atmospheric relief valve (ARV) or SRV. See Section 3.2 and Section 3.4.2 for additional information.

- The anticipated transient without scram (ATWS) event tree was substantially changed to streamline the event tree logic, account for availability of main feedwater (MFW) for certain applicable initiating events, and to account for different modeling assumptions. See Section 3.4.1 for additional information.

- The SGTR event tree was changed to account for all proceduralized actions and system functions that could affect either the Level 1 or Level 2 model results. See Section 3.3.5 for additional information.

- A screening approach was used to exclude ISLOCA pathways determined to have a negligible effect on the results; therefore, only four ISLOCA pathways are included in the L3PRA project Level 1 model. See Section 3.5 for additional information.

• Applicable fault tree modifications were made:

  - Fault trees to support the 72-hour safe/stable end-state modeling (e.g., charging and late depressurization) were developed and added to the applicable transient event trees. In addition, the AFW fault tree was modified to include the requirement for condensate storage tank makeup. See Section 3.1.1, Section 5.1.2, and Section 8.3 for additional information.

  - The modeling of consequential LOOP was added to the AC power fault tree logic. See Section 8.2 for additional information.

  - The fault tree logic for the turbine trip top event was expanded to include the potential for the TBVs to fail to reclose (if available). These failures lead to an

[7] For event tree sequences that are safe (i.e., no core damage), but not stable at 24 hours (i.e., they would result in core damage at some point after 24 hours), the L3PRA Level 1 model generally extends the accident sequence to 72 hours. See Section 8.3 for additional information.

overcooling transient like the turbine stop or control valves failing to close after a reactor trip. See Section 5.1.46 for additional information.

  - New fault tree logic for the SVC top event, which models the potential for the SG ARVs and SRVs to fail to reclose (if demanded), was developed. These failures lead to an overcooling transient like the turbine stop or control valves failing to close after a reactor trip. See Section 5.1.44 for additional information.

  - New fault tree logic was developed, and some existing fault tree logic was modified, for the revised ATWS and SGTR event trees. See Section 3.4.1 and Section 3.3.5 for additional information.

  - The NSCW fault tree logic was modified to include additional CCF combinations for pumps and cooling tower fans. See Section 7.3.3 for additional information.

- Reevaluations of some human reliability analysis (HRA) elements were performed:

  - Human failure events (HFEs) that were determined to be time critical were quantified using the Human Cognitive Reliability (HCR)/Operator Reliability Experiments (ORE) method, and in other cases using the Cause-Based Decision Tree (CBDT) method, but with different input parameters. See Section 6.2 for additional information.

  - HFEs for which cognition failure probabilities were determined to be too low (i.e., less than or equal to 10-4) were reevaluated. See Section 6.3 for additional information.

  - New HFEs as part of the revised event tree and fault tree logic in the L3PRA project Level 1 model were evaluated. See Section 6.5 for additional information.

  - Due to the occurrence of new HFE combinations, the HFE dependency analysis was re-performed, using the full EPRI dependency method. See Section 6.6 for additional information.

- Revised data was used in the following key areas:

  - Revised initiating event frequencies were calculated. See Section 2.2 for additional information.

The results of an expert elicitation were incorporated into the applicable ISLOCA scenarios. The key parameters provided by the expert elicitation include: (1) valve large internal leakage failure rate, (2) the conditional probability of second valve failure given failure of the first in a series, and (3) valve failure to close against differential pressure as a function of pressure. See Section 3.5 for additional information.

2 INITIATING EVENTS ANALYSIS

This section presents the initiating events analysis. Section 2.1 identifies the initiating events and grouping performed in the L3PRA project Level 1 model. Sections 2.2 and 2.3 describe the initiating event quantification performed as part of the L3PRA project Level 1 model.

2.1 Initiating Event Identification and Grouping

Based on the results of the peer review of the reference plant PRA model initiating event identification and grouping, and the comparison with the reference plant SPAR model initiating event analysis, the L3PRA project Level 1 model uses essentially the same set of initiating events as the reference plant model. The L3PRA project Level 1 model has the following at-power, internal initiating events modeled (36 initiating events total):[8]

1. Turbine Trip (IE-TTRIP)
2. Reactor Trip (IE-RTRIP)
3. Other Transients (IE-TRANS)
4. Loss of Main Feedwater (IE-LOMFW)
5. Loss of Condenser Heat Sink (IE-LOCHS)
6. Large Loss-of-Coolant Accident (IE-LLOCA)
7. Medium Loss-of-Coolant Accident (IE-MLOCA)
8. Small Loss-of-Coolant Accident (IE-SLOCA)
9. Reactor Vessel Rupture (IE-XLOCA)
10. ISLOCA from RCP Stage-One Leak-Off (IE-ISL-RCP-S1LO)
11. ISLOCA from RCP Thermal Barrier Heat Exchanger (IE-ISL-RCP-TBHX)
12. ISLOCA from RHR Cold Leg A Injection Path (IE-ISL-RHR-CLI-A)
13. ISLOCA from RHR Cold Leg B Injection Path (IE-ISL-RHR-CLI-B)
14. ISLOCA from RHR Hot Leg Suction Paths (IE-ISL-RHR-HLS)
15. Steam Generator Tube Rupture (SGTR) (IE-SGTR)
16. Loss of Offsite Power (IE-LOOPPC)
17. Loss of Offsite Power (IE LOOPSC)
18. Loss of Offsite Power (IE LOOPGR)
19. Loss of Offsite Power (IE LOOPWR)
20. Loss of Auxiliary Component Cooling Water (IE-LOACCW)
21. Loss of Nuclear Service Cooling Water (IE-LONSCW)
22. Inadvertent Safety Injection (IE-ISINJ)

[8] Initiating event identifiers are provided in parentheses.

23. Loss of RCP Seal Injection (IE-LOSINJ)
24. Secondary-Side Break Upstream Main Steam Isolation Valves/Downstream Main Feedwater Isolation Valves (IE-SSBI)
25. Secondary-Side Break Downstream Main Steam Isolation Valves/Upstream Main Feedwater Isolation Valves (IS-SSBO)
26. Loss of Instrument Air (IE-LOIA)
27. Loss of Safety-Related 125 volt (V) Direct Current (DC) Bus A – 1AD1 (IE-LO125AD1)
28. Loss of Safety-Related 125 V DC Bus B – 1BD1 (IE-LO125BD1)
29. Loss of Safety-Related 4.16 kilovolt (kV) AC Bus A – 1AA02 (IE-LO4160VA)
30. Loss of Safety-Related 4.16 kV AC Bus B – 1BA03 (IE-LO4160VB)
31. Loss of Safety-Related 120 V AC Panels A and B (IE-LO120VAB)
32. Loss of Safety-Related 120 V AC Panels A and C (IE-LO120VAC)
33. Loss of Safety-Related 120 V AC Panels A and D (IE-LO120VAD)
34. Loss of Safety-Related 120 V AC Panels B and C (IE-LO120VBC)
35. Loss of Safety-Related 120 V AC Panels B and D (IE-LO120VBD)
36. Loss of Safety-Related 120 V AC Panels C and D (IE-LO120VCD)

2.2 L3PRA Project Level 1 Model Initiating Event Quantification

The L3PRA project Level 1 model initiating event (for internal events) frequency quantification is summarized in Table 2-1. The initiating event frequencies were derived from the following sources:

- The Reliability and Availability Data System (RADS) computation was the preferred source as it provides access to the quality-assured initiating event data maintained by the INL for the NRC, and is able to provide plant-specific rates when justified by the available data.

- The published 2010 update to NUREG/CR-6928 (NRC, 2007), referred to as the "2010 update" in this report, was used to obtain frequencies for initiating events for which there is no (or only sparse) data.

- Fault tree models were used to compute initiating event frequencies for the special initiators.

The preferred approach was to determine, where possible, plant-specific initiating event rates for each unit using RADS. RADS does this using the parametric Empirical Bayes (EB) method described in Section 8.2 of NUREG/CR-6823, "Handbook of Parameter Estimation for Probabilistic Risk Assessment" (NRC, 2003a). The EB method attempts to determine the parameters describing the population variability via maximum likelihood estimation, and then performs a Bayesian update on those parameters to determine plant-specific posterior distributions for each plant in the population. The method requires significant event counts to succeed, and plant-to-plant variability in the observed counts. If the method fails, then the population is treated as homogeneous, and no plant-to-plant variability is computed. In these cases, the RADS calculation defaults to a Bayesian update of a Jeffreys prior using the queried

event counts and related reactor-critical years of operating exposure. The latter, for most initiators, is based on the pressurized-water reactor (PWR) population between 1995 and 2010, inclusive. The statisticians that established the baseline periods were seeking a stable baseline where such existed. Early data potentially representative of a learning period, or otherwise not representative of current performance, was excluded when possible. Statistical tests for homogeneity were performed to help determine suitable baseline periods. The largest possible baseline period was sought that satisfied the condition of homogeneity. The inputs and outputs from all RADS-based calculations are provided later in this section.

Some of the 2010 update values are based in some part on expert elicitation. In these cases, no attempt was made to determine a plant-specific initiating event rate [e.g., large loss-of-coolant accident (LOCA)], and the 2010 update frequencies were used as published. The LOOP frequencies represent another special case for which only sparse data are available and no plant-specific evaluation was attempted.

Finally, the special initiator frequencies were calculated from support system initiating event (SSIE) fault trees. The mean values and uncertainty distribution descriptions from the SSIE fault tree calculations are also provided in Table 2-1. The basic events supporting the SSIE model include complete uncertainty information. The resulting SSIE fault tree solution, which is propagated through sequence logic, ultimately results in cut sets in the core damage end state and, therefore, produces uncertainty results. These SSIE results, if considered in isolation, tend to be nearly lognormally distributed. Note that no attempt was made to estimate uncertainty distribution parameters for each frequency to be used in lieu of the uncertainty information obtained via the SSIE fault tree quantification.

The following sections provide summaries of the RADS input and output used in the initiating event frequency estimates. The input includes the date range for the applicable events, the plants included in the query (generally all PWRs), and the RADS codes selected to define each initiator. The RADS output includes the licensee event report numbers for the events counted in the estimate, and the Bayesian update results for the query.

2.2.1 Inadvertent Engineered Safety Features Actuation (Inadvertent Safety Injection)

The frequency for this event is not published in the 2010 parameter estimate update. RADS considers this event a member of the general plant transient category. The RADS identifier is QR9. The RADS query that follows used the same date range as TRANS (1998-2010 in the 2010 update).

RADS selection criteria summary:

Rule: ISINJ
Rule Description:
Date Range: 1998 to 2010
Analysis Type: Run RY
Data Grouping: Plant
Plants/PWR
IPF Codes/Q--General Transients
IPF Codes/Q--General Transients/QR9--Spurious Engineered Safety Feature Actuation

The RADS query returned 2 events. The licensee event report (LER) numbers are 3392007003 and 3062007001.

The RADS computation output was:

Unpartitioned Bayes Analysis for: ISINJ

Number of events: 2

Run Hours: 803.8919

Prior Type: Jeffreys (a, b)

Prior Source: Default Jeffreys Update

Prior Parameters: 0.50; 0.00

Posterior Type: Gamma (a, b)

Posterior Parameters: 2.50; 803.89

Posterior Confidence Interval for 90 percent Interval:

5^{th} Percentile: 7.12×10^{-4}

Mean: 3.11×10^{-3}

95^{th} Percentile: 6.89×10^{-3}

Posterior Variance: 3.87×10^{-6}

Posterior Std-Dev: 1.97×10^{-3}

There are insufficient counts in this category to determine a plant-specific frequency via the EB method. The computation defaulted to Bayesian update of a Jeffreys prior.

Table 2-1 L3PRA Project Level 1 Model Initiating Event Frequency Summary

Event Name	Point Estimate	Mean	Alpha	Beta	5th	50th	95th	Source
1-IE-ISINJ	3.11E-03	3.11E-03	2.500	8.04E+02	7.12E-04	2.71E-03	6.88E-03	RADS: QR9, Jeffreys prior 1998–2010, All PWRs
1-IEFT-ISL-RCP-S1LO	2.58E-06	2.37E-06			3.10E-07	1.43E-06	7.12E-06	Fault tree
1-IEFT-ISL-RCP-TBHX	2.56E-08	2.98E-08			6.92E-10	1.03E-08	1.13E-07	Reference plant PRA model value multiplied by 4 to account for number of identical paths (i.e., each RCP thermal barrier heat exchanger.
1-IEFT-ISL-RHR-CLI-A	5.63E-07	5.60E-07			6.63E-09	2.12E-07	2.21E-06	Fault tree
1-IEFT-ISL-RHR-CLI-B	5.63E-07	5.60E-07			6.63E-09	2.12E-07	2.21E-06	Fault tree
1-IEFT-ISL-RHR-HLS	2.25E-07	3.03E-07			1.52E-08	1.71E-07	1.05E-06	Fault tree
1-IE-LLOCA	1.27E-06	1.27E-06	0.400	3.16E+05	1.31E-09	4.59E-07	5.26E-06	2010 Update
1-IEFT-LO120VAB	1.68E-05	1.68E-05			3.09E-06	9.32E-06	5.31E-05	Fault tree
1-IEFT-LO120VAC	1.68E-05	1.68E-05			3.09E-06	9.32E-06	5.31E-05	Fault tree
1-IEFT-LO120VAD	1.68E-05	1.68E-05			3.09E-06	9.32E-06	5.31E-05	Fault tree
1-IEFT-LO120VBC	1.66E-05	1.65E-05			3.13E-06	9.22E-06	4.83E-05	Fault tree
1-IEFT-LO120VBD	1.66E-05	1.65E-05			3.13E-06	9.22E-06	4.83E-05	Fault tree
1-IEFT-LO120VCD	1.66E-05	1.65E-05			3.13E-06	9.22E-06	4.83E-05	Fault tree
1-IEFT-LO125AD1	2.06E-03	2.06E-03			2.59E-04	1.66E-03	5.33E-03	Fault tree
1-IEFT-LO125BD1	2.06E-03	2.06E-03			2.59E-04	1.66E-03	5.33E-03	Fault tree
1-IE-LO4160VA	1.09E-03	1.09E-03	1.250	1.15E+03	9.16E-05	8.15E-04	3.01E-03	RADS: C1, Jeffreys prior 1992–2010, All PWRs
1-IE-LO4160VB	1.09E-03	1.09E-03	1.250	1.15E+03	9.16E-05	8.15E-04	3.01E-03	RADS: C1, Jeffreys prior 1992–2010, All PWRs
1-IEFT-LOACCW	1.05E-03	1.02E-03			2.29E-04	6.33E-04	3.22E-03	Fault tree

Table 2-1 L3PRA Project Level 1 Model Initiating Event Frequency Summary (cont.)

Event Name	Point Estimate	Mean	Alpha	Beta	5th	50th	95th	Source
1-IE-LOCHS	6.01E-02	6.01E-02	4.705	7.83E+01	2.28E-02	5.59E-02	1.12E-01	RADS: L, Empirical Bayes 1995–2010, All PWRs
1-IEFT-LOIAS	3.49E-03	3.35E-03			1.50E-03	2.76E-03	7.35E-03	Fault tree
1-IE-LOMFW	6.61E-02	6.61E-02	3.240	4.90E+01	1.92E-02	5.95E-02	1.36E-01	RADS: P, Empirical Bayes 1993–2010, All PWRs
1-IEFT-LONSCW	3.47E-05	3.20E-05			5.27E-08	2.78E-06	1.60E-04	Fault tree
1-IE-LOOPGR	1.23E-02	1.23E-02	0.400	3.24E+01	1.28E-05	4.48E-03	5.13E-02	2010 Update
1-IE-LOOPPC	1.93E-03	1.93E-03	2.500	1.29E+03	4.44E-04	1.69E-03	4.29E-03	2010 Update
1-IE-LOOPSC	1.04E-02	1.04E-02	13.500	1.29E+03	6.26E-03	1.02E-02	1.55E-02	2010 Update
1-IE-LOOPWR	3.91E-03	3.91E-03	8.500	2.17E+03	2.00E-03	3.76E-03	6.36E-03	2010 Update
1-IEFT-LOSINJ	2.19E-02	1.88E-02			6.45E-04	9.13E-03	7.07E-02	Fault tree
1-IE-MLOCA	5.10E-04	5.10E-04	0.440	8.63E+02	9.72E-07	2.05E-04	2.05E-03	2010 Update
1-IE-OTRANS	3.99E-01	3.99E-01	11.800	2.96E+01	2.29E-01	3.87E-01	6.07E-01	RADS: QC5, QG9, QG10, QK4, QL4, QL5, QL6, QL7, QP2, QP3, QP4, QP5, QR0, QR1, QR2, QR3, QR4, Empirical Bayes 1998–2010, All PWRs
1-IE-RTRIP	1.56E-01	1.56E-01	6.220	3.98E+01	6.93E-02	1.48E-01	2.72E-01	RADS: QR6, QR7, QR8, Empirical Bayes 1998–2010, All PWRs
1-IE-SGTR	1.38E-03	1.38E-03	2.500	1.81E+03	3.16E-04	1.20E-03	3.06E-03	2010 Update
1-IE-SLOCA	3.67E-04	3.67E-04	0.500	1.36E+03	1.45E-06	1.67E-04	1.41E-03	2010 Update
1-IE-SSBI	3.67E-04	3.67E-04	0.500	1.36E+03	1.45E-06	1.67E-04	1.41E-03	2010 Update
1-IE-SSBO	7.70E-03	7.70E-03	10.500	1.36E+03	4.26E-03	7.48E-03	1.20E-02	2010 Update
1-IE-TTRIP	1.70E-01	1.70E-01	5.530	3.25E+01	7.10E-02	1.60E-01	3.04E-01	RADS: QR5, Empirical Bayes 1998–2010, All PWRs

Table 2-1 L3PRA Project Level 1 Model Initiating Event Frequency Summary (cont.)

Event Name	Point Estimate	Mean	Alpha	Beta	5th	50th	95th	Source
1-IE-XLOCA	1.00E-07	1.00E-07	0.3	3.00E+06	1.07E-11	2.44E-08	4.57E-07	Screening value taken from SPAR models, which is similar to value used for reactor vessel rupture provided in WASH-1400 (NRC, 1975).

2.2.2 Loss of Safety-Related 4.16 kV AC Vital Bus

RADS was queried for PWR-specific rates on the published loss of AC bus date range, which was 1992 to 2010.

The RADS selection criteria summary:

Rule: LOACB
Rule Description:
Date Range: 1992 to 2010
Analysis Type: Run RY
Data Grouping: Plant
Plants/PWR
FI Codes/C--Loss of Safety-Related Bus
FI Codes/C--Loss of Safety-Related Bus/C1--Loss of Vital Medium Voltage AC Bus (>600 V and <10 kV)

The RADS query returned 2 events. The LER numbers are 3182010001 and 3461998011.

RADS computation output was:

Unpartitioned Bayes Analysis for: LOACB

Number of events: 2

Run Hours: 1148.317

Prior Type: Jeffreys (a, b)

Prior Source: Default Jeffreys Update

Prior Parameters: 0.50; 0.00

Posterior Type: Gamma (a, b)

Posterior Parameters: 2.50; 1148.32

Posterior Confidence Interval for 90 percent Interval:

5^{th} Percentile: 4.99×10^{-4}

Mean: 2.18×10^{-3}

95^{th} Percentile: 4.82×10^{-3}

Posterior Variance: 1.90×10^{-6}

Posterior Std-Dev: 1.38×10^{-3}

The above result represents the expected number of events per reactor-critical year (RCY). Since two buses are modeled, the expected number of events is apportioned equally to the two

buses, thus the “a” parameter of the posterior gamma distribution is divided by 2.0 for use in the L3PRA project Level 1 model.

2.2.3 Loss of Condenser Heat Sink

Industry average loss of condenser heat sink values are provided in the 2010 parameter estimate update.

The RADS selection criteria summary:

Rule: LOCHS
Rule Description:
Date Range: 1995 to 2010
Analysis Type: Run RY
Data Grouping: Plant
Plants/PWR
FI Codes/L--Total Loss of Condenser Heat Sink

The RADS query returned 57 events. The LER numbers are:

3342003001	3152008006	3702001001	5282004006	3622004001
4572010003	3152003003	3362001004	5282004006	3272009003
4831995005	2751996012	3362010001	2662005008	3282000001
4832000002	2751999009	4232005002	2662010002	3272009003
3171997009	3641999001	4232005003	3012001001	3351999003
3172000005	2851996002	2552005001	3012004002	2502005005
3172004001	2442003002	5281995012	3062001004	2511997002
3181995002	2442007002	5281999001	3062001005	4242009003
3182004001	4001995011	5282004006	2722001008	4251996008
3182010001	3052006012	5282005005	2722006001	4251998005
3152003003	3691997009	5292000001	3612002003	3822005005
			3612009001	4821995001

Since the event count is high (57 events) an attempt was made to obtain an EB estimate for the reference plant. RADS computation output was:

Empirical Bayes Analysis for: LOCHS

The empirical Bayes method gives a model of the between-item variation, but the chi-squared test says that this may only be modeling random noise.

The Empirical Bayes statistical analysis includes a Kass-Steffey adjustment to the parameters of the gamma or beta EB population variability distribution.

Number of entries: 73

Number of events: 57

Run Hours: 974.6829

Value of X^2 = 81.22, degrees of freedom = 72

p-value = Pr (X^2 if rate of failure is the same for all plants) = 2.14×10^{-1}

Posterior Type: Gamma (a, b)

Posterior Parameters: 3.74; 63.82

Posterior Confidence Interval for 90 percent Interval:

5^{th} Percentile: 1.91×10^{-2}

Mean: 5.86×10^{-2}

95^{th} Percentile: 1.16×10^{-1}

Plant-Specific Result Summary:

Item	Distribution	Failures	RCRY	a	b	Lower	Mean	Upper
Unit 1	Gamma	1	14.9	4.71E+00	7.83E+01	2.29E-02	6.01E-02	1.12E-01
Unit 2	Gamma	2	14.6	4.73E+00	6.55E+01	2.75E-02	7.22E-02	1.34E-01

The above results indicate plant-to-plant variability in the PWR population is questionable. The difference between the pooled result using a Jeffreys prior and the EB result is minimal, the pooled result being 5.9×10^{-2} events per RCY. The EB result above has both a slightly higher frequency, and broader uncertainty range so it was retained for use in the L3PRA project Level 1 model.

2.2.4 Loss of Main Feedwater

The loss of main feedwater initiator also has a high event count indicating potential to determine plant-to-plant variability via the EB method.

The RADS selection criteria summary:

Rule: LOMFW
Rule Description:
Date Range: 1993 to 2010
Analysis Type: Run RY
Data Grouping: Plant
Plants/PWR
FI Codes/P--Total Loss of Feedwater Flow

The RADS query returned 75 events. The LER numbers are:

3131995004	3022005003	3691997009	2821999001	3352002002
4831999008	3022007002	3692005006	2721993002	3892004005
4832004005	2751995015	3362008005	2722000001	3951997002
3171999006	2751996008	2691994002	2722000005	3952005003
3172004001	3231997003	2691999005	3111993002	2811993006
4141995005	3481998004	2692001002	3111997014	4242002003
4142000003	3482002004	2701994002	3112007003	4251996006

4451995003	3641995005	2701994005	3612004002	4251996008
4451996002	3641995005	2871994002	3621999003	4251998008
4452003002	2442005001	2871994003	4431993001	4252001001
4461993011	4002003002	2551995003	3271994008	4252002002
4462006002	2861999010	2552000003	3271998001	3901996004
3152008006	2862007001	2552004001	3272009003	3901996016
3022004001	3051998005	5291993004	3282005001	3901997002
3022004003	3052006001	5291996001	3272009003	4822010012

RADS computation output was:

Empirical Bayes Analysis for: LOMFW

The empirical Bayes method gives a model of the between-item variation that was found by the chi-squared test.

The Empirical Bayes statistical analysis includes a Kass-Steffey adjustment to the parameters of the gamma or beta EB population variability distribution.

Number of entries: 73

Number of events: 75

Run Hours: 1089.954

Value of $X^2 = 95.71$, degrees of freedom = 72

p-value = Pr (X^2 if rate is the same for all plants) = 3.24×10^{-2}

Posterior Type: Gamma (a, b)

Posterior Parameters: 2.24; 32.40

Posterior Confidence Interval for 90 percent Interval:

5^{th} Percentile: 1.40×10^{-2}

Mean: 6.90×10^{-2}

95^{th} Percentile: 1.58×10^{-1}

Plant-Specific Result Summary:

Item	Distribution	Failures	RCRY	a	b	Lower	Mean	Upper
Unit 1	Gamma	1	16.6	3.24E+00	4.90E+01	1.92E-02	6.61E-02	1.36E-01
Unit 2	Gamma	5	16.5	5.02E+00	3.44E+01	5.76E-02	1.46E-01	2.67E-01

The low p-value in the above results indicates plant-to-plant variability in the PWR population is likely, and the plant-specific initiating event frequency was retained for use in the L3PRA project Level 1 model.

2.2.5 Reactor Trip

Reactor trip events are a subset of the published 2010 update TRANS result. The RADS system was queried over the same date range as TRANS (i.e., 1998–2010). The RADS codes used to define reactor trip where QR6, QR7, QR8.

Rule: RTRIP
Rule Description:
Date Range: 1998 to 2010
Analysis Type: Run RY
Data Grouping: Plant
Plants/PWR
IPF Codes/Q--General Transients
IPF Codes/Q--General Transients/QR6--Manual Reactor Trip
IPF Codes/Q--General Transients/QR7--Other Reactor Trip (Valid RPS Trip)
IPF Codes/Q--General Transients/QR8--Spurious Reactor Trip

The RADS query returned 149 events. The LER numbers are:

3132000004	3461998002	3701999004	5302008001	3951999008
3132001001	3461998012	3702000002	5302008002	3951999009
3132008001	3462004002	3702002002	5302009001	3952002003
3132008001	2752000011	3361999009	2662000010	3952009004
3132009001	2752000012	3362000003	3012010001	2802003001
3132009002	3232008002	3362003002	2822002002	2802003002
3132010004	3482002001	3362003006	2822008002	2802008001
3341999010	3482002002	3362003006	3062008002	2812006002
3342002002	3482008004	3362010001	2611998003	2892006003
3342006004	2441999007	3362010002	2612000001	2501998001
4562010004	2441999008	4231998038	2612008002	2501998004
4571999003	2442002001	4232005002	2612010007	2502003008
4572009001	2442003005	4232008003	2722000002	2502004006
4541999003	2442007001	4232010002	3112001008	2502004007
4832001003	4001998007	3382003003	4432005006	2502010006
4832002014	4002002002	3391998004	3271998003	2512010004
3172000001	4002007003	3392004004	3272003001	2512010006
3172002003	4002010002	3392005001	3272009003	4242000004
3172005002	2471999015	3392010004	3272009004	4252004004
4132000001	2472009002	2692010002	3272010002	4252009001
4132003005	2861998006	2871998004	3272009003	3821999011
4141999006	2861999003	2872005002	3282009001	3821999014
4461999002	2862005004	2872008001	4982010003	3822009005
3152005001	2862006002	2552005005	4992002004	3902001004
3152008001	2862009003	5282002001	3351998003	3902010003
3152008006	2862010002	5282006006	3351999007	4822003001
3162001004	3052000009	5291999005	3352010006	4822004004
3162009001	3052006013	5292004002	3892001001	4822004005
3022009001	3052007004	5292007003	3892003004	4822008003

3022009003 3692010003 5302006002 3892010002

RADS computation output was:

Empirical Bayes Analysis for: RTRIP

The empirical Bayes method gives a model of the between-item variation that was found by the chi-squared test.

The Empirical Bayes statistical analysis includes a Kass-Steffey adjustment to the parameters of the gamma or beta EB population variability distribution.

Number of entries: 69

Number of events: 149

Run Hours: 803.8919

Value of $X^2 = 94.92$, degrees of freedom = 68

p-value = Pr (X^2 if rate of failure is the same for all plants) = 1.72×10^{-2}

Posterior Type: Gamma (a, b)

Posterior Parameters: 5.43; 29.24

Posterior Confidence Interval for 90 percent Interval:

5^{th} Percentile: 7.68×10^{-2}

Mean: 1.86×10^{-1}

95^{th} Percentile: 3.33×10^{-1}

Plant-Specific Result Summary:

Item	Distribution	Failures	RCRY	a	b	Lower	Mean	Upper
Unit 1	Gamma	1	12.2	6.22E+00	3.98E+01	6.93E-02	1.56E-01	2.72E-01
Unit 2	Gamma	2	11.8	7.44E+00	4.10E+01	8.74E-02	1.81E-01	3.02E-01

The low p-value in the above results indicate plant-to-plant variability in the PWR population, and the plant-specific initiating event frequency was retained for use in the L3PRA project Level 1 model.

2.2.6 General Plant Transient

The general plant transient category in the 2010 update includes initiating events quantified separately in this analysis. Therefore, RADS was used to re-query the general plant transient initiator using the specific contributors identified below, using the same date range as the 2010 update, and to compute the plant-specific EB result if possible.

Rule: TRANS
Rule Description:
Date Range: 1998 to 2010
Analysis Type: Run RY
Data Grouping: Plant
Plants/PWR
IPF Codes/Q--General Transients
IPF Codes/Q--General Transients/QC5--Loss of Non-safety-Related Bus
IPF Codes/Q--General Transients/QG10--Inadvertent Open or Close: 1 Safety or Relief Valve
IPF Codes/Q--General Transients/QG9--Primary System Leak
IPF Codes/Q--General Transients/QK4--Steam or Feed Leakage
IPF Codes/Q--General Transients/QL4--Loss of Non-safety-Related Cooling Water
IPF Codes/Q--General Transients/QL5--Partial Closure of MSIVs
IPF Codes/Q--General Transients/QL6--Condenser Leakage
IPF Codes/Q--General Transients/QL7--Degraded condenser vacuum
IPF Codes/Q--General Transients/QP2--Partial Loss of Feedwater Flow
IPF Codes/Q--General Transients/QP3--Loss of Condensate Flow
IPF Codes/Q--General Transients/QP4--Partial Loss of Condensate Flow
IPF Codes/Q--General Transients/QP5--Excessive Feedwater Flow
IPF Codes/Q--General Transients/QR0--RCS High Pressure (RPS Trip)
IPF Codes/Q--General Transients/QR1--RCS Low Pressure (RPS Trip) PWR
IPF Codes/Q--General Transients/QR2--Loss of Primary Flow (RPS Trip) PWR
IPF Codes/Q--General Transients/QR3--Reactivity Control Imbalance
IPF Codes/Q--General Transients/QR4--Core Power Excursion (RPS Trip)

The RADS query returned 271 events. The LER numbers are:

3131998005	3162004002	3692002001	2822001005	4992002003
3131998005	3162005001	3692005006	2822006001	3352001007
3132001004	3021998009	3692008002	2611998005	3891999005
3682001002	3022003005	3362000001	2612009003	3892003001
3682009001	3022004003	3362001003	2612010002	3892003003
3682009005	3022005003	3362001004	2612010009	3892004004
3341998028	3022008003	3362002005	2721999004	3892005003
3341999001	3461998010	3362004001	2722000001	3892006001
3342000005	3462006003	3362004002	2722000003	3892008002
3342001003	2751999009	3362009001	2722001008	3892008003
3342003001	2752002004	3362010003	2722002004	3892009002
4122001001	3231998005	4231998043	2722003002	3952002004
4122003003	2751999009	4231998044	2722007002	3952004001
4562007001	3232002002	4231998045	2722007002	3952007001
4562010001	3232006004	3382007001	2722007003	3952008001
4572000002	3481999002	3391999004	3112003001	2801998013
4572001001	3482000006	3392000002	3112004006	2801998014
4572003004	3482004001	3392003001	3112004007	2802003004

4572004002	3642000004	3392006001	3112006003	2811999003
4572007001	3642007001	3392007004	3112007002	2802003004
4572009002	3642010002	3382009004	3112008002	2501999001
4552000002	2852003003	3392010002	3112010001	2502001003
4552001002	2852005001	2691999006	3112010002	2502005005
4552005001	2442000005	2692007001	3112010003	2512000001
4832000002	2442007002	2701998003	3612002006	2512001001
4832004005	4001999002	2701999005	3612002007	2512004002
4832005001	4001999004	2702006001	3621999004	2512004004
4832007002	4001999009	2692007001	3622001001	2512005001
4832008005	4002000005	2551998010	3622002001	2512008001
4832008006	4002002001	2552002002	4432000004	2512010002
4832008008	4002002003	2552006005	4432001003	2512010008
3172006004	4002003003	2552007005	4432003002	4242000002
3172010001	4002003005	2552008001	3272000004	4242004001
3182004001	4002004003	5281998002	3272002004	4242005003
3182006001	4002005002	5281999001	3272008001	4242005004
4132003001	4002008002	5282003002	3272009005	4242006001
4132004002	2472003003	5282005005	3282000001	4242009002
4142000003	2472004001	5282010001	3282002003	4251998005
4142001003	2472004002	5292001002	3282002004	4251999001
4142004002	2472006001	5292003001	3282003004	4252002002
4452003003	2472006003	5292006003	3282007001	4252006003
4461998002	2472007004	5302001001	3282007002	3821998014
4452003003	2472008001	5302004002	3282008001	3821999006
4462003001	2472008003	5302006005	3282009002	3822001003
4462006003	2862000007	5302006007	4981999004	3902001001
3152001001	2862003001	2662000001	4981999006	3902001002
3152002005	2862003003	2662007004	4982002003	3902004002
3152003003	2862005002	2662010002	4982003002	3902008002
3152007001	3051998005	3012001002	4982004001	4821999008
3162002005	3052001004	3012003004	4991998002	4822002003
3162002006	3052005016	3012010002	4992001001	4822003003
3162003002	3052006012	2821998008	4992001002	4822004002
3152003003	3691998002	2821998016	4992001004	4822009001
3162003005	3692000004	2822001004	4992002002	4822010005
				4822010006

RADS computation output was:

Empirical Bayes Analysis for: TRANS

The empirical Bayes method gives a model of the between-item variation that was found by the chi-squared test.

The Empirical Bayes statistical analysis includes a Kass-Steffey adjustment to the parameters of the gamma or beta EB population variability distribution.

Number of entries: 69

Number of events: 271

Run Hours: 803.8919

Value of X^2 = 109.43, degrees of freedom = 68

p-value = Pr (X^2 if rate of failure is the same for all plants) = 1.08×10^{-3}

Posterior Type: Gamma (a, b)

Posterior Parameters: 6.13; 18.12

Posterior Confidence Interval for 90 percent Interval:

5^{th} Percentile: 1.49×10^{-1}

Mean: 3.38×10^{-1}

95^{th} Percentile: 5.90×10^{-1}

Plant-Specific Result Summary:

Item	Distribution	Failures	RCRY	a	b	Lower	Mean	Upper
Unit 1	Gamma	6	12.2	1.18E+01	2.96E+01	2.29E-01	3.98E-01	6.06E-01
Unit 2	Gamma	4	11.8	1.01E+01	2.99E+01	1.84E-01	3.38E-01	5.30E-01

The above results indicate plant-to-plant variability in the PWR population is likely, and the plant-specific initiating event frequency was retained for use in the L3PRA project Level 1 model.

2.2.7 Turbine Trip

The 2010 update treats turbine trip as a contributor to the TRANS result and does not publish a separate result. The RADS system was queried over the same date range as TRANS (i.e., 1998–2010). The RADS code used to define turbine trip was QR5.

Rule: TTRIP
Rule Description:
Date Range: 1998 to 2010
Analysis Type: Run RY
Data Grouping: Plant
Plants/PWR
IPF Codes/Q--General Transients
IPF Codes/Q--General Transients/QR5--Turbine Trip

The RADS query returned 140 events. The LER numbers are:

3132002002	4462008001	2862009007	2822009005	4982000007
3132003001	3152003001	3052007001	3061998005	4991999002
3132005003	3022002002	3701998001	3062000001	3351999006
3682002002	2751999006	3362000010	3062010001	3892003005
3342000006	3232008001	3362002002	3062010002	3892006004
3342003007	3481998004	3362008003	2612006001	3952003002
4122006001	3642001001	4232003001	2612007001	3952009002

4571998001	3642001002	4232005005	2721999001	2801998002
4571999001	2852008001	4232009002	2722001006	2802000004
4572005002	2852010006	3382000004	2722006001	2812002003
4572008002	2442003002	3382003004	2722010002	2812003001
4572010003	2442009002	3392000001	2722010005	2812004001
4542002003	4002003001	3392001005	3112004008	2892006002
4542002003	4002006003	3392010001	3612003001	2502010003
4552000001	2472001007	2701998007	3612004004	2512005002
4832004002	2472003004	2701999001	3612005001	4242001001
4832004003	2472004005	2701999002	3612008004	4242005001
4832006004	2472006005	2701999005	4431998014	4251998003
3171999004	2472009005	2702008001	4432008001	4252007002
3172010003	2472010001	2872000001	3272000003	3901998001
3182003003	2472010007	2872002001	3272004001	3902002003
4132001001	2472010009	2872004001	3272005001	3902003001
4132004004	2862000008	2872009002	3281998001	3902003003
4452010001	2862002003	2552008003	3281998002	3902004001
4462001001	2862006001	5292000007	3282000004	3902006004
4462002001	2862007002	5302003004	3282003005	3902006005
4462003005	2862009004	3012000007	3282006001	3902008004
4462006002	2862009006	3012001001	4981999008	3902010001

RADS computation output was:

Empirical Bayes Analysis for: TTRIP

The empirical Bayes method gives a model of the between-item variation that was found by the chi-squared test.

The Empirical Bayes statistical analysis includes a Kass-Steffey adjustment to the parameters of the gamma or beta EB population variability distribution.

Number of entries: 69

Number of events: 140

Run Hours: 803.8919

Value of X^2 = 116.72, degrees of freedom = 68

p-value = Pr (X^2 if rate of failure is the same for all plants) = 2.19×10^{-4}

Posterior Type: Gamma (a, b)

Posterior Parameters: 3.53; 20.28

Posterior Confidence Interval for 90 percent Interval:

5^{th} Percentile: 5.41×10^{-2}

Mean: 1.74×10^{-1}

95^{th} Percentile: 3.49×10^{-1}

Plant-Specific Result Summary:

Item	Distribution	Failures	RCRY	a	b	Lower	Mean	Upper
Unit 1	Gamma	2	12.2	5.53E+00	3.25E+01	7.09E-02	1.70E-01	3.04E-01
Unit 2	Gamma	2	11.8	5.53E+00	3.21E+01	7.18E-02	1.72E-01	3.08E-01

The above results indicate plant-to-plant variability in the PWR population, and the plant-specific initiating event frequency was retained for use in the L3PRA project Level 1 model.

2.3 L3PRA Project Level 1 Model Initiating Event Validation

This section provides an overview of the comparison of the initiating event frequencies used in the L3PRA project to a preferred industry source, which in this case was the 2010 update. The usefulness of this check in validating the L3PRA project Level 1 model estimate varies with each of the following situations:

- The 2010 update was the source of the initiating event frequency. In this case the comparison provides no useful insight. Examples of this are the LOCA and LOOP categories.

- The 2010 update does not have a category that is comparable to the L3PRA project internal event model category. This occurs when the initiator is so rare that there is no expectation that it will be observed in the data collection process and has not historically been considered important enough to be the subject of expert elicitation. In this case the 2010 update can provide an upper bound on what the frequency might me but provides no insight into how far below the bound the true value is.

- The 2010 update has categories that represent combinations of the L3PRA project categories. This case lends itself to subjective assessment that the L3PRA project estimate does not deviate too far from the bounding comparison category.

- The 2010 update has categories that are directly comparable to the L3PRA project categories, but the L3PRA project result is a plant-specific result not published in the 2010 update. In this case the initiating event frequencies are considered reasonable, or valid, if consistent with industry operating experience. In this case "consistent" is defined as the estimated mean frequency lies between the 5th and 95th percentiles of the comparable industry source uncertainty distribution.

Table 2-2 summarizes the comparison result for each initiator. The special initiator frequencies that were estimated using SSIE fault tree methods are of concern. Of these, only the loss of medium-voltage AC bus, loss of DC bus, loss of seal injection, and RHR ISLOCA frequencies were found to not be consistent with the industry source.

The L3PRA Level 1 model RHR ISLOCA mean frequencies are compared to the 2010 update PWR ISLOCA values, which are based on no observed events during the data collection period. The RHR ISLOCA means all fall below the industry-average estimates; therefore, the comparison only demonstrates that the L3PRA Level 1 model estimates are not higher than can be justified by the evidence. The true value of the ISLOCA frequency could be much lower than the upper bound provided by the evidence.

The L3PRA Level 1 model loss of RCP seal injection frequency estimate, like the RHR ISLOCA frequency estimates, is compared to the 2010 update upper bound based on seeing no PWR events during the data collection period. In this case the L3PRA Level 1 model loss of RCP seal injection mean frequency falls above the uncertainty range of the industry upper bound. The cut sets from the loss of RCP seal injection initiating event fault tree (IEFT-LOSINJ) show 99 percent of the frequency comes from one cut set that comprises failure of the normal charging pump (NCP) to run and failure of operators to establish alternate charging using the safety-related centrifugal charging pumps (CCPs).

The L3PRA Level 1 model loss of 125 V DC bus frequency estimate falls just outside the upper end of the uncertainty range on the 2010 update estimate. This estimate is dominated by one cut set having one event that is based on an industry average DC bus failure rate, as opposed to DC bus failure initiating event rate; the DC bus failure rate being about three times as large as the DC bus initiating event rate.

The L3PRA Level 1 model loss of medium voltage AC bus estimate mean falls outside the lower end of the industry average rate uncertainty range. However, the industry value is based on the reactor-critical years of the PWRs operating during the data collection period; it is not based on the number of buses operating at each plant. When the L3PRA Level 1 model loss of medium voltage bus initiators are combined to produce a plant-level estimate, the result is consistent with the 2010 update result

Table 2-2 L3PRA Project Level 1 Internal Event Model Initiating Event Comparison with Industry Sources

Initiating Event	L3PRA Project		Industry Source[9]			Consistent	Remarks
	Mean	Error Factor	Mean	5th	95th		
1-IE-ISINJ	3.11E-03	2.5					This is an unpublished subset of the transient category.
1-IEFT-ISL-RCP-S1LO	2.37E-06	5.1	3.67E-04	1.44E-06	1.41E-03	Yes	The means are consistent with the published PWR ISLOCA result based on observing no events.
1-IEFT-ISL-RCP-TBHX	2.98E-08	10.5	3.67E-04	1.44E-06	1.41E-03	No	The means are below the lower range of the industry estimate, which is an upper bound based on observing no events [IE-ISLOCA (PWR)].
1-IEFT-ISL-RHR-CLI-A	5.60E-07	7.0	3.67E-04	1.44E-06	1.41E-03	No	
1-IEFT-ISL-RHR-CLI-B	5.60E-07	7.0	3.67E-04	1.44E-06	1.41E-03	No	
1-IEFT-ISL-RHR-HLS	3.03E-07	3.6	3.67E-04	1.44E-06	1.41E-03	No	
1-IE-LLOCA	1.27E-06	11.5	1.33E-06	1.31E-09	5.26E-06	Yes	The L3PRA project Level 1 model estimate is slightly different than the industry-average value.
1-IEFT-LO120VAB	1.68E-05	5.6	3.67E-04	1.44E-06	1.41E-03	Yes	There are no comparable industry average values, however the estimate is consistent with no observed events in the PWR experience in the queried date range.
1-IEFT-LO120VAC	1.68E-05	5.6	3.67E-04	1.44E-06	1.41E-03	Yes	
1-IEFT-LO120VAD	1.68E-05	5.6	3.67E-04	1.44E-06	1.41E-03	Yes	
1-IEFT-LO120VBC	1.65E-05	5.6	3.67E-04	1.44E-06	1.41E-03	Yes	
1-IEFT-LO120VBD	1.65E-05	5.6	3.67E-04	1.44E-06	1.41E-03	Yes	
1-IEFT-LO120VCD	1.65E-05	5.6	3.67E-04	1.44E-06	1.41E-03	Yes	
1-IEFT-LO125AD1	2.06E-03	3.3	7.37E-04	8.64E-05	1.92E-03	No	The estimates fall just outside the upper bound of the industry average value range.
1-IEFT-LO125BD1	2.06E-03	3.3	7.37E-04	8.64E-05	1.92E-03	No	

[9] The industry source is the published 2010 update to NUREG/CR-6928 unless otherwise noted.

Table 2-2 L3PRA Project Level 1 Internal Event Model Initiating Event Comparison with Industry Sources (cont.)

Initiating Event	L3PRA Project		Industry Source			Consistent	Remarks
	Mean	Error Factor	Mean	5th	95th		
1-IE-LO4160VA	1.09E-03	3.7	4.35E-03	2.11E-03	7.26E-03	No	The estimate falls below the lower range of the industry average value range. Note that the industry average value is per RCY while the L3PRA project value is per reactor critical bus year, which makes the value consistent with industry experience.
1-IE-LO4160VB	1.09E-03	3.7	4.35E-03	2.11E-03	7.26E-03	No	
1-IEFT-LOACCW	1.02E-03	5.1	2.46E-04	9.66E-07	9.44E-04	Yes	The estimate is below the upper bound of the industry average value.
1-IE-LOCHS	6.01E-02	2.0	5.86E-02	1.87E-02	1.15E-01	Yes	The L3PRA project Level 1 model estimates are within the uncertainty range of the industry source.
1-IEFT-LOIAS	3.35E-03	2.7	8.22E-03	8.90E-06	3.57E-02	Yes	
1-IE-LOMFW	6.61E-02	2.3	6.89E-02	1.36E-02	1.57E-01	Yes	
1-IEFT-LONSCW	3.20E-05	57.6	2.46E-04	9.66E-07	9.44E-04	Yes	The L3PRA project Level 1 model estimate is within the uncertainty range of the industry source. Note that the uncertainty range on the estimate is very broad and largely driven by uncertainty in the CCF alpha factor estimates.
1-IE-LOOPGR	1.23E-02	11.5	1.22E-02	1.28E-05	5.13E-02	Yes	The estimates are the industry average value.
1-IE-LOOPPC	1.93E-03	2.5	1.93E-03	4.43E-04	4.28E-03	Yes	
1-IE-LOOPSC	1.04E-02	1.5	1.04E-02	6.24E-03	1.55E-02	Yes	
1-IE-LOOPWR	3.91E-03	1.7	3.91E-03	2.00E-03	6.35E-03	Yes	
1-IEFT-LOSINJ	1.88E-02	7.7					This is an unpublished sub set of the transient category.
1-IE-MLOCA	5.10E-04	10.0	5.10E-04	4.81E-07	1.93E-03	Yes	The estimate is the industry average value.

Table 2-2 L3PRA Project Level 1 Internal Event Model Initiating Event Comparison with Industry Sources (cont.)

Initiating Event	L3PRA Project		Industry Source			Consistent	Remarks
	Mean	Error Factor	Mean	5th	95th		
1-IE-OTRANS	3.99E-01	1.6	6.90E-01	3.46E-01	1.13E+00	Yes	The estimate is in the range of values considered consistent with the 2010 parameter estimate. The agreement is closer when the other reference plant model contributors to general transients are added in.
1-IE-RTRIP	1.56E-01	1.8					No comparable value as the 2010 estimate considers this an element of general plant transient.
1-IE-SGTR	1.38E-03	2.5	1.38E-03	3.17E-04	3.07E-03	Yes	The estimates are the industry average value.
1-IE-SLOCA	3.67E-04	8.4	3.67E-04	1.44E-06	1.41E-03	Yes	
1-IE-SSBI	3.67E-04	8.4	3.67E-04	1.44E-06	1.41E-03	Yes	The estimates are the industry average value.
1-IE-SSBO	7.70E-03	1.6	7.70E-03	4.25E-03	1.20E-02	Yes	
1-IE-TTRIP	1.70E-01	1.9					No comparable value as the 2010 estimate considers this an element of general plant transient.
1-IE-XLOCA	1.00E-07	18.8	1.00E-07	1.07E-11	4.57E-07	Yes	The estimate is the industry average value.

3 EVENT TREES

This section provides some information on accident sequence timing (particularly related to available time to recover offsite or emergency power during LOOP events), and presents the event tree models for the initiating events listed in Section 2. These event trees include:

1. Turbine Trip
2. Reactor Trip
3. Other Transients
4. Loss of Main Feedwater (MFW)
5. Loss of Condenser Heat Sink
6. Loss of Instrument Air
7. Loss of Two Safety-Related 120 volt (V) Alternating Current (AC) Panels
8. Loss of Safety-Related 125 V Direct Current (DC) Buses
9. Loss of Safety-Related 4.16 kilovolt (kV) AC Buses
10. Loss of Nuclear Service Cooling Water (NSCW)
11. Loss of Auxiliary Component Cooling Water (ACCW)
12. Loss of Reactor Coolant Pump (RCP) Seal Injection
13. Inadvertent Safety Injection (SI) Actuation
14. LOOPs
15. Secondary-Side Breaks (SSBs)
16. Excessive Loss-of-Coolant Accident (i.e., Reactor Vessel Rupture)
17. Large LOCA (LLOCA)
18. Medium LOCA (MLOCA)
19. Small LOCA (SLOCA)
20. Steam Generator Tube Rupture (SGTR)
21. Interfacing-Systems LOCAs (ISLOCAs)

The first 14 event trees listed are addressed in Section 3.1 (transient event trees). Secondary-side breaks and LOCAs (except ISLOCAs) are addressed in Section 3.2 and Section 3.3, respectively. Section 3.4 addresses transfer event trees that model consequential events [e.g.,

anticipated transient without scram (ATWS) and station blackout (SBO)] that can significantly alter event progression for transient initiators.[10] Section 3.5 addresses ISLOCAs.

The event trees for the L3PRA project Level 1 model are shown in the figures in this section. These event trees include several different end-states, namely:

- "OK" if core damage can be prevented for the 24-hour probabilistic risk assessment (PRA) mission time[11]
- The name of another event tree if the sequence is being transferred (i.e., continued) in a separate event tree (e.g., the ATWS, LOOP, or consequential LOCA event trees)
- Core damage (i.e., "1-CD-XFER")

3.1 Transient Event Trees

The following provides a description of the modeling of transient events trees. These event trees include:

1. Turbine Trip
2. Reactor Trip
3. Other Transients
4. Loss of MFW
5. Loss of Condenser Heat Sink
6. Loss of Instrument Air
7. Loss of Two Safety-Related 120 V AC Panels
8. Loss of Safety-Related 125 V DC Buses
9. Loss of Safety-Related 4.16 kV AC Buses
10. Loss of NSCW
11. Loss of ACCW
12. Loss of RCP Seal Injection
13. Inadvertent SI Actuation

[10] The ATWS event tree is also transferred to from the SLOCA and SGTR event trees.

[11] For those event tree sequences that are safe (i.e., no core damage), but not stable, at 24 hours (i.e., they would result in core damage at some point after 24 hours), the model generally extends the accident sequence to 72 hours.

14. LOOP

Sections 3.1.1 to 3.1.3 discuss general information about the collective set of transient event trees. Sections 3.1.4 to 3.1.17 discuss information pertaining to specific transient event trees.

3.1.1 General Structure for Transient Event Trees

The general event tree structure for transients (provided in Figure 3-1) is used to represent the interactions among several functional event groupings. The first grouping (as represented by the RPS top event) queries whether the reactor successfully tripped either automatically or manually by the operators.[12] If the reactor trip fails, the sequence is transferred to the ATWS event tree (see Section 3.4.1 for additional information).[13]

The second grouping (as represented by the TT and SVC top events) queries whether the turbine successfully tripped (i.e., turbine stop valves/control valves close) and whether a turbine bypass valve (TBV), steam generator (SG) atmospheric relief valve (ARV), or safety relief valve (SRV) sticks open.[14] If the turbine stop/control valves fail to close or an opened TBV fails to reclose, then the sequence is transferred to the consequential SSB downstream of the MSIVs (CSSBO) event tree. If the ARVs or the SRVs are demanded and at least one fails to reclose, then the sequence is transferred to the consequential SSB upstream of the MSIVs (CSSBI) event tree. See Section 3.4.2 for additional information on the consequential SSB event trees.

The third grouping (as represented by the PVC top event) queries whether the pressurizer power-operated relief valves (PORVs)/SRVs are challenged and, if so, do they reclose.[15] If a PORV/SRV fails to reclose, the sequence is transferred to the consequential SLOCA event tree (see Section 3.4.3 for additional information).

The fourth grouping (as represented by the RCPSI and RCPSC top events) queries whether RCP seal injection and RCP seal cooling (via ACCW through the thermal barrier heat exchangers) are successful.[16] In addition, the RCP seal cooling fault tree (RCPSC top event)

---

[12] The reactor trip or loss of RCP seal injection initiating events do not include the reactor protection system (RPS) top event since these initiators assume that reactor trip (itself) is the beginning of these transients (loss of RCP seal injection does not result in an automatic reactor trip, so the operators would need to manually trip the reactor for this transient to become an initiating event).

[13] A failure of a secondary valve(s) to close in combination with a failure of RPS (i.e., ATWS) is not queried in the L3PRA Level 1 model. It is not expected that a stuck-open ARV(s) or SRV(s) would have an appreciable effect on the progression of an ATWS. However, the L3PRA Level 1 model does query the success/failure of the turbine to trip in the ATWS event tree because the failure to trip the turbine given a loss of feedwater during an ATWS is expected to lead to dry out of the SG inventory due to the limited makeup of the auxiliary feedwater (AFW) pumps.

[14] The TBVs are also referred to as the steam dump valves. Each unit has a total of four banks of TBVs; however, all these banks of TBVs are only needed initially after the turbine trip. Only the bank 1 TBVs are used for decay heat removal; the bank 2, 3, and 4 TBVs remain closed below a pre-established temperature limit. Therefore, all 4 banks of TBVs are modeled for failure to close in the TT top event, and only the bank 1 TBVs are modeled for the steam removal paths in the AFW and MFW fault tree logic.

[15] The pressurizer SRVs are only challenged if the PORVs fail to open (if demanded).

[16] RCP seal injection is normally provided by the normal charging pump (NCP). Although the CCPs may also be manually aligned for RCP seal injection, they are not credited for RCP seal injection for most transient initiating events because under the worst-case scenario, a total loss of RCP cooling occurs just after the initiating event occurs. In these cases, it is unlikely that operators can restore RCP seal injection using CCPs within the required 13 minutes. After reactor trip, operators would follow the reactor trip or SI procedure (E-0). E-0 would transfer to post-trip response procedure (ES-0.1), if no SI is required. ES-0.1 directs operators to check if any abnormal operating procedures (AOPs) are in effect. After entering the related AOP, operators still need time to establish

also queries the integrity of RCP seals given a loss of all RCP seal injection/cooling.[17] If the RCP seals fail, the sequence is transferred to the consequential SLOCA event tree. Additional information on RCP seal failure modeling is provided in Section 8.4.

The fifth grouping (as represented by the FW, FAB, and FABR top events) queries whether decay heat removal/inventory control is successful. Unless there is a consequential LOCA from a stuck-open PORV/SRV or the failure of RCP seals, short-term inventory control is only needed if feed and bleed is initiated. Typically, early decay heat removal is provided by feedwater (represented by the FW top event) via the AFW or MFW systems to the SGs, with the steam removal provided by the TBVs (to the condenser) or via the SG ARVs/SRVs. In addition to providing short-term decay heat removal, feedwater provides long-term decay heat removal to a safe and stable end-state if RCP seal injection is maintained (i.e., RCP seal leakage remains at the nominal leakage rate for each RCP). If feedwater makeup to the SGs is not available and/or no steam removal path exists, operators will be directed to initiate feed and bleed cooling (represented by the FAB top event) using high-pressure injection and the pressurizer PORVs.[18] Long-term decay heat removal after initial feed and bleed cooling requires operators to switch to high-pressure recirculation (represented by the FABR top event).[19] The heat sink for recirculation is provided by the residual heat removal (RHR) heat exchangers [cooled by component cooling water (CCW)] or the containment cooling units (CCUs). Failure of either early or late decay heat removal results in core damage.[20]

The final grouping (represented by the CHG and SAFESTABLE top events) queries whether the plant is safe and stable at 72 hours for transients with elevated RCP seal leakage (given successful feedwater with no ATWS or consequential SSB or SLOCA).[21] If RCP seal injection is lost, but either seal cooling to the thermal barrier heat exchangers or RCP seal integrity is maintained, seal leakage is assumed to increase from nominal to 21 gpm per RCP. At this leakage rate, core damage would not occur prior to 24 hours, but could occur prior to 72 hours unless other mitigation is successful. Even though there is insufficient time available for operators to align the centrifugal charging pumps (CCPs) to provide alternate RCP seal injection for most transient initiating events, operators are procedurally directed to align a CCP to provide alternate charging to the reactor coolant system (RCS), as represented by the CHG top event. If charging is successful, core damage will not occur prior to 72 hours.[22] If operators fail to align

---

RCP seal injection using the CCPs. However, for the loss of ACCW and the loss of RCP seal injection initiating events, the applicable AOPs direct operators to start a CCP to provide RCP seal injection; and therefore, it is likely that operators can perform this action within 13 minutes.

[17] If RCP seal injection is lost, but seal cooling is maintained, the RCP seal leakage is conservatively assumed to be 21 gallons per minute (gpm) per RCP (as a modeling simplification). Note that WCAP-15603, "WOG 2000 Reactor Coolant Pump Seal Leakage Model for Westinghouse Pressurized Water Reactors," (Westinghouse, 2002) states that 21 gpm per RCP seal is assumed for complete loss of RCP injection and cooling scenarios. This modeling simplification has a negligible effect on the overall results.

[18] Only the CCPs are credited for feed and bleed cooling during transients (i.e., no credit is taken for the SI pumps);

[19] High-pressure recirculation (HPR) requires the starting and alignment of an RHR pump to the suction of the running CCP from the containment sump. Note that the containment sump isolation valves open automatically on low RWST level; however, operators need to manually close the RWST suction valve(s).

[20] The end-state for core damage in the L3PRA Level 1 model is shown as a transfer to the L1-Bridge event tree.

[21] For event tree sequences that are safe (i.e., no core damage), but not stable at 24 hours (i.e., they would result in core damage at some point after 24 hours), the L3PRA Level 1 model generally extends the accident sequence to 72 hours. See Section 8.3 for additional information.

[22] In addition to the alignment of charging, operators are procedurally directed to isolate RCP seal leakage if leakage exceeds 5 gpm per RCP. However, this operator action was not credited in the L3PRA Level 1 model. This model simplification has a negligible effect on the results.

charging, operators would enter one of the critical safety function status tree (CSFST) procedures for loss of core cooling (FR-C.1) or inadequate core cooling (FR-C.2). These procedures direct the operators to cooldown and depressurize the plant by depressurizing the SGs using the TBVs (if the condenser is available) or the SG ARVs. This depressurization will allow the accumulators to inject in the RCS thus providing makeup. Failure of the cooldown/ depressurization or injection from the accumulators results in core damage before 72 hours. For AFW to provide long term decay removal for at least 72 hours, additional inventory must be provided. This is accomplished by automatic makeup to the condensate storage tank (CST) 1 from the demineralizer water system. If automatic makeup is unavailable, operators would align to CST 2 to provide additional inventory for continued AFW operation.

3.1.2 Top Event Descriptions and General Success Criteria for Transients

The typical top events used in transient events trees and their associated success criteria are provided below.

IE-xxxx — Initiating event designator (e.g., IE- RTRIP, IE-LOCHS, etc.).

RPS — This top event represents the success or failure of RPS to insert enough negative reactivity by the control rods to shut down the reactor. If automatic reactor trip fails, operator action is necessary to manually trip the reactor (OA------MANRTH or RPS-XHE-XE-NSGNL, depending on whether a reactor trip signal is present). Sequences involving failure of the reactor to trip are transferred to the ATWS event tree. Additional information on the RPS fault tree modeling is provided in Section 5.1.37.

TT — This top event represents the success or failure of turbine trip (i.e., the turbine stop/control valves close) and opened TBVs to reclose. After a reactor trip, the main turbine should be tripped to prevent overcooling of the RCS. Failure of a turbine trip or a TBV to reclose leads to a consequential SSB downstream of the main steam isolation valves (MSIVs); and therefore, the sequence is transferred to the CSSBO event tree. Additional information on the TT fault tree modeling is provided in Section 5.1.46.

SVC — This top event represents the success or failure of SG ARVs and SRVs to reclose (if demanded). After a reactor trip, if the main turbine successfully trips and the TBVs either fail to open or are rendered unavailable, the ARVs will be required to open to provide decay heat removal. If the ARVs fail to open or are unavailable, the SRVs will be challenged to open. If the SRVs fail to reclose (after being demanded), this results in a consequential SSB upstream of the MSIVs; and therefore, the sequence is transferred to the CSSBI event tree. Additional information on the SVC fault tree modeling is provided in Section 5.1.44.

PVC — This top event represents the potential that the pressurizer PORVs/SRVs are challenged given the initiating event and the success or failure of the valves to reclose (if demanded).[23] Success requires that no pressurizer

[23] The failure of the pressurizer SRVs to reclose is only queried if the PORVs are challenged by the initiating event and fail to open.

PORVs/SRVs open given the transient or that either (1) all opened PORVs/SRVs reclose once RCS pressure is lower than the relief pressure set-points or (2) the PORV block valve(s) are subsequently closed (automatically on low RCS pressure).[24] If a PORV or SRV sticks open, a consequential SLOCA occurs; and therefore, the sequence is transferred to the consequential SLOCA event tree. Additional information on the PVC fault tree modeling is provided in Section 5.1.32.

RCPSI — This top event represents the success or failure of normal RCP seal injection via the NCP. As discussed previously, alignment of the CCPs for alternate seal injection is only credited for the loss of ACCW and loss of RCP seal injection initiating events. If RCP seal injection fails, seal leakage is assumed to increase to at least 21 gpm per RCP (higher leakage rates may occur depending on the success or failure of RCP thermal barrier cooling—see RCPSC below). Additional information on the RCPSI fault tree modeling is provided in Section 5.1.36.

RCPSC — This top event represents the success or failure of RCP seal cooling from the thermal barrier heat exchangers (cooled via ACCW). If RCP seal cooling fails, the integrity of the seals is challenged. Per the Westinghouse Owner's Group (WOG) 2000 RCP seal leakage model (Westinghouse, 2002), given the loss of all RCP seal cooling and injection, RCP seals have an approximately 21 percent chance of failure.[25] In addition, operator failure to trip the RCPs (RCS-XHE-XM-TRIP) will also result in failure of RCP seals. A failure of RCP seals is assumed to result in a consequential SLOCA; and therefore, the sequence is transferred to the consequential SLOCA event tree. Additional information on the RCPSC fault tree modeling is provided in Section 5.1.35.

FW — This top event represents the success or failure of the AFW or MFW system to remove decay heat via the SGs. If the transient initiating event does not render MFW unavailable (e.g., loss of MFW, loss of condenser heat sink, loss of instrument air, loss of safety-related AC/DC bus), the system will initially isolate given a reactor trip and low Tavg. This will require the use of 1 of 2 motor-driven AFW pumps or the turbine-driven AFW pump to provide flow to 2 of 4 SGs. In addition, sufficient steam removal is required by either: (1) three TBVs or (2) an ARV or 1 of 5 SRVs for 2 of 4 SGs. Success implies automatic actuation and operation of the AFW system to supply sufficient cooling water to the SGs. If the automatic AFW actuation signal fails, operator action (OA-START-AFW-H) is credited to manually start an AFW pump before a feed and bleed condition occurs. The MFW isolation on low Tavg only closes MFW valves but does not trip MFW pumps; the pumps will be on minimum flow after the isolation. If AFW fails to feed required flow to the SGs after MFW isolation, operator action (OAF_MFW------H) is required

[24] The operators can also manually close the PORV block valves; however, credit for manually closure of these valves is not provided in the L3PRA Level 1 model.

[25] The two stages of RCP seals are not separated because the failure of one or both seals is assumed to result in a SLOCA. The WOG RCP seal leakage model assumes that a failure of the stage 2 seals leads to a 182 gpm per RCP LOCA; whereas, a failure of stage 1 seals leads to 76 gpm per RCP LOCA. A failure of both stages of seals results in a 480 gpm per RCP LOCA.

to re-establish flow from 1 of 2 MFW pumps to 1 of 4 SGs.[26] While the condensate system could be used to feed the SGs, it was determined that there is insufficient time to implement this action prior to the need to initiate feed and bleed cooling. Additional information on the FW fault tree modeling is provided in Section 5.1.10.

FAB This top event represents the success or failure of feed and bleed cooling. Feed and bleed cooling is required given secondary cooling (AFW and MFW) is unavailable. Success requires 1 of 2 CCPs to provide flow to the RCS cold legs and 1 of 2 PORVs to open and remove decay heat. Operator action (OAB_TR-------H) is required to trip all the RCPs and initiate feed and bleed operation when the feed and bleed criteria are met. If feed and bleed cooling fails, core damage is assumed to occur. Additional information on the FAB fault tree modeling is provided in Section 5.1.8.

FABR This top event represents the success or failure of long term feed and bleed operation using high-pressure recirculation (HPR). If feed and bleed is initiated due to failure of AFW and MFW, operators need to switch to HPR when the refueling water storage tank (RWST) level drops below the set-point.[27] Success requires the CCPs to take suction from the discharge of the RHR pumps and deliver the water to the RCS.[28] HPR will provide long-term cooling for the reactor given high-pressure injection (HPI) was successful in supplying early makeup water to the reactor. The decay heat will be removed from the containment sump by the RHR heat exchangers (cooled via CCW) or by 4 of 8 CCUs. An operator action (OAR_LTFB-TRA-H if CCUs are available or OAR_LTFB-TRB-H if CCUs are not available) is required to align the RHR pump discharge to the HPI pump suction and verify that the containment sump valves are open and the RWST suction valves are closed. If feed and bleed recirculation fails, core damage is assumed to occur. Additional information on the FABR fault tree modeling is provided in Section 5.1.9.

CHG This top event represents the success or failure of alternate charging to the RCS. In addition to providing the normal source of RCP seal injection, the NCP is also the source of normal charging to the RCS. For transients where the NCP fails after the reactor trip, operators are directed to align a CCP as an alternate source of charging. Given a loss of RCP seal injection, but with RCP seal integrity maintained, seal leakage is assumed to increase from nominal to 21 gpm per RCP. If AFW or MFW is providing long-term decay heat removal, charging via a CCP is required to provide makeup to the RCS to prevent core damage within 72 hours. An operator action (CHG-XHE-NORMAL) is required to start and align a CCP to provide

---

[26] In addition to restoring MFW to provide makeup to the SGs, the loss of secondary-side heat sink procedure (FR-H.1) directs operators to feed the SGs using condensate; however, it was determined that there was insufficient time prior to the need to initiate feed and bleed.

[27] The switch-over to high-pressure recirculation is a semi-automatic process. When the RWST lowers to the low-level setpoint, the containment sump isolation valves are automatically opened. However, operators must manually restart the RHR pumps, align the CCP suction to the discharge of the RHR pump, and isolate the RWST.

[28] The pump success criterion for feed and bleed recirculation is assumed to be the same as the pump success criterion for feed and bleed in the injection mode. This is potentially conservative because no credit is given for the SI pumps for feed and bleed in the injection mode, while it is possible that an SI pump may provide adequate flow in the recirculation mode.

makeup to the RCS. Additional information on the CHG fault tree modeling is provided in Section 5.1.5.

SAFE/STABLE This top event represents the success or failure of cooldown and depressurization to allow the accumulators to provide makeup to the RCS. If the RCP seals are leaking at the assumed rate of 21 gpm per RCP due to lack of seal injection, core damage prior to 72 hours can occur if a source of inventory makeup to the RCS is not provided. If alternate charging fails, operators will eventually be directed by CSFST procedures to depressurize the SGs with a modeled minimal success criterion of 3 of 3 TBVs (to the condenser) or an ARV for 1 of 4 SGs. If successful, this depressurization will allow the accumulators (2 of 4 accumulators required for success) to inject into the RCS, thus providing makeup. An operator action is required (CAD-XHE-SAFESTABLE). If AFW is to provide long-term decay heat removal for at least 72 hours, additional inventory must be provided. This is typically accomplished by automatic makeup to the CST 1 from the demineralizer water system. If automatic makeup is unavailable (e.g., loss of instrument air), operator action (OA-ALTAFW----H) is required to align CST 2 to provide additional inventory for continued AFW operation. If the cooldown/depressurization, accumulators, or CST makeup fail, core damage will occur prior to 72 hours. Additional information on the SAFE/STABLE fault tree modeling is provided in Section 5.1.41.

3.1.3 Turbine Trip Event Tree

The turbine trip initiating event category considers all the initiators that directly result in a turbine trip. A turbine trip with P-9 (reactor power ≥ 50 percent) will generate an automatic reactor trip. Turbine trips due to major support system failures such as LOOP or turbine trip after a reactor trip (turbine trip by P-4) were not included in this category because they are separately modeled. The NUREG/CR-5750 (NRC, 1999a) event category for this initiating event is QR5, turbine/generator trip. The turbine trip event tree follows the general structure for transient initiating events described in Section 3.1.1.[29] Figure 3-2 shows the turbine trip event tree.

3.1.4 Reactor Trip Event Tree

While all transient initiating events lead to a reactor trip, the initiators considered here are those that began directly with a reactor trip as opposed to other transient categories that may require a reactor trip in the process of the event. Therefore, the potential failure of the RPS leading to an ATWS is not considered as part of this initiating event category. All other event tree modeling aspects for the reactor trip event tree follow the general structure for transient initiating events described in Section 3.1.1. The following NUREG/CR-5750 event categories are included in this initiating event category: (1) QR8, spurious reactor trip; (2) QR7, other reactor trip; and (3) QR6, manual reactor trip. Figure 3-3 shows the reactor trip event tree.

3.1.5 Other Transients Event Tree

This initiating event category includes all primary and secondary transient events that require a reactor trip except those included in other initiating event categories. The following NUREG/CR-5750 event categories are included in this initiating event category: (1) QC5, loss of

[29] The turbine stop and control valves are assumed to be closed for this initiating event because the turbine trip itself is the initiating event. However, the TT top event is still queried in the turbine trip event tree because it is possible the TBVs may fail to close.

nonsafety-related bus; (2) QG10, inadvertent open or closure of 1 safety or relief valve; (3) QG9, primary system leak; (4) QK4, steam or feed leakage; (5) QL4, loss of nonsafety-related cooling water;[30] (6) QL5, partial closure of MSIVs; (7) QL6, condenser leakage; (8) QL7, degraded condenser vacuum; (9) QP2, partial loss of feedwater flow; (10) QP3, loss of condensate flow; (11) QP4, partial loss of condensate flow; (12) QP5, excessive feedwater flow; (13) QR0, RCS high pressure (RPS trip); (14) QR1, RCS low pressure (RPS trip) PWR; (15) QR2, loss of primary flow (RPS trip) PWR; (16) QR3, reactivity control imbalance; and (17) QR4, core power excursion (RPS trip). The other transients event tree follows the general structure for transient initiating events described in Section 3.1.1. Figure 3-4 shows the other transients event tree.

3.1.6 Loss of Main Feed Water Event Tree

This initiating event category includes transients that involve the complete and sustained loss of main feedwater flow. Feedwater isolation after reactor trip by P-4 (low T_{avg} setpoint) or by an SI actuation were not included in this category, because they are covered by different transient initiating events. The NUREG/CR-5750 event category for this initiating event is P1, total loss of MFW flow. The loss of MFW event tree follows the general structure for transient initiating events described in Section 3.1.1, except the AFW (only) top event fault tree is used instead of the combined FW top event. Figure 3-5 shows the loss of MFW event tree.

3.1.7 Loss of Condenser Heat Sink Event Tree

This initiating event category includes the loss of the condenser as a heat sink. With the condenser unavailable, the TBVs cannot be used to direct steam to the condenser. In addition, the MFW pumps will trip on low condenser vacuum, which causes a total loss of MFW flow. Although feedwater might be used after resetting feedwater isolation, the MFW and condensate systems are assumed unavailable given a loss of condenser heat sink since condenser hot well water inventory is not sufficient for a 24-hour mission operation time. The NUREG/CR-5750 event category for this initiating event is L, loss of condenser heat sink. The loss of condenser heat sink event tree follows the general structure for transient initiating events described in Section 3.1.1, with two exceptions. First, the TT top event is not included because for this initiating event the turbine and TBVs would be isolated due to the closure of the MSIVs or the turbine would be isolated (and the TBVs rendered unavailable by a permissive circuit) due to a loss of condenser vacuum. The second exception is that the AFW (only) top event fault tree is used instead of the combined FW top event. Figure 3-6 shows the loss of condenser heat sink event tree.

3.1.8 Loss of Instrument Air Event Tree

This initiating event category includes the complete loss of instrument air initiating event. The main feed water regulating valves (MFRVs) and bypass valves will close on loss of instrument air. The closure of MFRVs will cause a reactor trip on low SG water level. The MSIVs also fail closed on loss of instrument air. After closure of the MFRVs and MSIVs, the event would progress like a loss of condenser heat sink, with some additional components unavailable due to the loss of instrument air. The loss of instrument air event tree follows the general structure

---

[30] The functional impact (instead of initial plant fault) definition is used for classification of these initiating events. Therefore, loss of nonsafety-related cooling water events that result in a loss of feedwater or condenser heat sink would be included in those initiating events.

for transient initiating events described in Section 3.1.1, with three exceptions. First, a SSIE fault tree (IEFT-LOIAS) is used to develop the loss of instrument air frequency based on both the operating components and the standby components. The components in this SSIE fault tree include the air compressors (reciprocating and rotary), air receivers, moisture separators, distribution header valves, and system isolation valves. The IEFT-LOIAS fault tree represents both the frequency of a loss of instrument air leading to a reactor trip and the unavailability of instrument air for support to the frontline systems (see Section 5.2.6 for additional information on this SSIE fault tree). The second exception is that the TT top event is not included because the loss of instrument air results in the closure of the MSIVs; and therefore, isolates the turbine and TBVs. The third exception is that the AFW (only) top event fault tree is used instead of the combined FW top event (due to the closure of the MFRVs and bypass valves). The impacts of this initiator on mitigating systems and their support systems are implicitly reflected via the fault trees. Figure 3-7 shows the loss of instrument air event tree.

3.1.9 Loss of Two Safety-Related 120 V AC Panels Event Tree

This initiating event category includes the six initiating events involving the loss of two safety-related 120 V AC panels. The model is based on a unit having four safety-related 120 V AC panels (panels A, B, C, D). Failure of one of these four panels does not cause a reactor trip; however, the failure of any two of these four panels does cause a reactor trip due to the loss of 2 of the 4 RPS channels. The six corresponding event trees are identical in structure and include the following panel combinations: (1) panels A and B, (2) panels A and C, (3) panels A and D, (4) panels B and C, (5) panels B and D, and (6) panels C and D.

These event trees follow the general structure for transient initiating events described in Section 3.1, except that support system initiating event (SSIE) fault trees (IEFT-LO120VAB, IEFT-LO120VAC, IEFT-LO120VAD, IEFT-LO120VBC, IEFT-LO120VBD, and IEFT-LO120VCD) are used to quantify the frequency of the loss of two 120 V AC panels, based on both the operating components and the standby components. The components in these SSIE fault trees include the panels themselves; as well as the breakers, inverters, and fuses located between the panels and their respective safety-related 125 V DC buses and 480 V motor control centers (MCCs).

These fault trees represent both the frequency of a loss of two safety-related 120 V AC panels leading to a reactor trip and the unavailabilities of two safety-related 120 V AC panels to support frontline systems (see Section 5.2.2 for additional information on these SSIE fault trees).The impacts of these initiating events on mitigating systems and their support systems are implicitly reflected via the fault trees.[31, 32] Figure 3-8 shows the loss of two safety-related 120 V AC panels event tree (for panels A and B).

3.1.10 Loss of a Safety-Related 125 V DC Bus Event Tree

This initiating event category includes the two loss of safety-related 125 V DC bus initiating events for DC bus A and bus B. The two corresponding event trees are identical in structure. The loss of safety-related 125 V DC bus A or B causes a main steam line and MFW line

---

[31] The loss of safety-related 120 V AC panel A and/or B causes automatic actuation failure of components receiving the engineered safety features actuation system (ESFAS) train A and B signals, respectively. Therefore, a loss of both safety-related 120 V AC panels A and B results in a complete loss of ESFAS, which will require operators to manually start needed pumps [e.g., AFW and emergency core cooling system (ECCS) pumps].

[32] Panels A and B supply power to pressure instrumentation for the ARVs; each panel supplies two ARVs each. Therefore, the loss 120 V AC Panels A and B results in the total unavailability of the ARVs.

isolation (and subsequent reactor trip); therefore, they are modeled as special initiating events.[33] These two event trees follow the general structure for transient initiating events described in Section 3.1.1, with three exceptions. First, SSIE fault trees (IEFT-LO125 VAD1 and IEFT-LO125 VBD1) are used to develop the loss of safety-related 125 V DC bus frequencies based on both the operating components and the standby components. The components in these fault trees include the buses themselves; as well as the batteries, battery chargers, and breakers located between the buses and their respective battery and 480 V MCCs. These fault trees represent both the frequency of a loss of a safety-related 125 V DC bus leading to a reactor trip and the unavailability of the bus to support frontline systems (see Section 5.2.1 for additional information on these SSIE fault trees). The second exception is that the TT top event is not included because the loss of safety-related 125 V DC bus A or B results in the closure of the MSIVs; therefore, isolating the turbine and TBVs. The third exception is that the AFW (only) top event fault tree is used instead of the combined FW top event (due to the isolation of the main steam and main feedwater lines).

The impacts of these initiating events on mitigating systems and their support systems are implicitly reflected via the fault trees. Key safety-related equipment rendered unavailable by a loss of safety-related 125 V DC bus A and bus B are provided in the following table.[34] Figure 3-9 shows the loss of safety-related 125 V DC bus A event tree.

Loss of 125 V Safety-Related DC Bus A	Loss of Safety-Related 125 V DC Bus B
Train A inverters	Train B inverters
Emergency Diesel Generator (EDG) A	EDG B
Pressurizer PORV A	Pressurizer PORV B
SGs 1 and 4 ARVs	SGs 2 and 3 ARVs
Train A ECCS pumps	Train B ECCS pumps
Motor-Driven AFW Pump A	Motor-Driven AFW Pump B
Train A NSCW pumps (1, 3, and 5)	Train A NSCW pumps (2, 4, and 6)
Train A NSCW cooling tower fans	Train A NSCW cooling tower fans
ACCW Pump 1	ACCW Pump 2
CCW Pumps 1, 3, and 5	CCW Pumps 2, 4, and 6
Train A CCUs (1, 2, 5, and 6)	Train A CCUs (3, 4, 7, and 8)

3.1.11 Loss of a Safety-Related 4.16 kV AC Bus Event Tree

This initiating event category includes two loss of safety-related 4.16 kV AC bus initiating events, for bus A and bus B, respectively.[35] The two corresponding event trees are identical in structure. While the loss of either bus does not directly result in a reactor trip, it does lead to a loss of the associated safety-related 125 V DC bus after depletion of its safety-related battery (assumed to occur after 4 hours). After the batteries are depleted, the event progression is like

[33] The loss of either (or both) safety-related 125 V DC Bus C and/or D will render some structure, system, and components (SSCs) unavailable (e.g., turbine-driven AFW pump steam valves, RHR valves); however, the loss of these buses will not cause a reactor trip.

[34] A loss of safety-related DC power renders standby SSCs failed. However, running equipment (e.g., NSCW pumps, NSCW cooling tower fans, ACCW pump) remain running as long as the (LOOP) sequencer does not strip these loads and attempt to restart this equipment.

[35] These initiating events also capture losses of offsite power to the safety-related AC bus(es) (i.e., partial LOOP events) in which the emergency AC power system (i.e., EDGs) fails to restore power to the affected bus(es).

a corresponding loss of safety-related 125 V DC bus initiating event. The loss of safety-related 4.16 kV AC bus event trees follow the general structure for transient initiating events described in Section 3.1.1, with two exceptions. First, the TT top event is not included because the loss of safety-related 4.16 kV AC bus results in the eventual loss of safety-related 125 V DC bus A or B, which causes the closure of the MSIVs, isolating the turbine and TBVs. The second exception is that the AFW (only) top event fault tree is used instead of the combined FW top event (due to the isolation of the main steam and main feedwater lines). The impacts of these initiating events on mitigating systems and their support systems are implicitly reflected via the fault trees.[36] Figure 3-10 shows the loss of safety-related 4.16 kV AC bus event tree (for bus A).

3.1.12 Loss of Nuclear Service Cooling Water Event Tree

This initiating event category includes the loss of NSCW initiating event. The NSCW system has two trains with three pumps in each train. During normal operation, 2 of 3 NSCW pumps in each train are running, while the third pump is in standby. If neither of the NSCW trains can be maintained or placed in normal two-pump operation, operators are directed to trip the reactor and attempt to place one train of NSCW in single-pump operation.[37] If one or both standby pump(s) remain available, operator action (OA-OSW-------H) to align for single-pump operation can be established after the initiator, allowing cooling support for the ECCS pumps in the associated train.

The event progression would be like a transient with all AFW pumps available, since they do not need NSCW or any other cooling water for operation. However, the frequency of a reactor trip due to loss of NSCW (a manual reactor trip is required if two pumps in both train A and train B fail) is much smaller than the transient initiating event frequency, which in turn makes the contribution from the loss of NSCW scenarios with at least one pump in operation very small as compared to other transient contributions. Thus, the loss of NSCW event tree only addresses those sequences initiated by loss of all six NSCW pumps, or those initiated by failure to place at least one train of NSCW in single-pump operation. Key safety-related equipment rendered unavailable by a loss of NSCW includes:

- EDGs (jacket water cooler)
- ECCS pumps (oil and motor coolers)
- CCUs
- CCW pumps (motor coolers) and motor coolers
- ACCW heat exchangers

The loss NSCW event tree follows the general structure for transient initiating events described in Section 3.1.1, with four exceptions. First, a SSIE fault tree (IEFT-LONSCW) is used to

---

[36] If the initiating event is from a loss of safety-related 4.16 kV AC bus A, the battery charging capability for safety-related 125 V DC bus C is also lost. When the train C battery is depleted at 4 hours (the train A, B, and C batteries all have a 4-hour battery life), the turbine-driven AFW pump is rendered unavailable. In addition, RCS hot leg 'B' suction isolation valve is rendered unavailable (i.e., valve remains closed).

[37] These same procedure steps also direct operators to trip the RCPs; and therefore, it is assumed that the RCPs are tripped for the loss of NSCW initiating event.

develop the loss of NSCW frequency based on both the operating components and the standby components. The components in this SSIE fault tree include the pumps, discharge MOVs, and discharge check valves.[38] The IEFT-LONSCW fault tree represents both the frequency of a loss of NSCW leading to a reactor trip and the unavailability of the NSCW to support frontline systems (see Section 5.2.7 for additional information on this SSIE fault tree). The second exception is that RCPSI and RCPSC top events are excluded from this event tree since RCP seal injection and cooling are rendered unavailable by the loss of NSCW.[39] The third exception is that the FAB and FABR top events are excluded from the loss of NSCW event tree, because feed and bleed cooling and subsequent recirculation is not an option if feedwater (AFW or MFW) fails, since no cooing will be available for the ECCS pumps. The last exception is that the CHG top event is excluded, since the charging pumps are also unavailable due to lack of pump cooling. Figure 3-11 shows the loss of NSCW event tree.

3.1.13 Loss of Auxiliary Component Cooling Water Event Tree

This initiating event category includes the loss of ACCW initiating event. A total loss of ACCW flow requires a manual reactor trip and is considered as a special initiating event in the L3PRA project Level 1 model. Loss of ACCW due to the loss of NSCW to the ACCW heat exchangers is not included in this category because the loss of NSCW is modeled as a separate special initiating event. The RCP thermal barrier heat exchangers, RCP lube oil coolers, and the NCP motor coolers lose cooling water on a loss of ACCW. Loss of cooling water to RCP thermal barrier heat exchangers does not cause a significant challenge to the integrity of RCP seals unless operators fail to align the CCPs to provide alternate seal injection (OA-CCP-ALIGN---H). Event tree specific success criteria are provided below, followed by a description of the event tree headings and the event tree structure.

The loss ACCW event tree follows the general structure for transient initiating events described in Section 3.1.1, with four exceptions. First, a SSIE fault tree is used to develop the loss of ACCW frequency based on both the operating components and the standby components. The components in the loss of ACCW SSIE fault tree (IEFT-LOACCW) include the pumps; pump suction and discharge MOVs and check valves; surge tank; and heat exchangers. The IEFT-LOACCW fault tree represents both the frequency of a loss of ACCW leading to a reactor trip and the unavailability of the ACCW to support frontline systems (see Section 5.2.5 for additional information on this SSIE fault tree). The second exception is that the RCPSI top event has been replaced with the RCPSI-LOACCW top event. This top event fault tree models the potential for operators to align the CCPs for alternate seal injection, which as discussed previously is only credited for the loss of ACCW and loss of RCP seal injection initiating events. The third exception is that RCPSC top event is excluded from this event tree since loss of ACCW renders RCP seal cooling unavailable. However, the integrity of the RCP seals is queried if alternate RCP seal injection via the CCPs is unsuccessful in this event tree (represented in the RCPS-BP top event). The fourth exception is that CHG top event is excluded, since the alignment of the CCPs is queried in the RCPSI-LOACCW top event fault tree. Figure 3-12 shows the loss of ACCW event tree.

---

[38] The NSCW cooling towers fans and sprays are not considered as part of the SSIE fault tree, since it is assumed that these failures will result in slower system heat-up and lead to a technical specification-directed, controlled shutdown, instead of a reactor trip.

[39] Only the integrity of the RCP seals is queried in this event tree (as represented in the RCPS-BP top event).

3.1.14 Loss of Reactor Coolant Pump Seal Injection Event Tree

This initiating event category represents a loss of seal injection flow to all RCPs initiated by the loss of flow from the NCP. Loss of RCP seal injection flow from the NCP does not directly cause a reactor trip. If the loss of RCP seal injection flow occurs, operators are directed to check the availability of ACCW. Since the loss of ACCW is separately modeled as a special initiating event, the loss of RCP seal injection event tree does not include the loss of seal injection due to the impacts from loss of ACCW. Thus, it is assumed in this initiating event that ACCW is initially available. After verifying ACCW operation, operators are directed to establish safety grade charging using the CCPs. If safety grade charging is established, the plant may continue its operation and no initiating event (reactor trip) would occur. Otherwise, operators would trip the reactor, resulting in a plant transient.

The loss RCP seal injection event tree follows the general structure for transient initiating events described in Section 3.1.1, with four exceptions. First, a SSIE fault tree is utilized to develop the loss of RCP seal injection (from the NCP) frequency based on both the operating components and the standby components. The components in this SSIE fault tree (IEFT-LOSINJ) include the NCP, charging flow control valves, seal injection filters, and suction/discharge isolation valves. The IEFT-LOSINJ fault tree represents both the frequency of a loss of normal RCP seal injection and the failure to align the CCPs for alternate injection leading to a reactor trip (see Section 5.1.17 for additional information on this SSIE fault tree). The second exception is that the failure of RPS (and subsequent ATWS) is excluded from this event tree since this initiating event assumes a manual reactor trip has occurred.[40] The third exception is that the RCPSI top event is excluded from this event tree because both normal RCP seal injection and alternate injection is queried in the IEFT-LOSINJ top event fault tree. The fourth exception is that the CHG top event is excluded, since the alignment of the CCPs is also queried in the IEFT-LOSINJ top event fault tree. Figure 3-13 shows the loss of RCP seal injection event tree.

3.1.15 Inadvertent Safety Injection Event Tree

This initiating event category includes transients initiated by an inadvertent SI signal due to hardware failure or human error. An SI signal causes the following:

- Reactor trip
- Turbine trip
- MFW pump trip and system isolation
- NCP pump trip
- Motor-driven AFW pump start
- ECCS pump start (CCPs, SI pumps, and RHR pumps)

[40] This modeling assumption is potentially non-conservative and has been identified as a future model revision in Appendix D.

- EDG start[41]
- Containment isolation (Phase A)

This initiating event assumes that at least one CCP is injecting into the RCS. An SI actuation trips the NCP; therefore, RCP seal injection is provided by the running CCP(s). After the reactor trip, the ECCS pumps (especially the CCPs) should be terminated to prevent RCS inventory lost though pressurizer PORVs/SRVs.[42]

The inadvertent safety injection event tree follows the general structure for transient initiating events described in Section 3.1.1, with three exceptions. First, the RCPSI, RCPSC, CHG, and SAFESTABLE top events are excluded from this event tree because the initiating event assumes that a CCP is running, thereby supplying RCP seal injection. The second exception is that the AFW (only) top event fault tree is used instead of the combined FW top event (due to the trip of the MFW pumps and system isolation). The third exception is the inclusion of the TSI and PZRR top events to model the potential for a pressurizer PORV/SRV failing to reclose, which causes a consequential SLOCA. Figure 3-14 shows the inadvertent SI event tree.

3.1.16 LOOP Event Trees

This initiating event category includes LOOP events occurring in the following four categories:

- Plant-centered
- Grid-related
- Switchyard-related
- Weather-related

For all the above LOOP events, if the EDGs start and run, they can provide electrical power for the mitigating systems. However, certain systems will be rendered unavailable due to the loss of nonsafety-related AC power; including:

- The control rod drive mechanisms (CRDMs) lose power due to the RPS motor-generators being deenergized; therefore, only mechanical failure of the control rods to insert into the reactor will lead to an ATWS.
- The MSIVs will close due to the loss of instrument air caused by the deenergization of instrument air compressors (supplied by nonsafety-related AC power); therefore, there is no possibility of the consequential SSB downstream of the MSIVs due to failed open turbine control/stop valves or TBVs. In addition, the TBVs will be unavailable for decay heat removal.

---

[41] The EDGs start but will not load onto their respective safety-related 4.16 kV AC buses unless the bus(es) lose power [i.e., an under-voltage condition exists on the bus(es)].

[42] In addition to terminating the CCPs, operators must align the one running CCP to the normal charging path, including establishing letdown.

- The circulating water pumps and condensate pumps will be deenergized (supplied by nonsafety-related AC power); therefore, the MFW pumps are rendered unavailable. In addition, the MFRVs will be de-energized.

- The NCP will be rendered unavailable, since it cannot be powered from the EDGs.[43]

The initiating event frequencies and LOOP recovery probabilities for each of the four LOOP categories are different. However, the event tree structure is the same for all four LOOP categories and follows the general structure for transient initiating events described in Section 3.1, with four exceptions. First, a top event representing the start and loading of the EDGs to their respective safety-related AC buses is included in the LOOP event trees (see Section 5.1.7 for additional information on the EPS fault tree). If either EDG successfully starts and loads to its respective bus, the event progression after the LOOP is like that for transients. If both EDGs are unable to supply their respective buses, the sequence is transferred to the SBO event tree (see Section 3.4.4 for additional information). The second exception is that the TT top event is not included because the MSIVs close on loss of power, isolating the turbine and TBVs. The third exception is that the RCPSI top event is excluded, because the NCP is rendered unavailable during a LOOP initiating event. The fourth exception is that the AFW (only) top event fault tree is used instead of the combined FW top event (due to the isolation of the main steam and main feedwater lines). Figure 3-15 shows the LOOP (grid-related) event tree.

[43] Alternate seal injection via the CCPs is not credited during a LOOP initiating event, because there is insufficient time available for operators to get through the applicable procedures within the required 13 minutes.

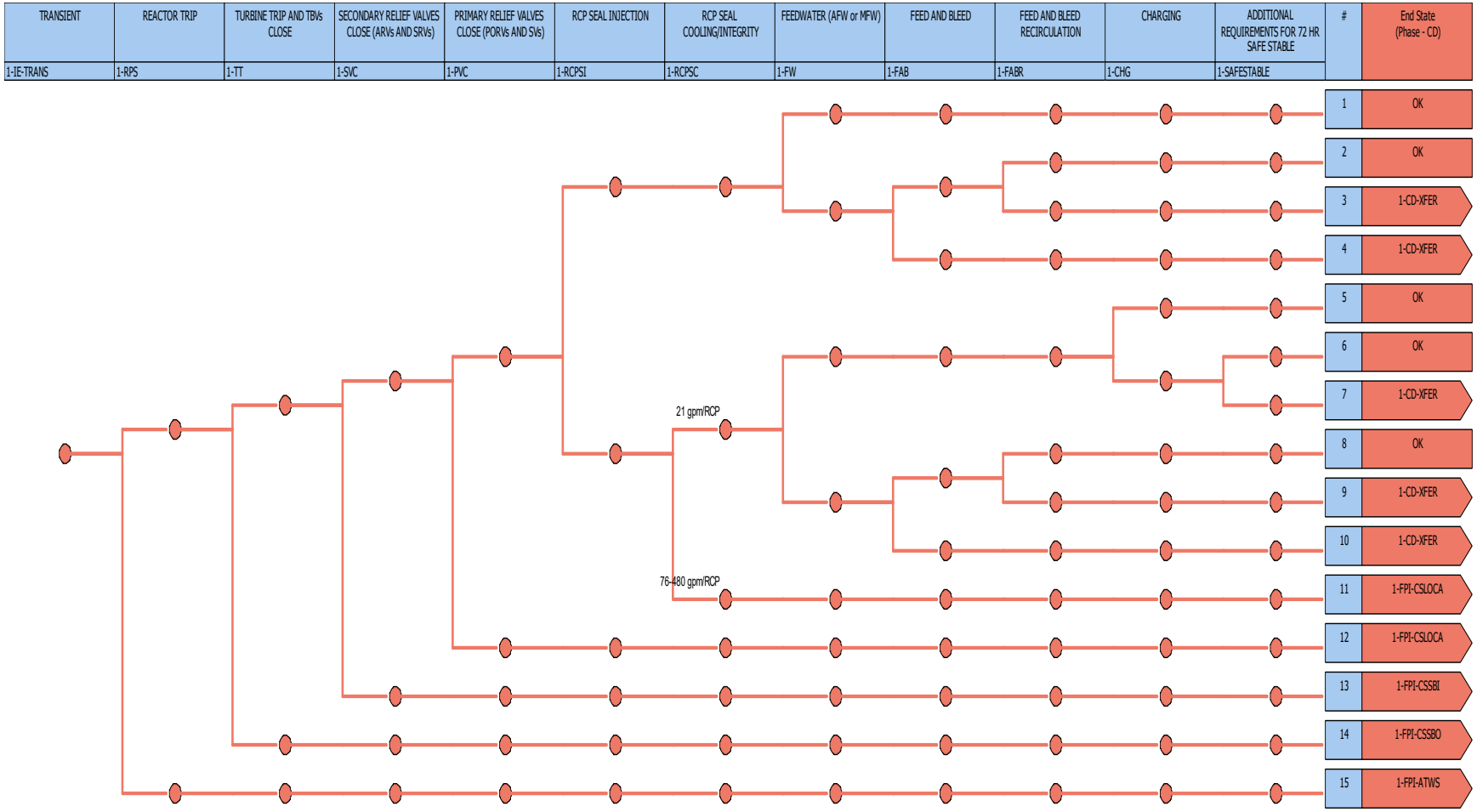


Figure 3-1 General Event Tree Structure for Transients

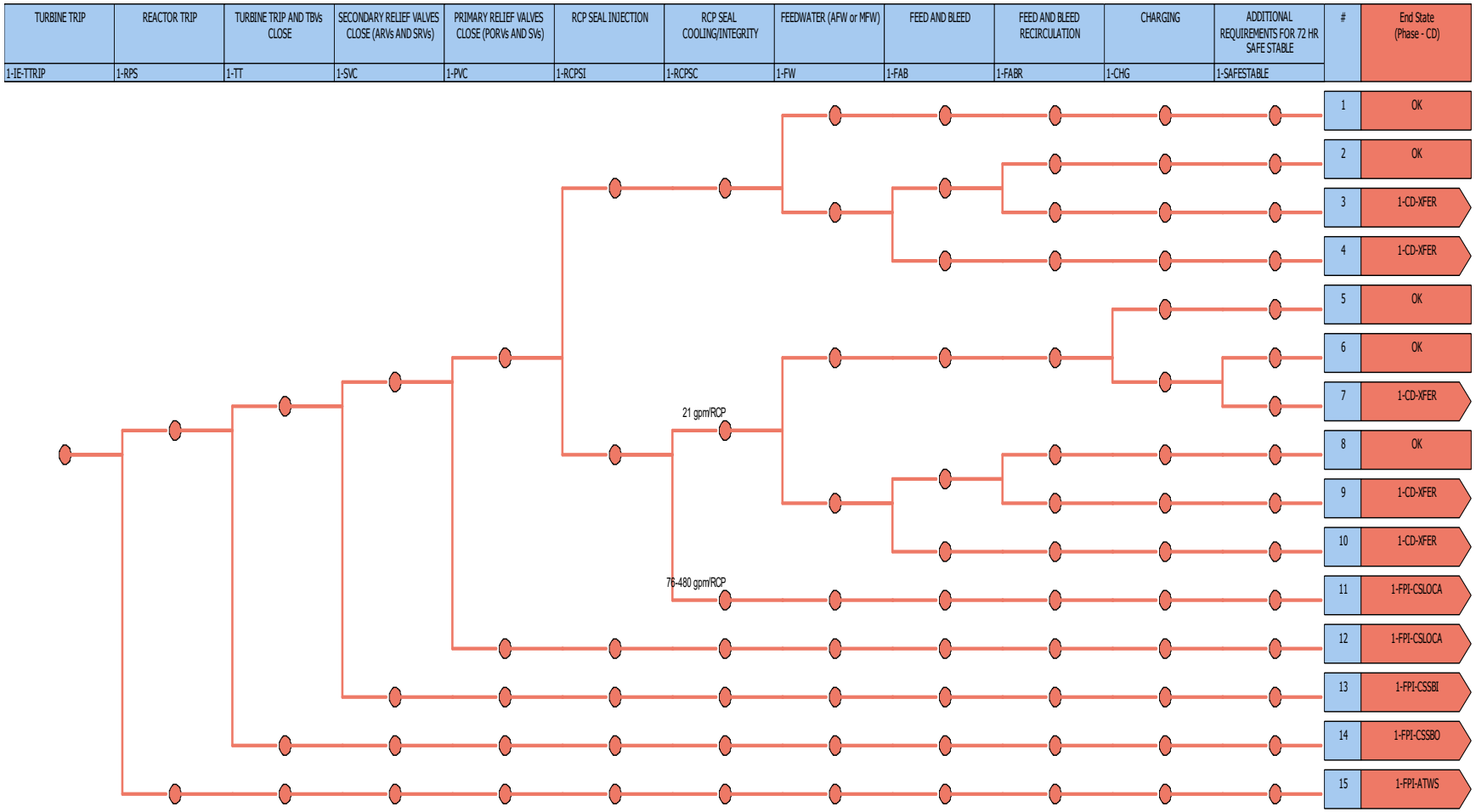


Figure 3-2 Turbine Trip Event Tree

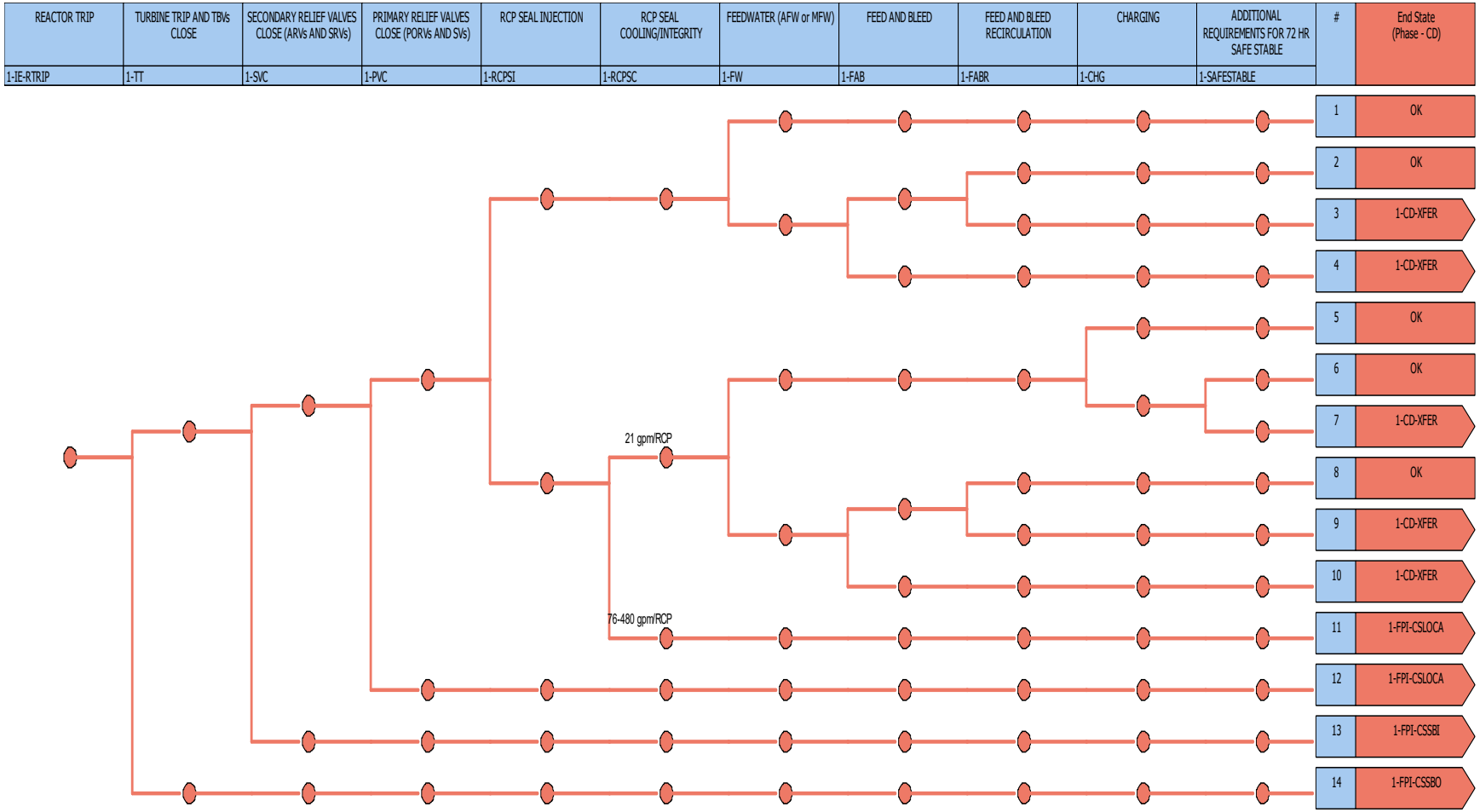


Figure 3-3 Reactor Trip Event Tree

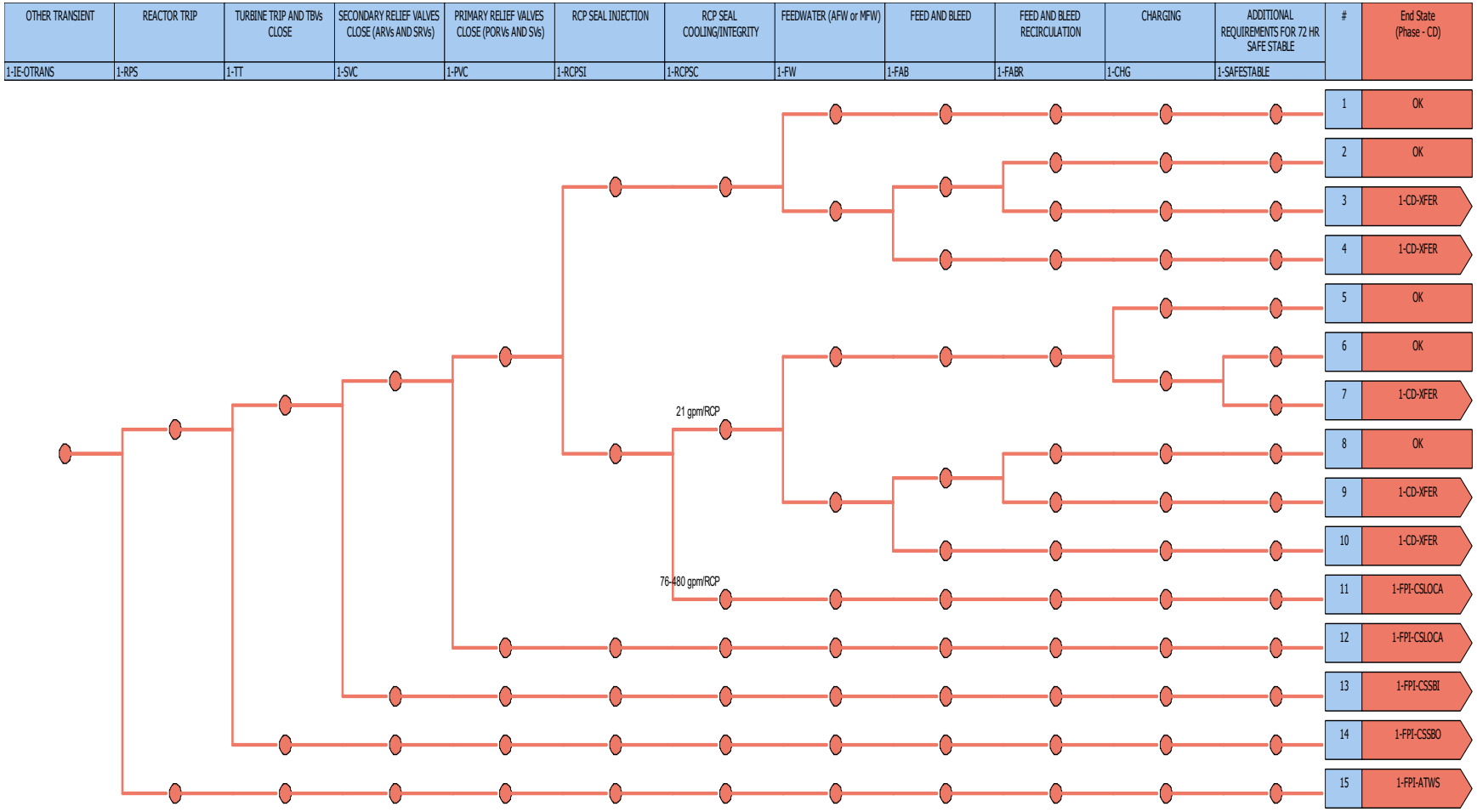


Figure 3-4 Other Transients Event Tree

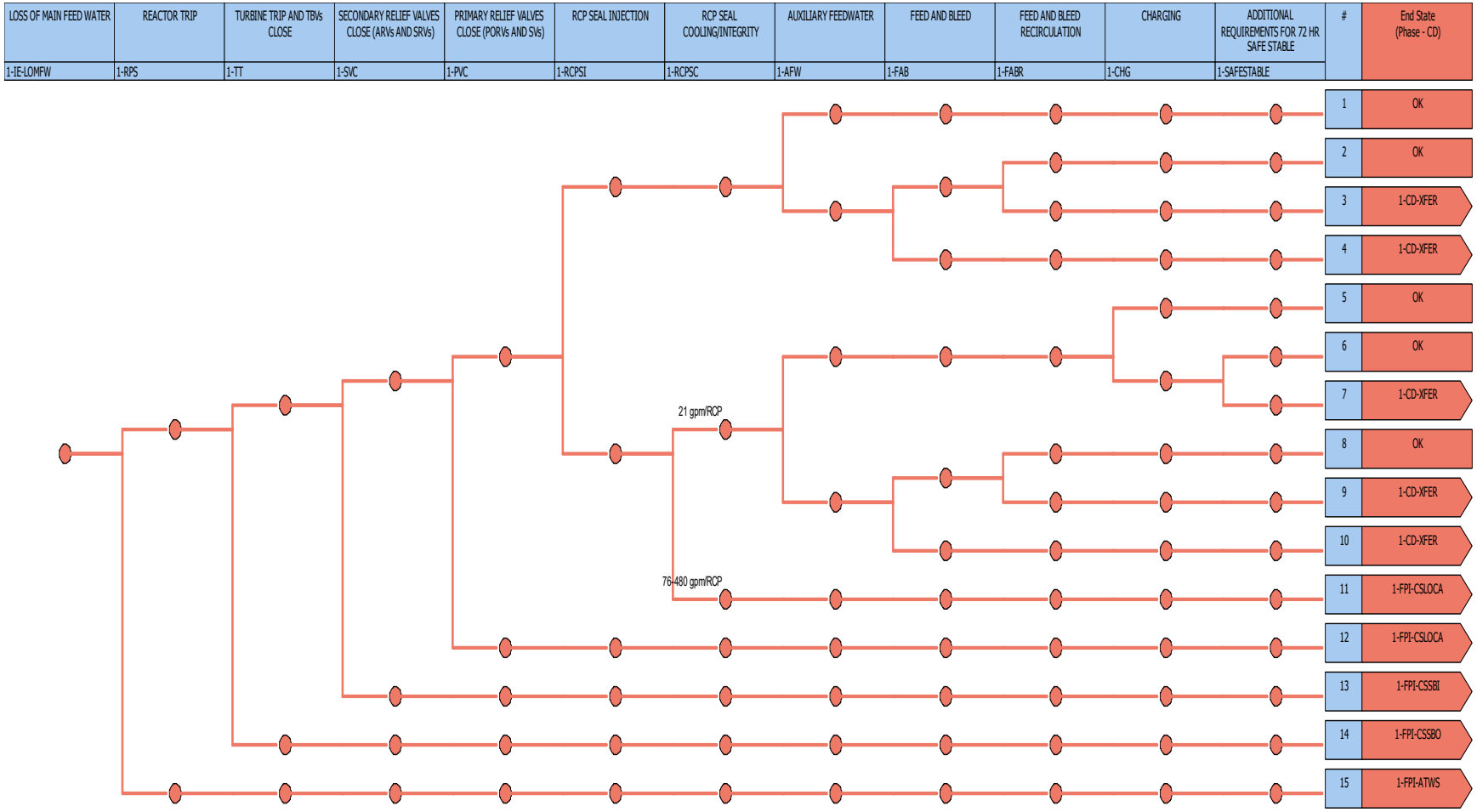


Figure 3-5 Loss of MFW Event Tree

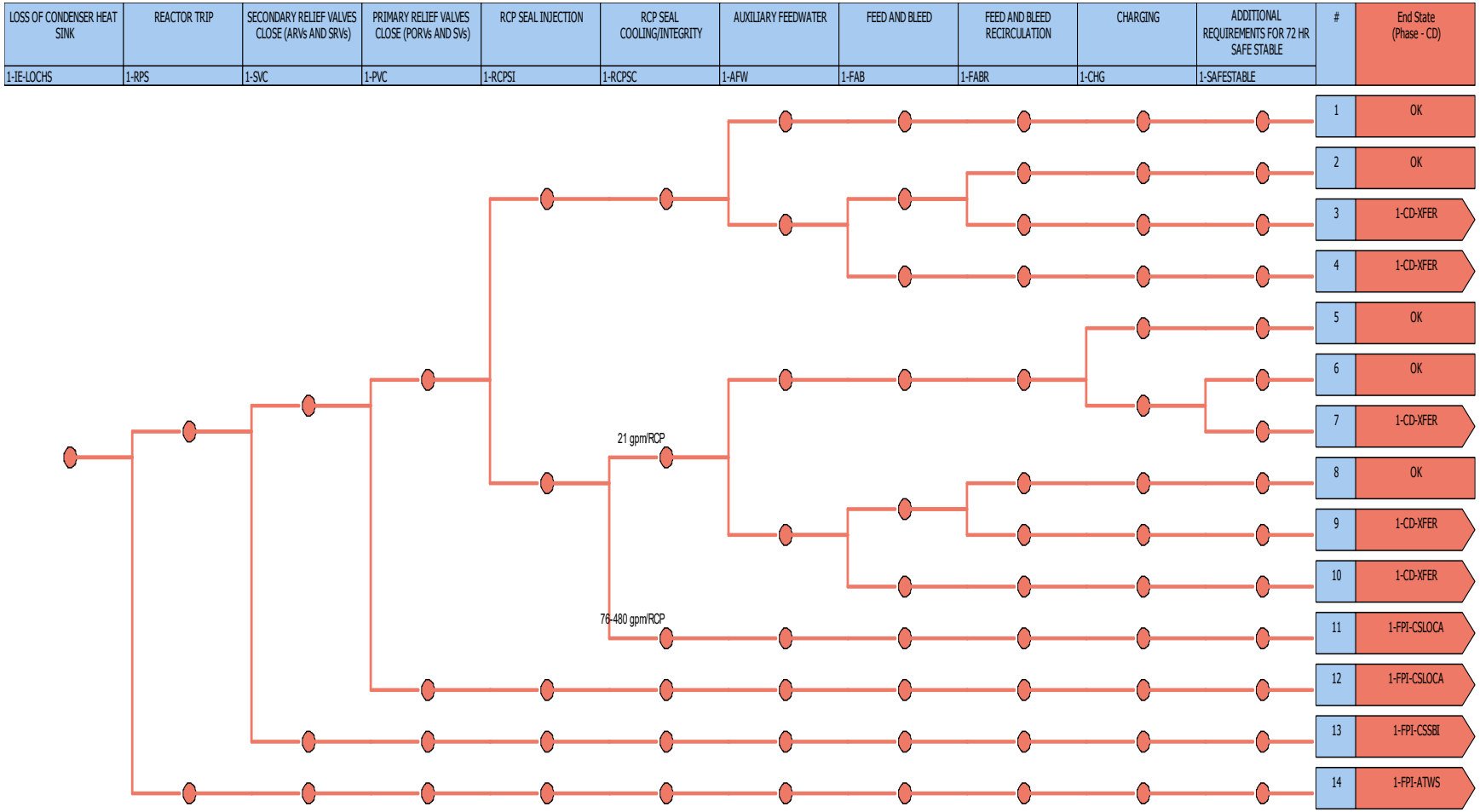


Figure 3-6 Loss of Condenser Heat Sink Event Tree

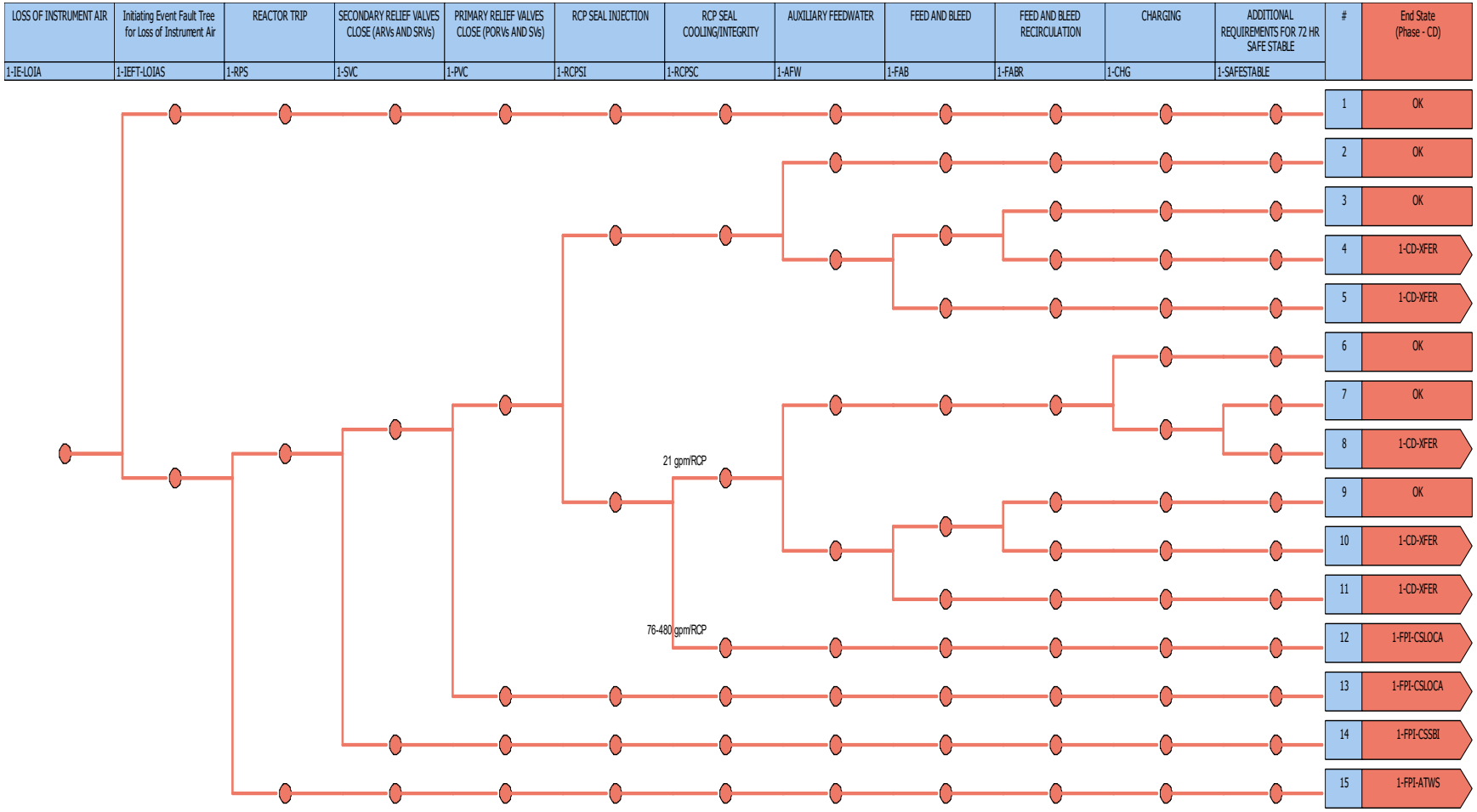


Figure 3-7 Loss of Instrument Air Event Tree

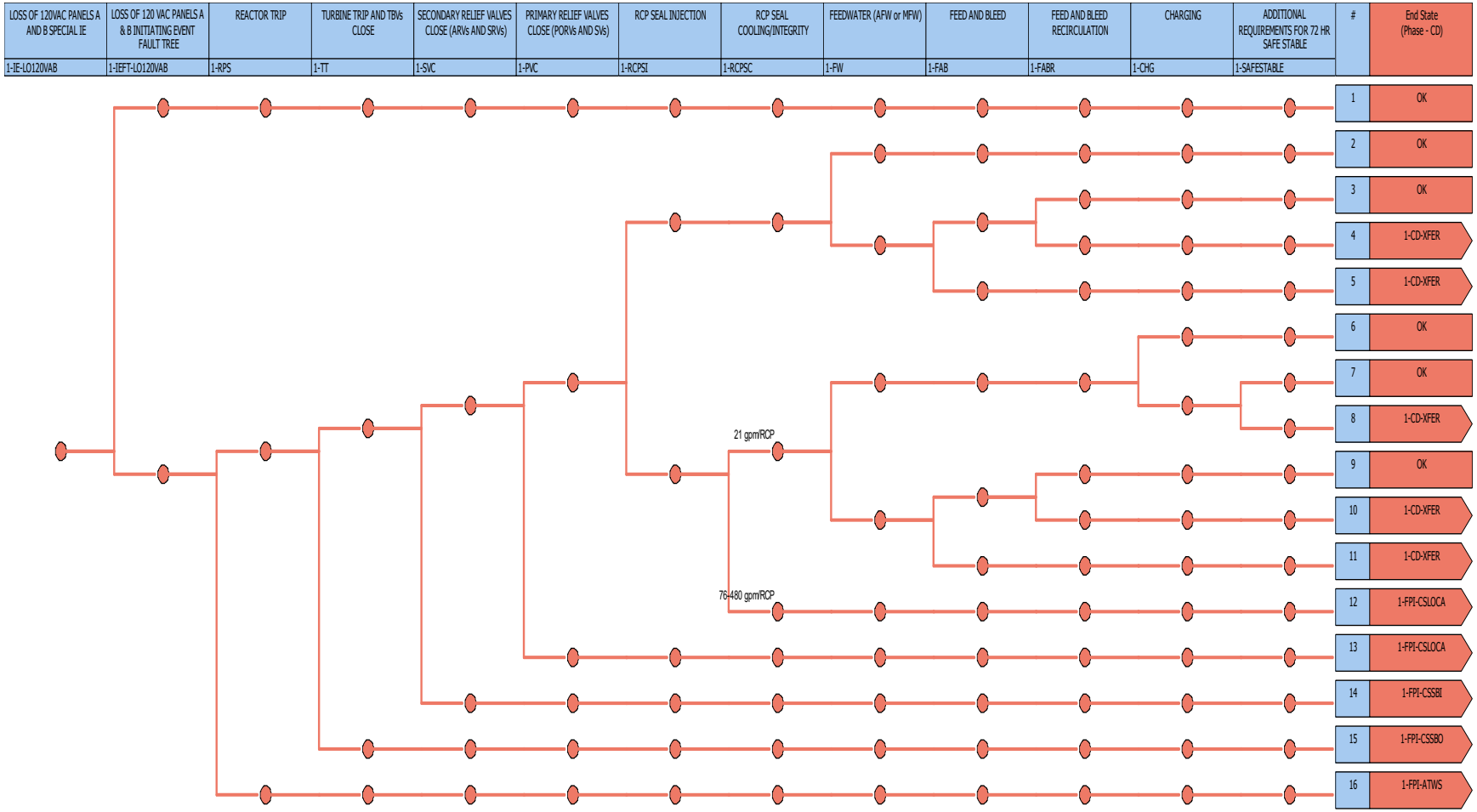


Figure 3-8 Loss of Two Safety-Related 120 V AC Panels Event Tree

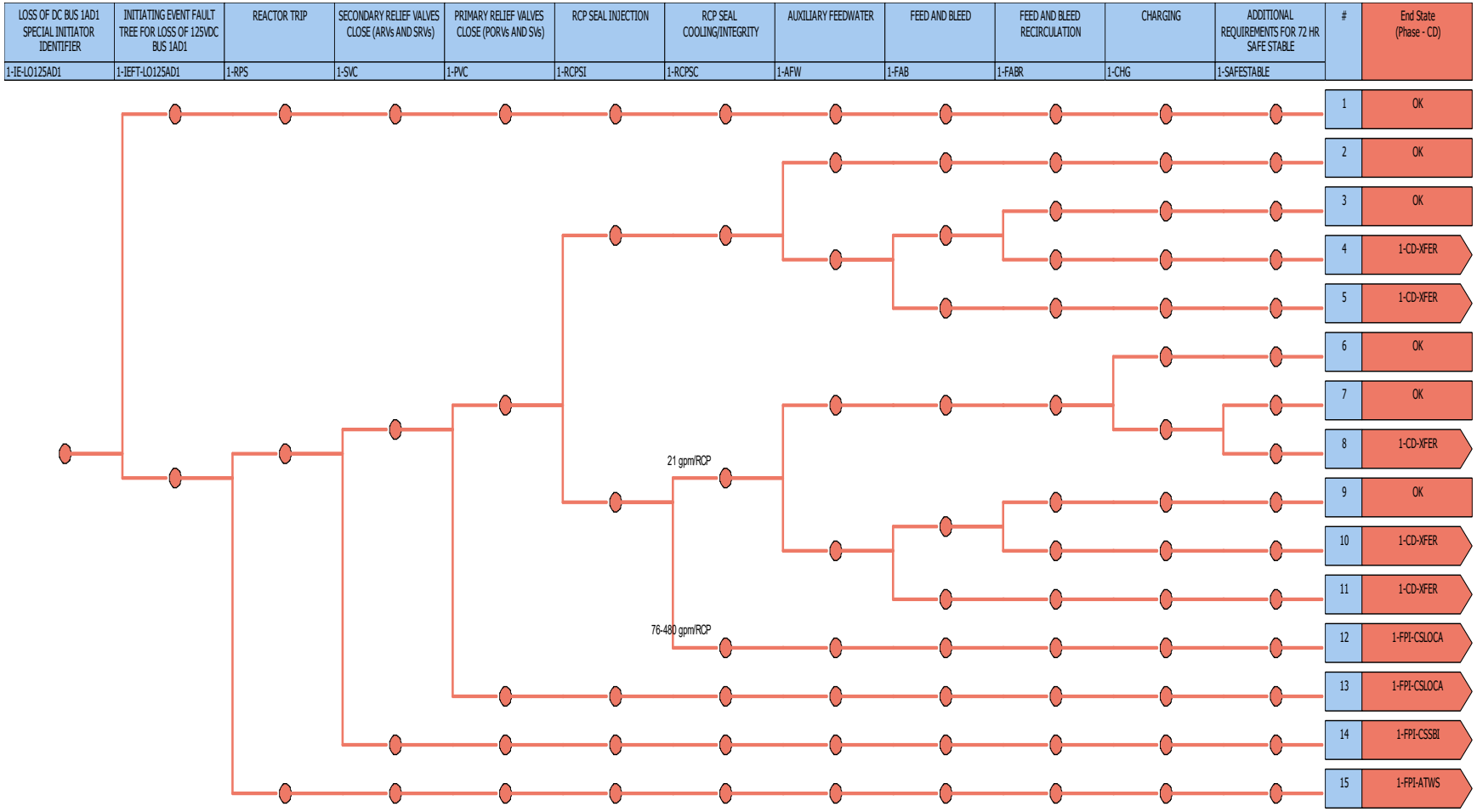


Figure 3-9 Loss of Safety-Related 125 V DC Bus Event Tree

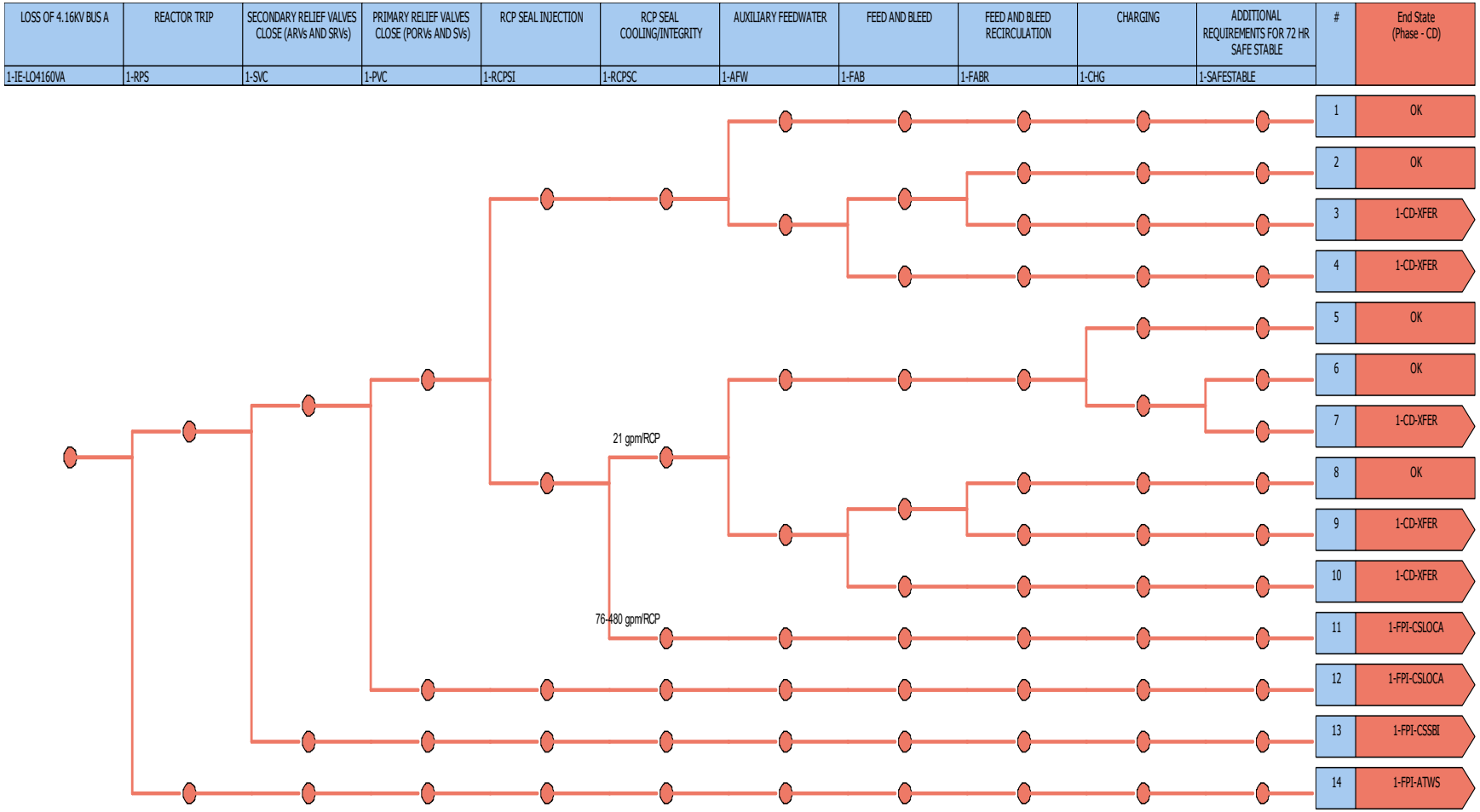


Figure 3-10 Loss of 4.16 kV Safety-Related AC Bus Event Tree

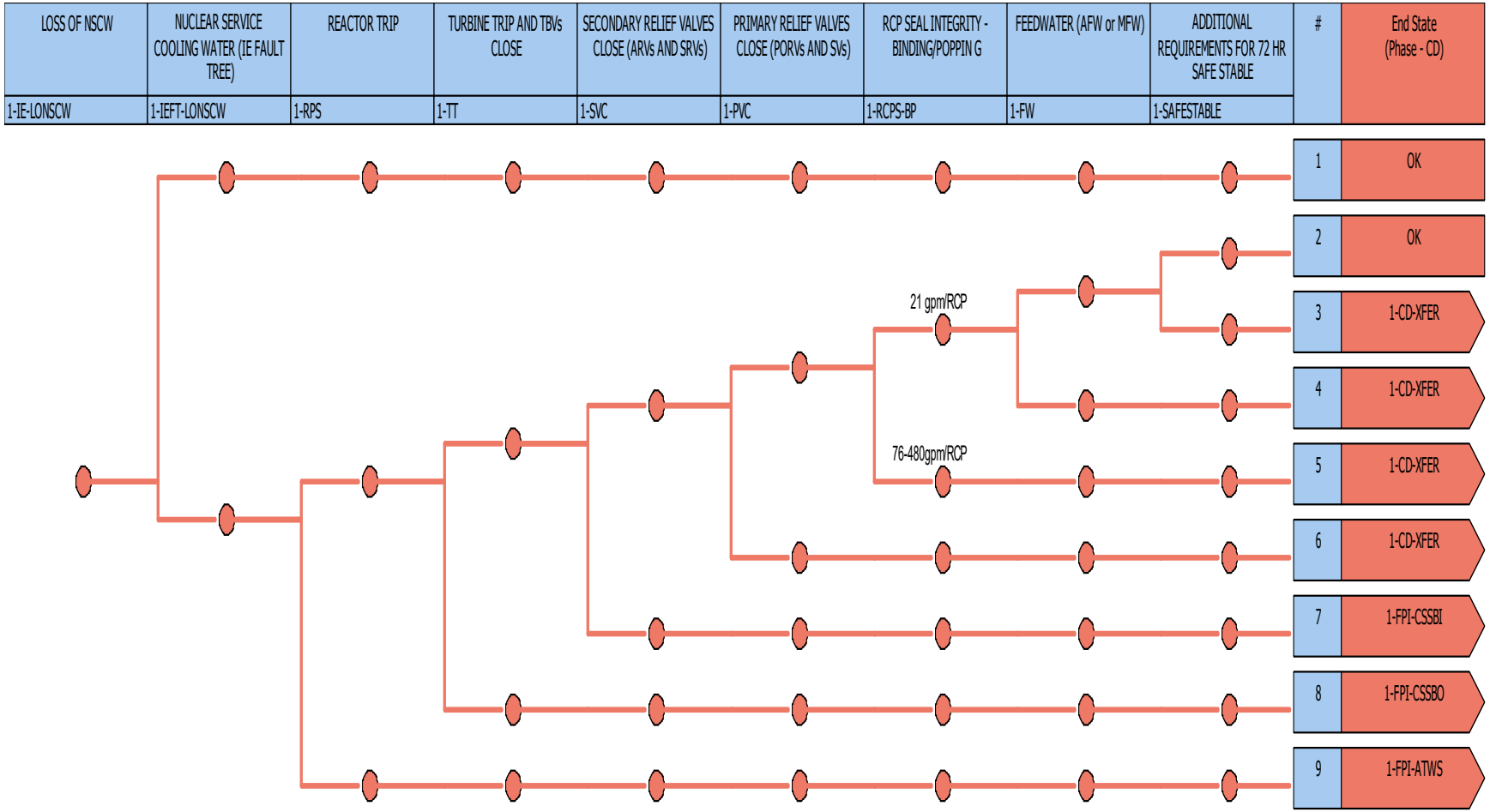


Figure 3-11 Loss of NSCW Event Tree

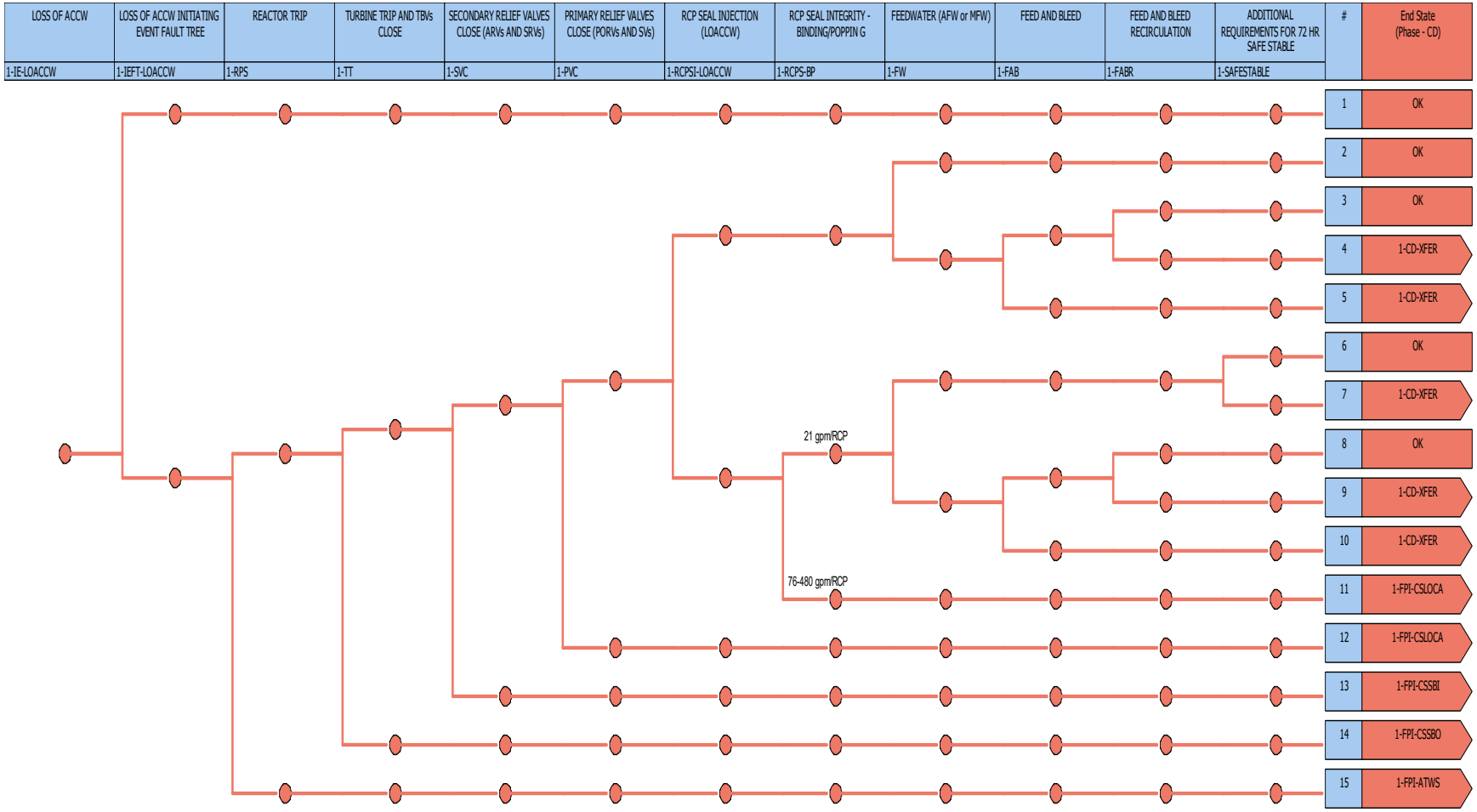


Figure 3-12 Loss of ACCW Event Tree

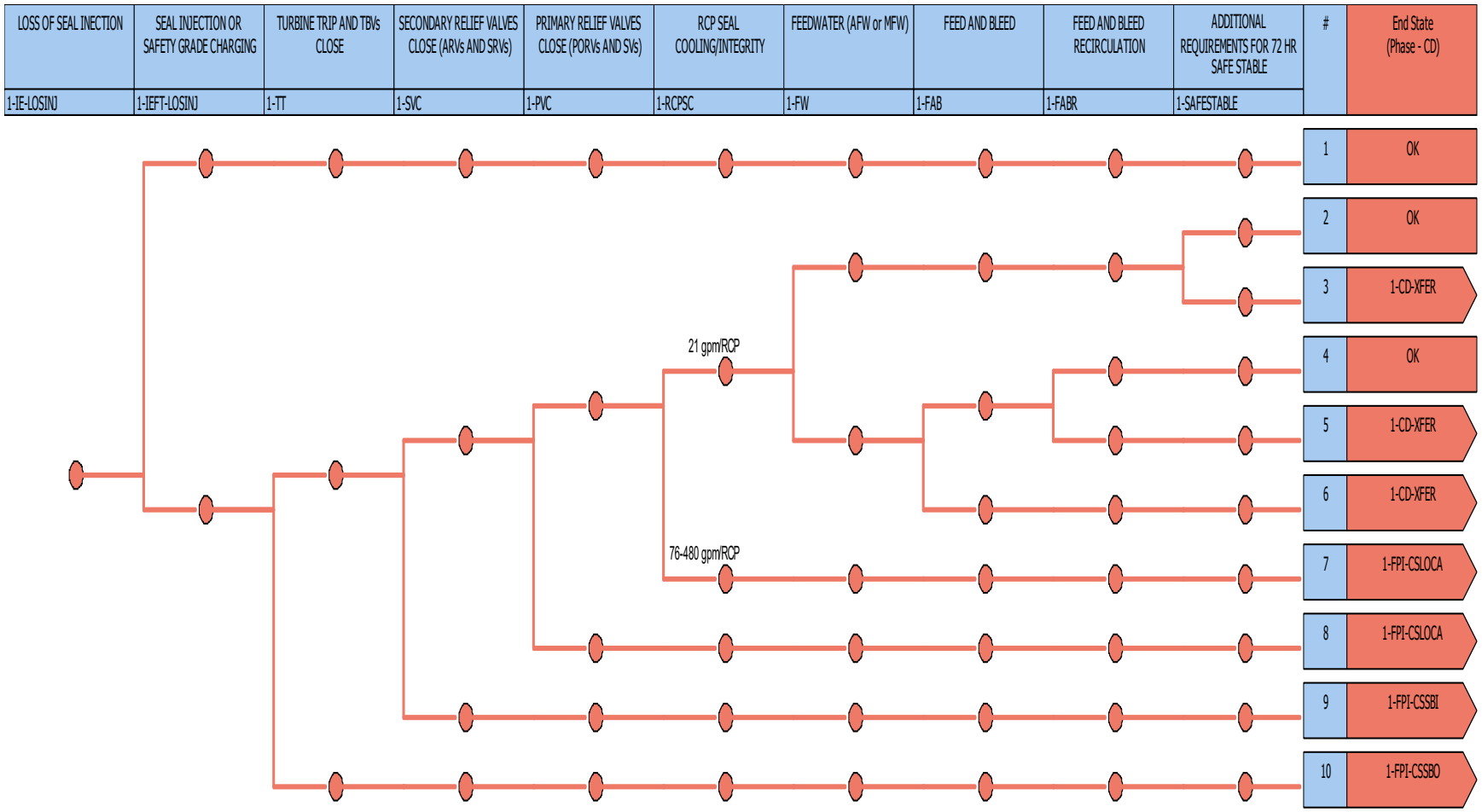


Figure 3-13 Loss of RCP Seal Injection Event Tree

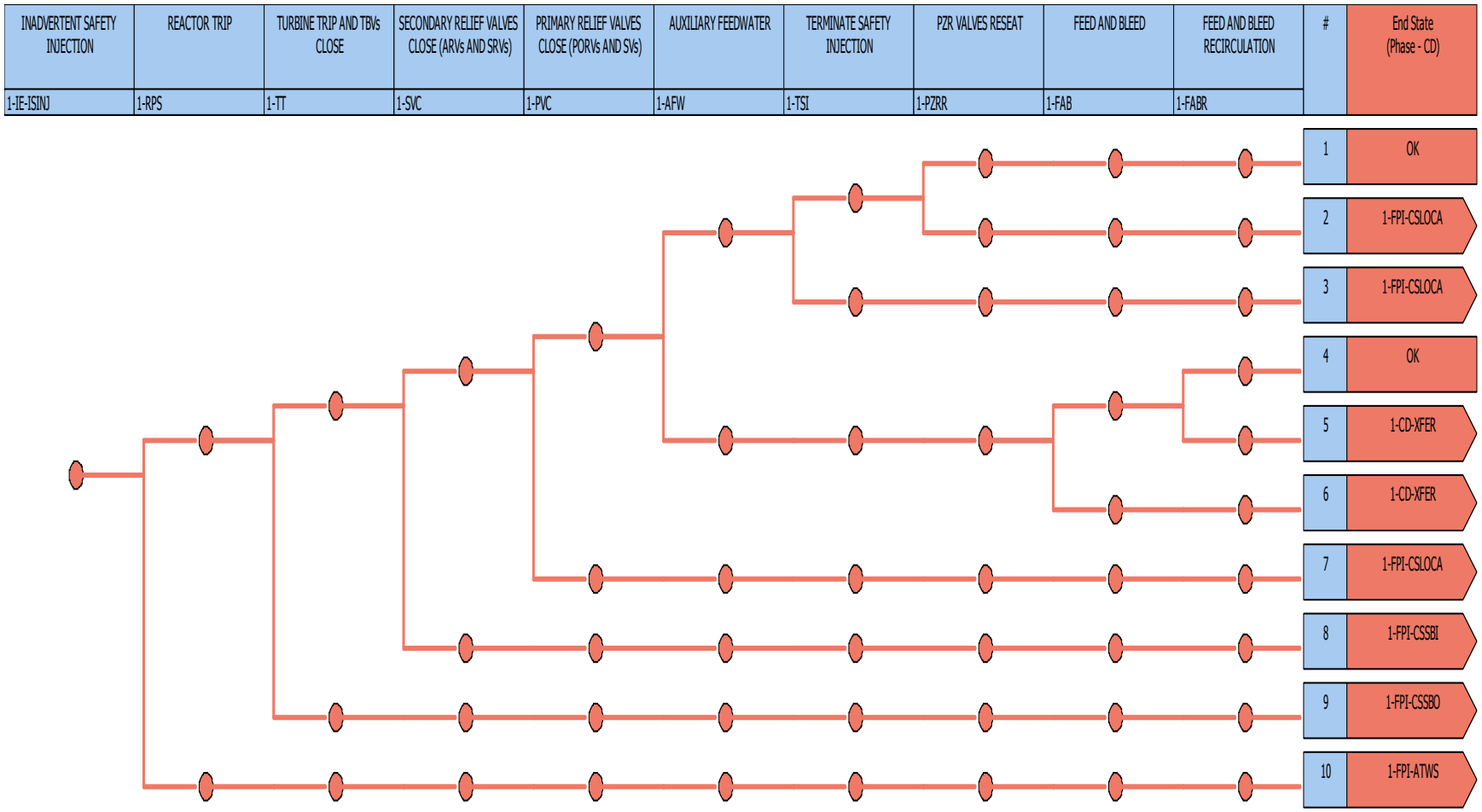


Figure 3-14 Inadvertent SI Event Tree

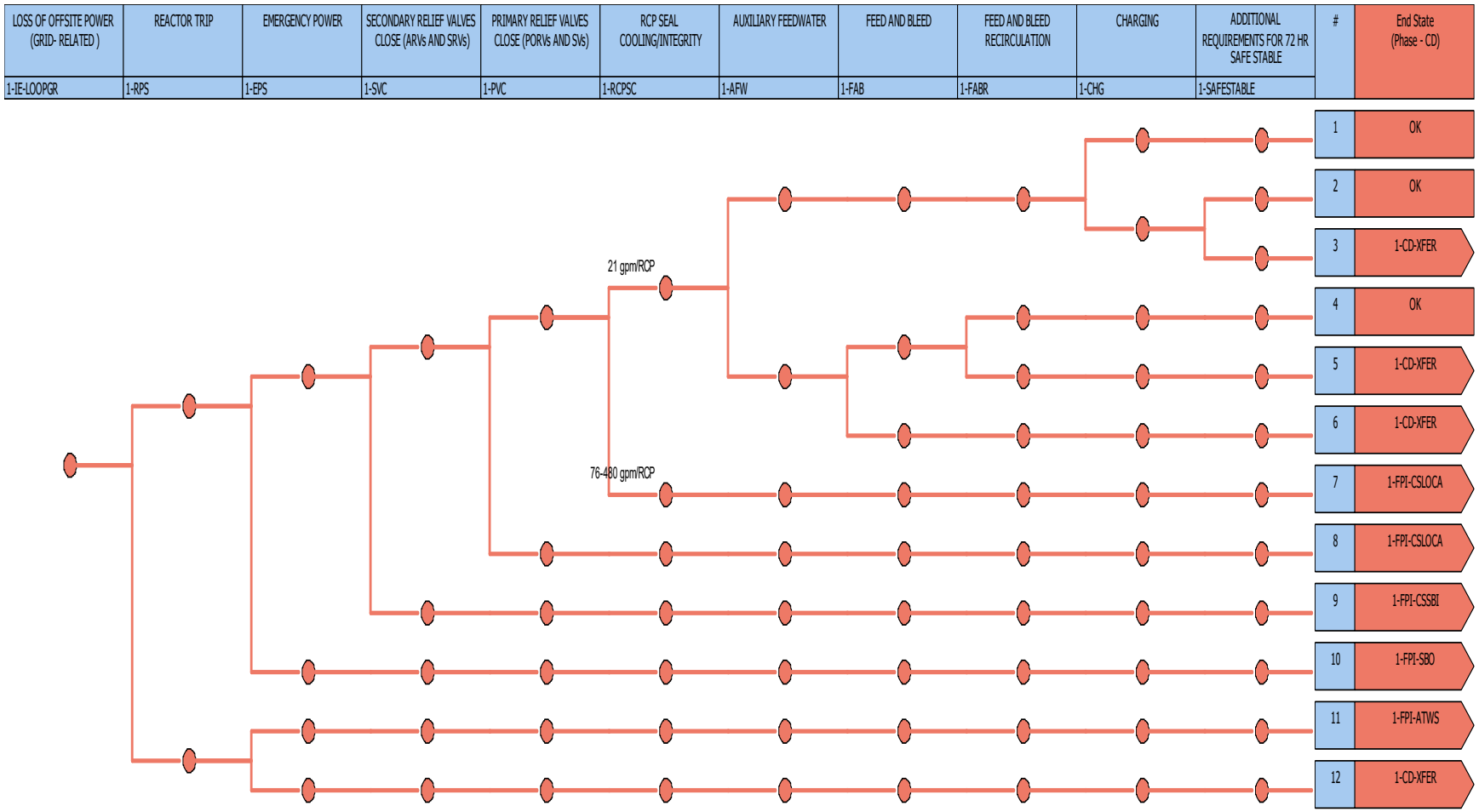


Figure 3-15 LOOP (Grid Related) Event Tree

3.2 Secondary-Side Break Initiating Event Trees

As discussed previously, in the L3PRA project separate initiating event categories are included for secondary-side breaks occurring upstream and downstream of the MSIVs (SSBI and SSBO, respectively). More specifically, the SSBI initiating event category includes steam line breaks upstream of the MSIVs and feedwater line breaks downstream of the main feedwater isolation valves (MFIVs). Also included in the SSBI initiating event category is the failure of one or more SG ARVs or SRVs.[44] The SSBO initiating event category includes steam line breaks downstream of the MSIVs and feedwater line breaks upstream of the MFIVs. Also included in the SSBO initiating event category is the failure of one or more TBVs to reclose.[45]

The major difference between the SSBI and SSBO event trees is in the isolation of the faulted SG, which is treated at the fault tree level. These initiating event categories were developed because an unisolable secondary-side break could lead to a severe cooldown of the reactor coolant system. The event tree structure for SSB initiating events is used to represent the interactions among several functional event groupings. The first grouping (as represented by the RPS top event) involves reactivity control. If the reactor trip fails, core damage is assumed due to the positive reactivity addition.[46]

The second grouping (as represented by the PI-SGTR top event) addresses the probability of a consequential, pressure-induced SGTR. This top event combines the probability of having a significant tube flaw (which is necessary to result in tube failure) with the probability that the ensuing pressure-induced SGTR would go to core damage. The latter term (i.e., the conditional probability of core damage) is calculated using a fault tree representation of the SGTR event tree (see Section 3.3.5 for additional information). [Note, during a SSB initiating event, the pressurizer PORVs/SRVs would not be challenged due to increasing RCS pressure because the overcooling transient would decrease RCS pressure; therefore, the PVC top event (included in the transient event trees) is not included in the SSBI or SSBO event trees. However, the PORVs and/or SRVs will open due to the SI actuation and the CCP(s) overfilling the pressurizer; this modeling is included in the SSB-CSLOCA fault tree.]

The third grouping (as represented by the SGI-SSBI or SGI-SSBO top events) represents whether the SSB has been isolated and the over-cooling transient terminated. For a SSBI initiating event, the faulted SG must be isolated by closure of its MSIVs and MFIVs (including the bypass valves). In addition, AFW injection valves to the faulted SG and the steam valves for the turbine-driven AFW pump (if at least one motor-driven AFW pump is running) need to be manually closed (SSB-XHE-ISOLATION).[47] For SSBO initiating event, the over-cooling transient can be terminated if the MSIVs and MFIVs (including bypass valves) are closed for all

---

[44] A failure of one SG ARV or SRV will result in an effective break diameter greater than 1-inch; and therefore, is included in NUREG/CR-5750 category K. Note that NUREG/CR-5750 category QK4 events are comprised of leaks of less than a 1-inch diameter line break (e.g., flange and packing leaks).

[45] A failure of one TBV to reclose will result in an effective break diameter greater than 1-inch; and therefore, is included in NUREG/CR-5750 category K.

[46] Core damage during these ATWS scenarios is likely to be due to the departure of nucleate boiling (DNB), and not due to core uncovery as it is typically considered in the rest of the L3PRA Level 1 model.

[47] Procedures also direct operators to close the faulted SG's sample and blowdown valves. However, based on discussion with NRC technical training center staff, it was determined that the failure to close these valves would not appreciably affect SG isolation; therefore, the modeling of these valves is not included in SGI-SSBI fault tree.

four SGs. The MSIVs (high containment pressure or low steam line pressure) and MFIVs (SI actuation) receive an automatic closure signal.[48]

The fourth grouping (as represented by the RCPSI-CCPs, RCPSC, and SSB-CSLOCA top events) queries whether a consequential SLOCA occurs, either due to seal failure or via the pressurizer PORVs and SRVs. A SSB initiating event will cause an SI actuation, which trips the NCP; and therefore, normal RCP seal injection will be lost. However, if the CCPs successfully start and run (during the high-pressure injection phase of the ECCS), they will provide high pressure water injection flow to the RCP seals. The RCP seal cooling fault tree (RCPSC top event) also queries the integrity of RCP seals given a loss of all RCP seal injection/cooling. If RCP seal injection is lost, but either seal cooling to the thermal barrier heat exchangers or RCP seal integrity is maintained, the RCP seal leakage is assumed to be 21 gpm per RCP.[49] If the RCP seals fail (due to loss of both seal injection and seal cooling), the sequence is transferred to the consequential SLOCA event tree. If CCPs successfully provide high-pressure injection (and, therefore, seal injection), then operators must terminate SI and align a CCP for normal charging (including establishing letdown) to prevent a CSLOCA via the pressurizer PORVs or SRVs. Additional information on RCP seal failure modeling is provided in Section 8.4.

The fifth grouping (as represented by the AFW, FAB, and FABR top events) queries whether early and late decay heat removal are successful. Unless there is a consequential LOCA from a stuck-open PORV/SRV or the failure of RCP seals, short-term inventory control is only needed if feed and bleed is initiated. Typically, early decay heat removal is provided by the AFW system to the SGs, with the steam removal provided via the SG ARVs or SRVs.[50] In addition to providing short-term decay heat removal, AFW provides long-term decay heat removal to a safe and stable end-state as long as RCP seal leakage remains at the nominal 3–5 gpm per RCP.[51] If AFW flow to the SGs is not available and/or no steam removal path exists, operators will be directed to initiate feed and bleed cooling (represented by the FAB top event) using high-pressure injection and the pressurizer PORVs.[52] Long-term decay heat removal after initial feed and bleed cooling requires operators to switch to HPR, as represented by the FABR top event. The heat sink for recirculation is provided by the RHR heat exchangers or the CCUs. Failure of either early or late decay heat removal results in core damage.

The final grouping (represented by the SAFESTABLE top event) queries whether the plant is safe and stable at 72 hours for transients with elevated RCP seal leakage, but for which no consequential LOCA has occurred. If RCP seal injection is lost, but seal cooling to the thermal barrier heat exchangers or RCP seal integrity is maintained, seal leakage is assumed to increase from nominal (3–5 gpm per RCP) to 21 gpm per RCP. At this leakage rate, core damage could occur prior to 72 hours unless other mitigation (in addition to AFW) is successful. Operators would enter one of the CSFST procedures for loss of core cooling (FR-C.1) or

---

[48] For SSBs with isolation failure, there is the possibility that CST 1 will be emptied prior to 24 hours from accident initiation. The SSB event trees in the L3PRA Project Level 1 model do not currently include the requirement for CST refill for failure of SG isolation scenarios, which is potentially non-conservative. However, this is expected to have a negligible impact on SSB CDF.

[49] This assumption is conservative for scenarios with successful RCP seal cooling (via ACCW through the thermal barrier heat exchangers).

[50] The SI actuation will cause the trip of the MFW pumps and system isolation. The MSIV closure will render the TBVs unavailable.

[51] Additional CST inventory is needed earlier than 24 hours if the SSB is not terminated. In addition, CST makeup for AFW to provide long term decay heat removal for at least 72 hours is needed if the SSB is terminated.

[52] The SI pumps are not credited for feed and bleed cooling during transients.

inadequate core cooling (FR-C.2). These procedures direct the operators to cooldown and depressurize the plant by depressurizing the SGs to 200 pounds per square inch (psi) using the TBVs (which will be unavailable during a SSB) or the SG ARVs. This depressurization will allow the accumulators to inject in the RCS, thus providing makeup. Failure of the cooldown/ depressurization, injection from the accumulators, or CST inventory makeup results in core damage before 72 hours. See Section 8.3 for additional information on the requirements for the 72-hour safe and stable end-state. Figure 3-16 shows the SSBI event tree.

The top events used in SSBI and SSBO event trees and their associated success criteria are provided below.

IE-SSBI or IE-SSBO — Secondary-side break upstream of the MSIVs/downstream of the MFIVs initiating event or a SSB downstream of the MSIVs/upstream of the MFIVs initiating event.

RPS — This top event represents the success or failure of RPS to insert enough negative reactivity by the control rods to shut down the reactor. If automatic reactor trip fails, operator action is necessary to manually trip the reactor (OA------MANRTH or RPS-XHE-XE-NSGNL, depending on whether a reactor trip signal is present). If RPS fails during a SSBI or SSBO initiating event, core damage is assumed due to the positive reactivity addition. Additional information on the RPS fault tree modeling is provided in Section 5.1.37.

PI-SGTR — This top event represents the probability of a pressure-induced SGTR due to SSB. Following a SSB event (without an ATWS), a SG tube leak may result from a pressure differential across the tubes that exceeds the reference plant design limit of 1600 psi. If the secondary-side pressure drops suddenly to atmospheric pressure, the pressure difference across the tubes can be as high as 2250 psi. Such a pressure difference can occur with larger size SSBs. Even then, without the existence of deep existing flaws (beyond the tube plugging criteria), this pressure difference is not expected to cause a consequential SGTR. The upper branch of this event tree node continues the SSB event without an ensuing SGTR. The lower branch means that a consequential SGTR has occurred. In that case, this top event captures the probability of having a sufficiently deep flaw along with the probability that the ensuing tube rupture will proceed to core damage (using a fault tree representation of the relevant top event fault trees from the SGTR event tree), bypassing the remaining event tree nodes in the SSB event tree. The SSB and the consequential SGTR events are postulated to occur within a very short time (within seconds or minutes); otherwise, the RCS pressure will also drop due to overcooling by the large SSB initiating event, reducing the pressure difference across the SG tubes. This means that consequential SSB events involving the failure of only one or two valves (e.g., turbine control/stop valves, TBVs, SG ARVs or SRVs) may not result in thermal-hydraulic conditions that would have the potential for consequential SGTR to occur. Nevertheless, the PI-SGTR top event fault tree is applied consistently across the SSB initiators and consequential SSB event trees as a simplifying (and inclusive) assumption that is not expected to overly impact model results. Additional information on the PI-SGTR fault tree modeling is provided in Section 5.1.31.

SGI-SSBI or SGI-SSBO	This top event represents the success or failure of isolating the faulted SGs in a SSB event. The success criteria for faulted SG isolation are different between SSBI and SSBO initiating events. For SSBI, the faulted SG can be isolated by closure of its MSIVs and FWIVs (including bypass valves), because the break is not in the common steam or feedwater header [AFW flow to the faulted SG also must be manually isolated (SSB-XHE-ISOLATION)].[53] The faulted SG can also be isolated by closing MSIVs and feedwater valves on the other three (intact) SGs and terminating AFW flow to the faulted SG. For SSBO, the MSIVs and MFIVs (including bypass valves) in all four SGs need to be closed to terminate the SSB. AFW flow is not required to be isolated in a SSBO case if steam and feedwater lines are isolated. Additional information on the SGI-SSBI and SGI-SSBO fault tree modeling is provided in Section 5.1.42.
RCPSI-CCPS	This top event represents the success or failure of RCP seal injection via the CCPs during the high-pressure injection phase of ECCS given an SI actuation.[54] If RCP seal injection fails, seal leakage is assumed to increase to at least 21 gpm per RCP (higher leakage rates may occur depending on the success or failure of RCP thermal barrier cooling—see RCPSC below). Additional information on the RCPSI fault tree modeling is provided in Section 5.1.36.
RCPSC	The top event represents the success or failure of RCP seal cooling from the thermal barrier heat exchangers (cooled via ACCW). If RCP seal cooling fails, the integrity of the seals is challenged. Given the loss of all RCP seal cooling and injection, RCP seals have approximately 21 percent chance of failure. In addition, operator failure (RCS-XHE-XM-TRIP) to trip the RCPs will also result in failure of RCP seals. A failure of RCP seals is assumed to result in a consequential SLOCA; and therefore, the sequence is transferred to the consequential SLOCA event tree. Additional information on the RCPSC fault tree modeling is provided in Section 5.1.35.
SSB-CSLOCA	This top event represents the success or failure of operators to terminate SI and to align a CCP to the normal charging path (including the establishment of letdown). Since the head of the CCPs is higher than the set-points of the pressurizer PORVs and SRVs, the CCPs will pressurize the RCS. If the CCPs are not stopped and a single CCP is not aligned for normal charging (including the establishment of letdown), the pressurizer PORVs or SRVs (if the PORVS fail to open) will remain open.[55] After the operators terminate SI,

[53] The MSIVs will receive an automatic closure signal during a SSB from high containment pressure or low steam line pressure. MFIVs will receive an automatic closure signal from the SI actuation. As a modeling simplification, the steam generator isolation fault trees for the SSBs (including consequential) do not include the manual operator action to close the MSIVs and MFIVs given the failure of the automatic closure signal. This conservative assumption has a negligible impact on the overall CDF.

[54] The SI actuation causes the trip of the NCP; therefore, normal seal injection is lost.

[55] The pressurizer PORVs or the SRVs are assumed to be open by the time operators get to the procedure steps to terminate SI.

align a single CCP for normal charging, and establish letdown (as represented by OAT----------H), if the PORVs or SRVs (if opened) do not reclose, a consequential LOCA occurs; and therefore, the sequence is transferred to the consequential SLOCA event tree. Additional information on the SSB-CSLOCA fault tree modeling is provided in Section 5.1.43.

AFW

This top event represents the success or failure of the AFW system to remove decay heat via the SGs. The MFW pumps will trip and the system will isolate on the SI actuation. This will require the use of 1 of 2 motor-driven AFW pumps or the turbine-driven AFW pump to provide flow to at least 2 intact SGs.[56] In addition, sufficient steam removal is required by either an ARV or 1 of 5 SRVs for at least 2 intact SGs. Success implies automatic actuation and operation of the AFW system to supply sufficient cooling water to the SGs. If the automatic AFW actuation signal fails, operator action (OA-START-AFW-H) is credited to manually start an AFW pump before a feed and bleed condition occurs. Additional information on the FW fault tree modeling is provided in Section 5.1.2.

FAB

This top event represents the success or failure of feed and bleed cooling. Feed and bleed cooling is required given secondary cooling (AFW and MFW) is unavailable. Success requires 1 of 2 CCPs to provide flow to the RCS cold legs and 1 of 2 PORVs to open and remove decay heat.[57] Operator action (OAB_TR-------H) is required to trip all the RCPs and initiate feed and bleed operation when the feed and bleed criteria are met. If feed and bleed cooling fails, core damage is assumed to occur. Additional information on the FAB fault tree modeling is provided in Section 5.1.8.

FABR

This top event represents the success or failure of long term feed and bleed operation using HPR. If feed and bleed is initiated due to failure of AFW and MFW, operators need to switch to HPR when the RWST level drops below the set-point of 29 percent. Success requires the CCPs to take suction from the discharge of the RHR pumps and deliver the water to the RCS. HPR will provide long-term cooling for the reactor given the HPI system was successful in supplying early makeup water to the reactor. The decay heat will be removed from the containment sump by the RHR heat exchangers (cooled via CCW) or by 4 of 8 CCUs. An operator action (OAR_LTFB-TRA-H if CCUs are available or OAR_LTFB-TRB-H if CCUs are not available) is required to align the RHR pump discharge to the HPI pump suction and verify that the containment sump valves are open and the RWST suction valves are closed. If feed and bleed recirculation fails, core damage is assumed to occur. Additional information on the FABR fault tree modeling is provided in Section 5.1.9.

---

[56] For a SSBI initiating event, the faulted steam generator is assumed to be unavailable for decay heat removal. For a SSBO initiating event, if the MSIVs for a SG fail to close, that SG is assumed to be unavailable for decay heat removal.

[57] The pump success criterion for feed and bleed recirculation is assumed to be the same as the pump success criterion for feed and bleed in the injection mode. This is potentially conservative because no credit is given for the SI pumps for feed and bleed in the injection mode, while it is possible that an SI pump may provide adequate flow in the recirculation mode.

SAFE/STABLE This top event represents the success or failure of cooldown and depressurization to allow the accumulators to provided makeup to the RCS. If the RCP seals are leaking at the assumed rate of 21 gpm per RCP due to lack of seal injection, core damage prior to 72 hours can occur if a source of inventory makeup to the RCS is not provided. Given the failure of the CCPs to provided RCP seal injection, operators will eventually be directed by CSFST procedures to depressurize the SGs to 200 psi using the ARVs for 2 of 4 SGs.[58] This depressurization will allow the accumulators (2 of 4 required) to inject into the RCS, thus providing makeup. An operator action (CAD-XHE-SAFESTABLE) is required. If AFW is to provide long-term decay heat removal for at least 72 hours, additional inventory must be provided.[59] This is typically accomplished by automatic makeup to CST 1 from the demineralizer water system. If automatic makeup is unavailable (e.g., loss of instrument air), operator action (OA-ALTAFW----H) is required to align CST 2 to provide additional inventory for continued AFW operation. If the cooldown/depressurization, accumulators, or CST makeup fail, core damage will occur prior to 72 hours. Additional information on the SAFE/STABLE fault tree modeling is provided in Section 5.1.41.

[58] For SSBIs, the success criterion is using the ARVs for 2 of 3 intact SGs.

[59] Additional CST inventory is needed earlier than 24 hours if the SSB is not terminated.

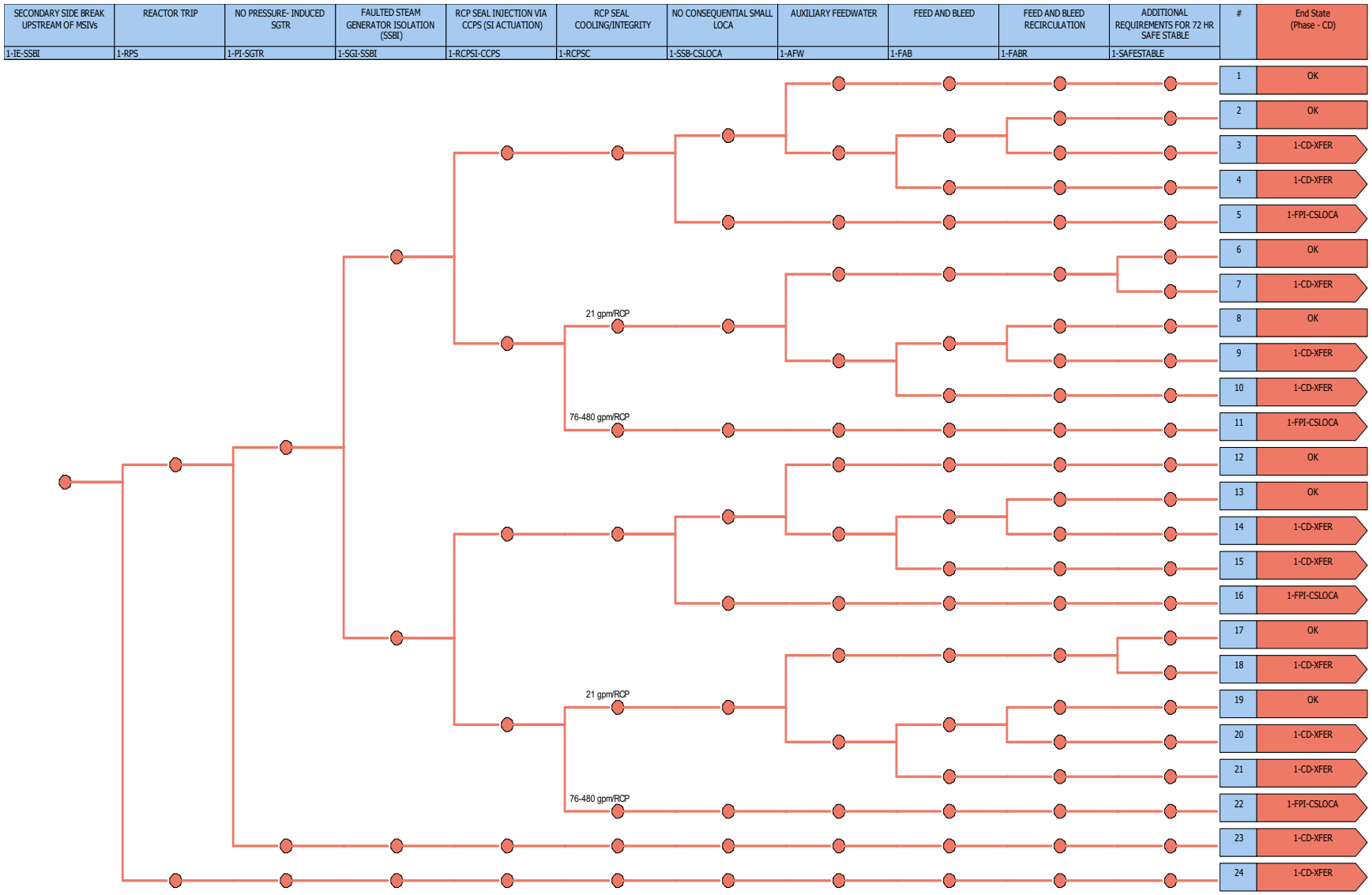


Figure 3-16 SSBI Event Tree

3.3 LOCA Event Trees

The following provides a description of the modeling of LOCA events trees.[60] These event trees include:

- Excessive LOCA (Reactor Vessel Rupture)
- LLOCA
- MLOCA
- SLOCA
- SGTR

3.3.1 Excessive LOCA (Reactor Vessel Rupture) Event Tree

Given an excessive LOCA (reactor vessel rupture), core uncovery is assumed to occur. There are no safety systems that can mitigate an excessive LOCA. An excessive LOCA (reactor vessel rupture) leads directly to core damage. Figure 3-17 shows the excessive LOCA (reactor vessel rupture) event tree.
The top events used in the excessive LOCA (reactor vessel rupture) event tree are provided below.

IE-XLOCA — Excessive LOCA (reactor vessel rupture) initiating event. The excessive LOCA (reactor vessel rupture) initiating event is defined as a catastrophic failure of the reactor vessel.

RPVRM — This top event represents the success or failure of mitigation against the initiator. It is set to TRUE because there are no safety systems that can mitigate an excessive LOCA (reactor vessel rupture).[61]

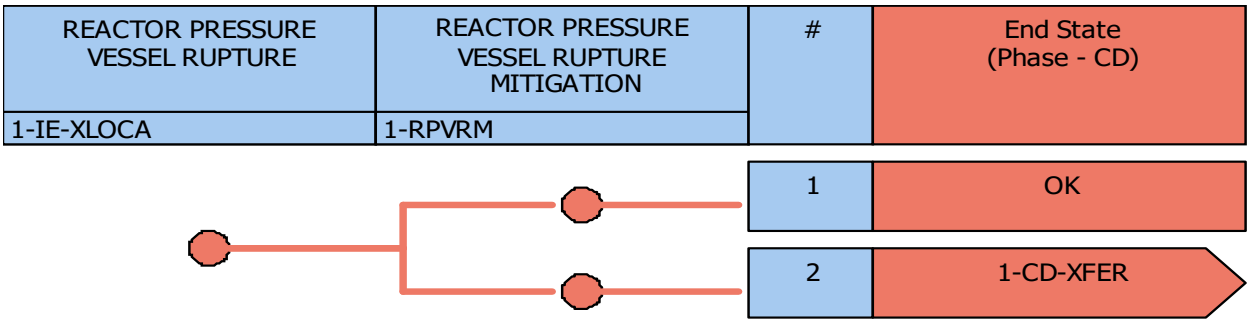


Figure 3-17 Excessive LOCA (Reactor Vessel Rupture) Event Tree

[60] ISLOCAs are described separately in Section 3.5.

[61] SAPHIRE requires an event tree structure to have at least one top event; however, there are no safety systems that can mitigate an excessive LOCA (reactor vessel rupture).

3.3.2 Large Loss-of-Coolant Accident Event Tree

The LLOCA initiating event is defined as a steam or liquid break that is large enough to rapidly depressurize the RCS pressure to a point below the low-pressure injection (LPI) and accumulator shutoff pressure. This break size is generally defined as having an effective break diameter of greater than 6 inches. Thus, the break size range for LLOCA events used in the L3PRA project Level 1 model is from a 6-inch equivalent diameter break up to the double-ended rupture of the largest pipe in the RCS.

Given a LLOCA, secondary cooling is not required since the break size is sufficient to remove the decay heat. In addition, high-pressure injection (via the SI pumps and/or CCPs) alone cannot provide sufficient flow to prevent core damage during a LLOCA. Therefore, the LLOCA event tree structure is used to represent the interactions among only three functional event groupings.

The first event grouping addresses reactor shutdown as represented by the RPS top event. A reactor trip is not expected to be required because the break will cause voiding in the reactor core that will interrupt the nuclear chain reaction. In addition, the successful injection of borated water from the accumulators and LPI will keep the reactor subcritical. However, it has conservatively been assumed that failure of RPS to trip the reactor during a LLOCA will result in core damage. This assumption has a negligible impact on the overall CDF.

The second grouping in the LLOCA event tree involves inventory control as represented by the ACC-M&LLOCA and LPI top events. Success of the accumulators and LPI meet the need for short-term inventory control. The accumulators are required to inject water to keep the core covered until the pressure lowers to a point below the shutoff head of the RHR pumps. LPI is queried after the accumulators have injected their water into the core. LPI provides sufficient flow to keep the core covered until the RWST is depleted and sump recirculation is initiated. If either the accumulators or LPI fail to provide makeup water, then the core will become uncovered and fuel damage is assumed to occur.

The third event grouping queries late decay heat removal/long-term cooling as represented by the low-pressure recirculation (LPR) and hot leg recirculation (HLR) top events. Long-term core cooling and late decay heat removal require the use of low-pressure recirculation. The RHR pumps take suction from the containment sump and discharge the sump water through the RHR heat exchangers. The RHR heat exchangers remove the decay heat prior to the sump water being injected into the RCS cold legs. If both RHR heat exchangers are unavailable, then the CCUs can provide the heat sink for recirculation. For long-term cooling, it is assumed that the heat sink (RHR heat exchangers or CCUs) will remove not only the decay heat from the RCS, but also the decay heat rejected to the containment by the LLOCA. Long-term cooling using the LPR system requires a switch to hot leg recirculation prior to the completion of the 24-hour PRA mission time. Hot leg recirculation is modeled to account for this requirement. Figure 3-18 shows the LLOCA event tree.

The top events used in the LLOCA event tree and their associated success criteria are provided below.

IE-LLOCA — LLOCA initiating event. The LLOCA initiating event is defined as a steam or liquid break that will rapidly depressurize the RCS pressure to the LPI and accumulator shutoff head. The break size ranges from a 6-inch equivalent diameter break up to the double-ended rupture of the largest pipe in the RCS.

RPS — This top event represents the success or failure of the RPS to insert enough negative reactivity by the control rods to shut down the reactor. Failure of the reactor to trip after a LLOCA initiating event is conservatively assumed to result in core damage (even though the break is expected to result in voiding in the reactor core sufficient to shut down the reactor). This assumption has negligible impact on CDF. Additional information on the RPS fault tree modeling is provided in Section 5.1.37.

ACC-M&LLOCA — This top event represents the success or failure of the accumulators to inject borated water into the RCS. Success implies that 3 of 3 accumulators inject their entire volume of water into the intact RCS cold legs. It is assumed that the RCS loop with the large break cannot be used for either ECCS injection/recirculation or accumulator injection. Additional information on the ACC-M&LLOCA fault tree modeling is provided in Section 5.1.1.

LPI — This top event represents the success or failure of the LPI system to provide makeup water to the RCS. Success implies automatic actuation and operation of 1 of 2 LPI trains once RCS pressure has lowered to below the RHR pump shutoff head. The pumps take suction from the RWST and must provide flow to 2 of 3 intact RCS cold legs. LPI provides sufficient water to keep the core covered. Additional information on the LPI fault tree modeling is provided in Section 5.1.27.

LPR — This top event represents the success or failure of LPR. Success implies 1 of 2 RHR pumps to provide sump recirculation to 1 of 3 intact RCS cold legs. The pumps take suction from the containment sump and pass the water through the RHR heat exchangers to slowly cool down the reactor. The decay heat will be removed from the containment sump by 1 of 2 RHR heat exchangers or by 4 of 8 CCUs. Operator action (OAR_LPLL-----H) is required to establish LPR. Additional information on the LPR fault tree modeling is provided in Section 5.1.28.

HLR — This top event represents the success or failure of hot-leg recirculation. Success implies 1 of 2 RHR pumps to provide recirculation to RCS hot leg 1 or 4.[62] Hot leg recirculation prevents flow path blockage within the reactor vessel due to boron precipitation. Operator action is required to establish low pressure hot leg recirculation (OAL_LPLL-----H).[63] Additional information on the HLR fault tree modeling is provided in Section 5.1.11.

---

[62] If the LLOCA occurred on either RCS loop 1 or 4, then hot leg recirculation is only possible using the intact hot leg.

[63] The NRC staff evaluated whether a switch to hot-leg injection is required to prevent core damage. The evaluation showed that modeling the need for hot leg recirculation during a LLOCA varies among PWR PRAs. In those instances where hot leg recirculation was excluded from PRA models, the NRC staff could not determine a clear technical basis for the exclusion. The exclusion of hot leg recirculation is based on expert judgment. Some industry tests suggest that core cooling may be available for some time after the onset of boric acid precipitation. However, the staff consensus view on core cooling performance with boron precipitation after a LLOCA is not presently available. Therefore, the L3PRA Project Level 1 model requires successful hot leg recirculation to mitigate a LLOCA. This potentially conservative assumption has a negligible impact on CDF.

3.3.3 Medium Loss-of-Coolant Accident Event Tree

The MLOCA initiating event is defined as a steam or liquid break that is large enough to remove decay heat without using the SGs, but small enough that RCS pressure is above the injection pressure of the accumulators and RHR pump shutoff pressure. This break size is generally defined as having an effective break diameter of between 2 to 6 inches.

The MLOCA event tree structure is used to represent the interactions among four functional event groupings. The first event grouping addresses reactor shutdown as represented by the RPS top event. As in the LLOCA event tree, it is conservatively assumed that failure of RPS to trip the reactor during a MLOCA will result in core damage. This assumption has a negligible impact on the overall CDF.

The second event grouping involves short-term inventory control as represented by the HPI top event. Given a MLOCA, secondary cooling is not initially required since the break size is of sufficient size to remove decay heat. High-pressure injection (via the CCPs and/or SI pumps) is initially actuated to provide RCS makeup.

The third event grouping queries alternate short-term decay heat removal and inventory control as represented by the AFW-LOCA, CAD-MLOCA, ACC-M&LLOCA, and LPI top events. If HPI fails, AFW flow to SGs can provide initial decay heat removal. In addition, operators will need to cooldown and depressurize the RCS by depressurizing the SGs using the ARVs.[64] Cooldown and depressurization of the RCS allows the accumulators to inject to the RCS, and along with LPI, provides inventory control and decay heat removal.

The fourth event grouping queries long-term core cooling as represented by the HPR and LPR top events. If HPI or LPI is successful, recirculation will be initiated when the RWST level reaches the low-level setpoint. In HPR, the HPI pumps (CCPs or SI pumps) take suction from the discharge of the RHR heat exchangers and provide flow to the intact RCS cold legs. The RHR pumps take suction from the containment sump and deliver the water through the RHR heat exchangers to cool it down prior to discharging it to the HPI pumps. For LPR, the RHR pumps take the suction from the containment sump and deliver water through the RHR heat exchangers to the intact RCS cold legs. If both RHR heat exchangers are unavailable, then the CCUs can provide the heat sink for recirculation. It is assumed that the heat sink (RHR heat exchangers or CCUs) will remove not only the decay heat from the RCS, but also the decay heat rejected to the containment by the MLOCA. The plant can be placed in a stable condition using HPR or LPR.[65] Figure 3-19 shows the MLOCA event tree.

The top events used in the MLOCA event tree and their associated success criteria are provided below.

IE-MLOCA — MLOCA initiating event. The MLOCA initiating event is defined as a steam or liquid break that is large enough to remove decay heat without using the SGs, but small enough that RCS pressure is above the injection pressure of the

[64] The TBVs will be unavailable for some break sizes (depending on the availability of the CCUs) in the MLOCA break range due to main steam isolation on high containment pressure.

[65] For the L3PRA Project Level 1 model hot leg recirculation is not needed based on Westinghouse and reference plant specific calculations and not modeled for MLOCAs.

accumulators and RHR pump shutoff pressure. The break size is in the range of 2 to 6 inches (equivalent diameter break).

RPS — This top event represents the success or failure of the RPS to insert enough negative reactivity by the control rods to shut down the reactor. Failure of the reactor to trip after a MLOCA initiating event is conservatively assumed to result in core damage. This assumption has negligible impact on CDF. Additional information on the RPS fault tree modeling is provided in Section 5.1.37.

HPI — This top event represents the success or failure of the HPI system to provide makeup water to the RCS. Success implies automatic actuation and operation of 2 of 4 CCPs/SI pumps to take suction from the RWST and provide flow to 2 of 3 intact RCS cold legs. It is assumed that the RCS loop with the medium break cannot be used for either ECCS injection/recirculation or accumulator injection. Additional information on the HPI fault tree modeling is provided in Section 5.1.12

AFW-LOCA[66] — This top event represents the success or failure of the AFW system to remove decay heat via the SGs. The MFW pumps will trip and the system will isolate on the SI actuation. This will require the use of 1 of 2 motor-driven AFW pumps or the turbine-driven AFW pump to provide flow to 2 of 4 SGs. In addition, sufficient steam removal is required by either an ARV or 1 of 5 SRVs for 2 of 4 SGs. Success implies automatic actuation and operation of the AFW system to supply sufficient cooling water to the SGs. If the automatic AFW actuation signal fails, operator action (OA-START-AFW-H) is credited to manually start an AFW pump before a feed and bleed condition occurs. Additional information on the AFW-LOCA fault tree modeling is provided in Section 5.1.2.

CAD-MLOCA — This top event represents the success or failure of the depressurization of the SGs to decrease RCS pressure to allow for the accumulators and LPI to supply RCS inventory makeup. If HPI fails, operators will be directed by FR-C.1/C.2 to depressurize the SGs to 200 psi, with the minimal success criteria of the ARVs for 2 of 4 SGs being used. This depressurization will allow the accumulators to inject into the RCS, thus providing makeup until RCS pressure decreases below the head of the RHR pumps. Operator action (OAD_MLA------H) is required to initiate the SG depressurization of the SGs by opening the ARVs. Additional information on the CAD-MLOCA fault tree modeling is provided in Section 5.1.4.

ACC-M&LLOCA — This top event represents the success or failure of the accumulators to inject borated water into the RCS. Success implies that 3 of 3 accumulators inject their entire volume of water into the intact RCS cold legs. Additional information on the ACC-M_LLOCA fault tree modeling is provided in Section 5.1.1.

---

[66] The AFW and AFW-LOCA fault trees are identical. There were differences between these fault trees in previous model versions; however, these differences have been removed.

LPI — This top event represents the success or failure of the LPI system to provide makeup water to the RCS. Success implies automatic actuation and operation of 1 of 2 LPI trains once RCS pressure has been lowered to below the RHR pump shutoff head. The pumps take suction from the RWST and must provide flow to 2 of 3 intact RCS cold legs. LPI provides sufficient water to keep the core covered. Additional information on the LPI fault tree modeling is provided in Section 5.1.27.

HPR — This top event represents the success or failure of HPR. Success requires the 1 of 4 HPI pumps (CCPs or SI pumps) to take suction from the discharge of 1 of 2 RHR pumps and deliver the water to the RCS. HPR will provide long-term cooling for the reactor given the HPI system was successful in supplying early makeup water to the reactor. The decay heat will be removed from the containment sump by 1 of 2 RHR heat exchangers or 4 of 8 CCUs. An operator action (OAR_HPML-----H) is required to establish HPR by aligning the RHR pump discharge to the HPI pump suction and verifying that the containment sump valves are open and the RWST suction valves are closed. Additional information on the HPR fault tree modeling is provided in Section 5.1.13.

LPR — This top event represents the success or failure of LPR. Success implies 1 of 2 RHR pumps to provide sump recirculation to 1 of 3 intact RCS cold legs. The pumps take suction from the containment sump and pass the water through the RHR heat exchangers to slowly cool down the reactor. The decay heat will be removed from the containment sump by 1 of 2 RHR heat exchangers or by 4 of 8 CCUs. Operator action (OAR_LPML-----H) is required to establish LPR. Additional information on the LPR fault tree modeling is provided in Section 5.1.28.

3.3.4 Small Loss-of-Coolant Accident Event Tree

The SLOCA initiating event is defined as a steam or liquid break in the RCS that exceeds normal charging flow, other than a SG tube rupture. In this break size range, defined as having an effective break diameter of between 3/8 inch and 2 inches, normal charging cannot maintain pressurizer level. A SLOCA will depressurize the RCS and cause a reactor trip. A SI signal will also be generated to start the HPI pumps (CCPs and SI pumps). Secondary cooling is required to remove decay heat. If secondary cooling fails, then feed and bleed cooling is required to remove decay heat.

The SLOCA event tree structure is used to represent the interactions among four functional event groupings. The first grouping (as represented by the RPS top event) queries whether the reactor successfully tripped either automatically or manually by operators. If the reactor trip fails, the sequence is transferred to the ATWS event tree (see Section 3.4.1 for additional information).

The second grouping (as represented by the AFW-LOCA, HPI, and FAB-SLOCA top events) addresses early decay heat removal and inventory control. For early decay heat removal, secondary-side cooling is provided via AFW. Given successful AFW, high-pressure injection (via the CCPs and/or SI pumps) meets the need for short-term inventory control. If AFW is unavailable, feed and bleed cooling is used both to remove decay heat and to provide short-term inventory control. Failure of both AFW and feed and bleed cooling results in core damage.

The third grouping (as represented by CAD-ES12, ACC, and LPI top event) deals with system cooldown and depressurization, as well as alternate means of early decay heat removal and inventory control when HPI fails. During a SLOCA, the operators are procedurally directed to cooldown and depressurize the RCS. If HPI is successful, ES-1.2 will direct operators to cooldown and depressurize the RCS by dumping steam from the SGs using the ARVs.[67] If HPI has failed, FR-C.1/C.2 will direct operators to cooldown and depressurize the RCS in a similar manner; however, operators will have less time to initiate the cooldown in this case. Given successful cooldown and depressurization, the accumulators will inject, supplying additional RCS inventory makeup. In addition, the RCS cooldown and depressurization allows the RHR pump(s) to supply low-pressure injection to the RCS (if HPI has failed). Given a failure of HPI, any failure of the cooldown with depressurization, accumulator injection, or LPI will result in core damage.

The final event grouping (as represented by the RHR-ES12, HPR, and LPR top events) queries late decay heat removal and long-term cooling. Long-term core cooling or late decay heat removal requires the use of either RHR or recirculation (HPR or LPR). Given at least three CCUs are running, the RCS is depressurized, and temperature has been reduced to the point where the RCS hot leg suction valves can be opened, RHR is used for long-term core cooling as the optimal recovery path after a SLOCA. The core heat is removed via the RHR heat exchangers. If the RCS cannot be depressurized, then HPR is required to stabilize the reactor. For HPR success, the HPI pumps take suction from the discharge of the RHR heat exchangers and provide flow to the RCS cold legs. The RHR pumps take suction from the containment sump and deliver the water through the RHR heat exchangers to cool it down prior to discharging it to the HPI pumps. CCUs are also credited in this mode to provide the heat sink for the recirculation water. It is assumed that the heat sink (RHR heat exchangers or CCUs) will remove not only the decay heat from the RCS, but also the decay heat rejected to the containment by the SLOCA. If the shutdown cooling mode of RHR fails or the RCS has been depressurized to allow for LPI, then LPR is used for long-term cooling. Figure 3-20 shows the SLOCA event tree.

The top events used in the SLOCA event tree and their associated success criteria are provided below.

IE-SLOCA — SLOCA initiating event. The SLOCA initiating event is defined as a steam or liquid break that exceeds normal charging makeup, other than a SGTR. The break size is in the range of 3/8-inch to 2-inch equivalent diameter.

RPS — This top event represents the success or failure of RPS to insert enough negative reactivity by the control rods to shut down the reactor. If automatic reactor trip fails, operator action is necessary to manually trip the reactor (OA------MANRTH or RPS-XHE-XE-NSGNL, depending on whether a reactor trip signal is present). Sequences involving failure of the reactor to trip are transferred to the ATWS event tree. Additional information on the RPS fault tree modeling is provided in Section 5.1.37.

AFW-LOCA — This top event represents the success or failure of the AFW system to remove decay heat via the SGs. The MFW pumps will trip and the system

[67] The TBVs will be unavailable for some break sizes (depending on the availability of the CCUs) in the SLOCA break range due to main steam isolation on high containment pressure.

will isolate on the SI actuation. This will require the use of 1 of 2 motor-driven AFW pumps or the turbine-driven AFW pump to provide flow to 2 of 4 SGs. In addition, sufficient steam removal is required by either an ARV or 1 of 5 SRVs for 2 of 4 SGs. Success implies automatic actuation and operation of the AFW system to supply sufficient cooling water to the SGs. If the automatic AFW actuation signal fails, operator action (OA-START-AFW-H) is credited to manually start an AFW pump before a feed and bleed condition occurs. Additional information on the AFW fault tree modeling is provided in Section 5.1.2.

HPI — This top event represents the success or failure of the HPI system to provide makeup water to the RCS. Success implies automatic actuation and operation of 1 of 4 CCPs/SI pumps to take suction from the RWST and provide flow to 2 of 4 RCS cold legs.[68] It is assumed that the RCS loop with the small break cannot be used for either ECCS injection/recirculation or accumulator injection. Additional information on the HPI fault tree modeling is provided in Section 5.1.12.

FAB-SLOCA — This top event represents the success or failure of feed and bleed cooling. Feed and bleed cooling is required given secondary cooling is unavailable. Success requires 1 of 2 PORVs if a CCP is providing HPI. If a SI pump is providing HPI, then 2 of 2 PORVs are required. Success also requires the HPI system to provide flow from 1 of 4 CCPs/SI pumps to 2 of 4 RCS cold legs. Operator action (OAB_SI-------H) is required to trip all the RCPs and initiate feed and bleed operation when the feed and bleed criteria are met. Additional information on the FAB-SLOCA fault tree modeling is provided in Section 5.1.8.

CAD-ES12 — This top event represents the success or failure of depressurizing the SGs to decrease RCS pressure to allow for the shutdown cooling mode of RHR to be initiated or for the accumulators and LPI to supply RCS inventory makeup. If HPI is successful, ES-1.2 will direct operators to cooldown and depressurize the RCS by dumping steam from the SGs to 200 psi (OAC_NC-------H), with a minimal success criterion of ARVs for 2 of 4 SGs. If HPI has failed, FR-C.1/C.2 will direct operators in a similar manner (OAC_AC-------H); however, operators will have less time to initiate the cooldown in this case. Additional information on the CAD-ES12 and CAD-FRC1 fault tree modeling is provided in Section 5.1.4.

ACC — This top event represents the success or failure of the accumulators to inject borated water into the RCS. Success implies that 2 of 3 accumulators associated with intact RCS cold legs inject their entire volume of water. Additional information on the ACC fault tree modeling is provided in Section 5.1.1.

LPI — This top event represents the success or failure of the LPI system to provide makeup water to the RCS. Success implies automatic actuation and operation of 1 of 2 LPI trains once RCS pressure has been lowered to below

[68] For a SLOCA, HPI and HPR assume that the associated broken LOOP is available for these functions.

the RHR pump shutoff head. The pumps take suction from the RWST and must provide flow to 2 of 4 RCS cold legs. LPI provides sufficient water to keep the core covered. Additional information on the LPI fault tree modeling is provided in Section 5.1.27.

RHR — This top event represents the success or failure of shutdown cooling with the RHR system. Success implies that after depressurization, the RCS pressure and temperature are within the requirements to allow the suction valves for 1 of 2 RHR pumps in the RCS hot leg to be opened to align for shutdown cooling. One of 2 RHR heat exchangers (cooled by CCW) will slowly cool down the reactor. This is the optimal recovery path after a SLOCA. The success of RHR depends on whether the RHR system can be put in operation before the RWST is depleted.[69] Using the shutdown cooling mode of RHR requires an operator action (OAN_SL-------H) to open the RCS hot leg valves to provide the suction source for the pumps and align the pump discharge through the RHR heat exchangers. Additional information on the RHR fault tree modeling is provided in Section 5.1.39.

HPR or FABR-SLOCA — This top event represents the success or failure of HPR or long-term feed and bleed operation. Success requires 1 of 4 HPI pumps (CCPs or SI pumps) to take suction from the discharge of the RHR pumps and deliver the water to the RCS. HPR will provide long-term cooling for the reactor given the HPI system was successful in supplying early makeup water to the reactor. HPR is required if RHR cannot be established or feed and bleed is initiated due to failure of AFW. The decay heat will be removed from the containment sump by 1 of 2 RHR heat exchangers or 4 of 8 CCUs. An operator action (OAR_HPSLA----H if CCUs are available, OAR_HPSLB----H if CCUs are not available) is required to align the RHR pump discharge to the HPI pump suction and verify that the containment sump valves are open and the RWST suction valves are closed.[70] Additional information on the HPR and FABR-SLOCA fault trees modeling is provided in Section 5.1.13 and Section 5.1.9.

LPR — This top event represents the success or failure of LPR. Success implies 1 of 2 RHR pumps to provide sump recirculation to 1 of 4 RCS cold legs. The pumps take suction from the containment sump and pass the water through the RHR heat exchangers to slowly cool down the reactor. The decay heat will be removed from the containment sump by 1 of 2 RHR heat exchangers or by 4 of 8 CCUs. An operator action (OAR_LPSL-----H if CCUs are available, OAR_LPSL2----H if CCUs are not available) is required to establish

---

[69] At least 3 of 8 CCUs need to be successfully running to prevent high containment pressure actuation of the containment spray system. If six or more CCUs fail, the actuation of containment spray will cause the rapid depletion of RWST inventory, leaving insufficient time for operators to reach entry conditions for the shutdown cooling mode of RHR.

[70] In the FABR-SLOCA event tree, different HFEs (OAR_LTFB_SLA-H and OAR_LTFB_SLB-H) are used, which have similar HEPs to the HFEs used in the HPR fault tree, the only difference is the time it takes for RWST level to be depleted to less than 29 percent.

LPR. Additional information on the LPR fault tree modeling is provided in Section 5.1.28.

3.3.5 Steam Generator Tube Rupture Event Tree

The SGTR initiating event is defined as a double-ended break of a single tube (as representative of a spectrum of possible break sizes).[71] Although this SGTR size is within the SLOCA spectrum, a SGTR is treated separately because it will cause direct primary to secondary leakage and bypass containment (thus preventing sump recirculation). Initial plant response is like that for a SLOCA.

After a SGTR initiating event occurs (which includes reactor trip and SI actuation) operators will enter E-0 and will perform the subsequent steps (e.g., verifying operation of the AFW and the ECCS given the expected SI actuation) until they are transferred to the E-3 guideline (due to high secondary radiation level or uncontrollable increase in SG water level), which will direct the operators to do the following:

- Identify and isolate ruptured SG
- Perform steps to stop the primary to secondary leakage:
  - Cooldown to establish RCS sub-cooling margin
  - Depressurize RCS to restore inventory
  - Terminate SI
  - Align normal charging flow and establish letdown
- Prepare for cool down to cold shutdown

If all the above steps are successful, the plant will stabilize near hot shutdown conditions and all immediate safety concerns will have been addressed. The operators will then attempt to bring the plant to cold shutdown by initiating a secondary cooldown to allow alignment of the shutdown cooling mode of RHR (via either ES-3.1 or ES-3.3). The operators are transferred to ECA-3.1 (from E-3) for any of the following conditions:

- Ruptured SG cannot be isolated (MSIVs and bypass valves)
- Ruptured SG pressure is below the analysis limit (due to faulted SG or failed isolation)
- Ruptured SG is needed for RCS cool down
- Stuck-open PORV and its associated block valve fails (after RCS depressurization)
- SI termination criteria are not met

[71] Limiting the definition of the SGTR to a double-ended break of the single tube in the L3PRA Project Level 1 model is believed to be consistent with the state-of-practice. Evaluation of additional break sizes is beyond the scope of this project.

- SI re-initiation is required to maintain RCS sub-cooling

Most of the steps in ECA-3.1 provide a source of recovery for potential operator failures to perform actions in E-3; and therefore, are not modeled explicitly in the event tree, but are accounted for in the evaluation of the applicable HFEs. In addition, ECA-3.1 provides actions to cool down and depressurize the RCS to cold shutdown conditions while minimizing loss of RCS inventory and voiding in the RCS.

The SGTR event tree structure is used to represent the interactions among five functional event groupings. The first grouping (as represented by the RPS top event) queries whether the reactor successfully tripped either automatically or manually by operators. If the reactor trip fails, the sequence is transferred to the ATWS event tree (see Section 3.4.1 for additional information).

The second grouping (as represented by the AFW-LOCA, HPI, and FAB-SLOCA top events) addresses early decay heat removal and inventory control.[72] For early decay heat removal, secondary-side cooling is provided via AFW. Given successful AFW, high-pressure injection (via the CCPs and/or SI pumps) meets the need for short-term inventory control. If AFW is unavailable, feed and bleed cooling is used both to remove decay heat and to provide short-term inventory control. Failure of both AFW and feed and bleed cooling results in core damage.

The third grouping (as represented by SGI and CAD-SGTR-EARLY) models whether primary-to-secondary leakage through the ruptured SG is stopped (i.e., the LOCA is terminated). Unlike a SLOCA initiating event, the LOCA caused by a SGTR can be terminated if operators first isolate the ruptured SG by closing one of its MSIVs and the associated bypass valve.[73] If operators are unable to shut the ruptured SG's MSIVs (and bypass valves), then they are directed to shut the MSIVs to the intact SGs. In addition, AFW flow to the ruptured SG should be isolated.[74, 75] After the ruptured SG is isolated, operators must depressurize the RCS to a pressure less than that of the ruptured SG to prevent overfilling it, which would cause its ARVs/SRVs to open. Procedures also direct operators to use pressurizer sprays or PORVs to restore pressurizer level. In addition, operators must also terminate SI, align normal charging, and establish letdown to stop the primary-to-secondary leakage.

The fourth event grouping (as represented by the CAD-SGTR-LATE, RHR, and HPR top events) involves late decay heat removal and long-term cooling. Long-term core cooling or late decay heat removal requires either the use of the shutdown cooling mode of RHR or, if feed and bleed cooling has been initiated (given a failure of AFW), the use of high pressure recirculation (HPR) is required. The entry conditions for the shutdown cooling mode of RHR require operators to perform a manual cooldown and depressurization of the RCS by dumping steam using the TBVs or (intact) SG ARVs. When shutdown cooling is initiated, decay heat is removed via the RHR heat exchangers. If feed and bleed cooling is being used for decay heat

---

[72] The FAB-SLOCA top event was placed after the SGI top event based on a timing evaluation of OAI_SG-------H and OAB_SI-------H. The T_{sw} values for these HFEs indicate that the ruptured SG will be isolated prior to the entry conditions to initiate feed and bleed cooling.

[73] Operators are also directed to close the steam supply valve to the turbine-driven AFW pump if SG 1 or SG 2 is ruptured.

[74] Procedures also direct operators to close the SG blowdown valves. However, the failure of these valves to close would not appreciably affect SG isolation; therefore, the modeling of these valves is not included in the SGI fault tree.

[75] The MFW pumps will trip and the system will isolate due the SI actuation.

removal (given failure of AFW), HPR must be aligned when RWST level reaches the low-level setpoint.[76] During HPR, the CCPs or SI pumps take suction from the discharge of the RHR heat exchangers and provide flow to the RCS cold legs. The RHR pumps take suction from the containment sump and deliver the water through the RHR heat exchangers to cool it down prior to discharging it to the HPI pumps. CCUs are also credited in this mode to provide an alternative heat sink for the recirculation water.

The final event grouping (as represented by the CSTR and RFL top events) captures the requirements for a safe and stable end-state at 72 hours. If the AFW is the source of long-term decay removal (i.e., shutdown cooling mode of RHR cannot be established or HPR is not available) makeup to the CST is needed to prevent core damage for 72 hours. In addition, if primary-to-secondary leakage is not terminated; makeup to the RWST must be provided, since RCS inventory is being lost through the ruptured SG. Figure 3-21 shows the SGTR event tree.

The top events used in the SGTR event tree and their associated success criteria are provided below.

IE-SGTR	SGTR initiating event.
RPS	This top event represents the success or failure of RPS to insert enough negative reactivity by the control rods to shut down the reactor. If automatic reactor trip fails, operator action is necessary to manually trip the reactor (OA------MANRTH or RPS-XHE-XE-NSGNL, depending on whether a reactor trip signal is present). Sequences involving failure of the reactor to trip are transferred to the ATWS event tree. Additional information on the RPS fault tree modeling is provided in Section 5.1.37.
AFW-LOCA[77]	This top event represents the success or failure of the AFW system to remove decay heat via the SGs. The MFW pumps will trip and the system will isolate on the SI actuation. This will require the use of 1 of 2 motor-driven AFW pumps or the turbine-driven AFW pump to provide flow to 2 of 3 intact SGs. In addition, sufficient steam removal is required by either an ARV or 1 of 5 SRVs for 2 of 3 intact SGs. Success implies automatic actuation and operation of the AFW system to supply sufficient cooling water to the SGs. If the automatic AFW actuation signal fails, operator action (OA-START-AFW-H) is credited to manually start an AFW pump before a feed and bleed condition occurs. Additional information on the AFW-LOCA fault tree modeling is provided in Section 5.1.2.
HPI	This top event represents the success or failure of the HPI system to provide makeup water to the RCS. Success implies automatic actuation and operation of 1 of 4 CCPs/SI pumps to take suction from the RWST and

[76] Feed and bleed recirculation is queried when feed and bleed injection is successful. Regardless of whether the ruptured SG is isolated, most of RCS leakage will pass through the open PORV(s) rather than through the ruptured SG tube, thus permitting recirculation.

[77] The AFW-LOCA fault tree is used in the SGTR event tree because CST inventory makeup is included in a separate top event (CSTR). Unlike some of the other LOCA initiating events (e.g., MLOCA, SLOCA, consequential SLOCA), AFW can provide long-term decay heat removal during a SGTR.

provide flow to 2 of 4 RCS cold legs. Additional information on the HPI fault tree modeling is provided in Section 5.1.12.

SGI — This top event represents the success or failure of isolating the ruptured SG. Success requires an operator to diagnose the loss of coolant as a SGTR, identify the ruptured SG, and isolate it to prevent overfill. This top event models both the operator performing the isolation (OAI_SG-------H) and the required equipment (e.g., closure of the applicable MSIVs and bypass valves, and AFW SG injection valves). Additional information on the SGI fault tree modeling is provided in Section 5.1.42.

FAB-SLOCA — This top event represents the success or failure of feed and bleed cooling. Feed and bleed cooling is required given secondary cooling is unavailable. Success requires 1 of 2 PORVs if a CCP is providing HPI. If a SI pump is providing HPI, then 2 of 2 PORVs are required. Success also requires the HPI system to provide flow to 2 of 4 RCS cold legs. Operator action (OAB_SI-------H) is required to trip all the RCPs and initiate feed and bleed operation when the feed and bleed criteria are met. Additional information on the FAB-SLOCA fault tree modeling is provided in Section 5.1.8.

CAD-SGTR-EARLY — This top event represents the success or failure of cooldown and depressurization of the RCS to stop primary-to-secondary leakage. Operator action (OAD_SGR------H) is required to use the TBVs or the ARVs for 2 of 3 intact SGs to depressurize the RCS to a pressure less than that of the ruptured SG, to prevent overfilling.[78] The E-3 procedure also directs operators to use pressurizer sprays or PORVs to restore pressurizer level. In addition, operators must terminate SI, align normal charging, and establish letdown to stop the primary-to-secondary leakage.[79] Additional information on the CAD-SGTR-EARLY fault tree modeling is provided in Section 5.1.4.

CAD-SGTR-LATE — This top event represents the success or failure of depressurizing the SGs to decrease RCS pressure to allow for the shutdown cooling mode of RHR to be initiated. If the ruptured SG is isolated and primary-to-secondary leakage has been stopped, operators will transition from E-3 to ES-3.1 or ES-3.3, which will direct operators to cooldown and depressurize the RCS by dumping steam from using the TBVs or ARVs for 2 of 3 intact SGs (CAD-XHE-SGTR-LT).[80,81] Additional information on the CAD-SGTR-LATE fault tree modeling is provided in Section 5.1.4.

---

[78] There is the potential that the timing for this operator action may depend on the success or failure of HPI; however, given the lack of scenario-specific information, a conservative modeling simplification was used.

[79] As a modeling simplification, the CAD-SGTR-EARLY fault tree does not include the potential for the SG SRVs to reclose, given they are demanded prior to completion of the cooldown and depressurization.

[80] Operators are directed to maintain a cooldown rate in the RCS cold legs of less than 100°F per hour.

[81] Procedures also direct operators to use pressurizer sprays to backfill the ruptured SG; however, this is not believed to be needed for entry into the shutdown cooling mode of RHR. Therefore, the use of pressurizer sprays is not included in this fault tree.

RHR

This top event represents the success or failure of shutdown cooling with the RHR system. Success implies that after depressurization, the RCS pressure and temperature are within the requirements to allow the RCS hot leg suction valves for 1 of 2 RHR pumps to be opened to align for shutdown cooling. One of 2 RHR heat exchangers (cooled by CCW) will slowly cool down the reactor. This is the optimal recovery path after a SGTR. Using the shutdown cooling mode of RHR requires an operator action (OAN_SL-------H) to open the RCS hot leg valves to provide the suction source for the pumps and align the pump discharge through the RHR heat exchangers. Additional information on the RHR fault tree modeling is provided in Section 5.1.39.

FABR-SLOCA

This top event represents the success or failure of long term feed and bleed operation.[82] Success requires 1 of 4 HPI pumps (CCPs or SI pumps) to take suction from the discharge of the RHR pumps and deliver the water to the RCS. Feed and bleed recirculation will provide long-term cooling for the reactor given that feed and bleed cooling was successful in supplying early makeup water/decay heat removal to the reactor. The decay heat will be removed from the containment sump by 1 of 2 RHR heat exchangers or 4 of 8 CCUs. An operator action (OAR_LTFB_SLA-H if CCUs are available or OAR_LTFB_SLB-H if CCUs are not available) is required to align the RHR pump discharge to the HPI pump suction and verify that the containment sump valves are open and the RWST suction valves are closed. Additional information on the FABR-SLOCA fault tree modeling is provided in Section 5.1.9.

CSTR

This top event represents the success or failure of inventory makeup to AFW via the CST(s). If AFW is to provide long-term decay heat removal for at least 72 hours, additional inventory must be provided. This is typically accomplished by automatic makeup to CST 1 from the demineralizer water system. If automatic makeup is unavailable (e.g., loss of instrument air), operator action (OA-ALTAFW----H) is required to align CST 2 to provide additional inventory for continued AFW operation. Additional information on the CSTR fault tree modeling is provided in Section 5.1.6.

RFL

This top event represents the success or failure of refilling the RWST. If primary-to-secondary leakage is not terminated, the RCS inventory will continue to be lost out the open ARV/SRVs of the ruptured SG.[83] Thus, makeup to the RWST is needed to reach a 72-hour safe and stable end-state. Operator action (RFL-XHE-REFILL-LT) is required to refill the RWST.[84] Additional information on the RFL fault tree modeling is provided in Section 5.1.40.

---

[82] If SG isolation fails and operators successfully initiate feed and bleed cooling, based on reference plant MAAP calculations, there is expected to be sufficient inventory in the sump for the switchover to recirculation.

[83] While in E-3, RWST refill will be initiated via ES-1.3 (and subsequent procedure links) when the RWST level reaches the low level setpoint. If in ECA-3.1, operators will initiate RWST makeup earlier.

[84] The fault tree modeling for refilling the RWST only includes the HFE, and does not include hardware failures, because the information necessary to develop this additional logic was not readily available, and it is expected that the HFE will likely dominate the failure to accomplish this action.

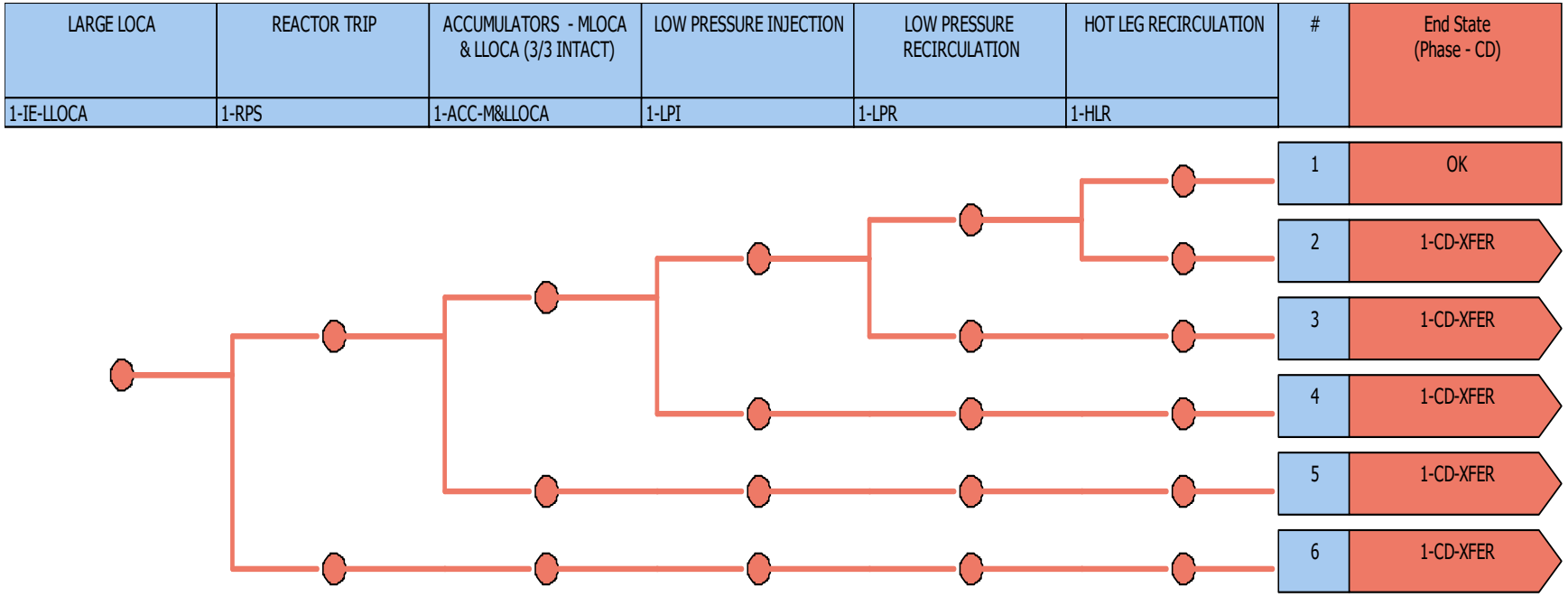


Figure 3-18 LLOCA Event Tree

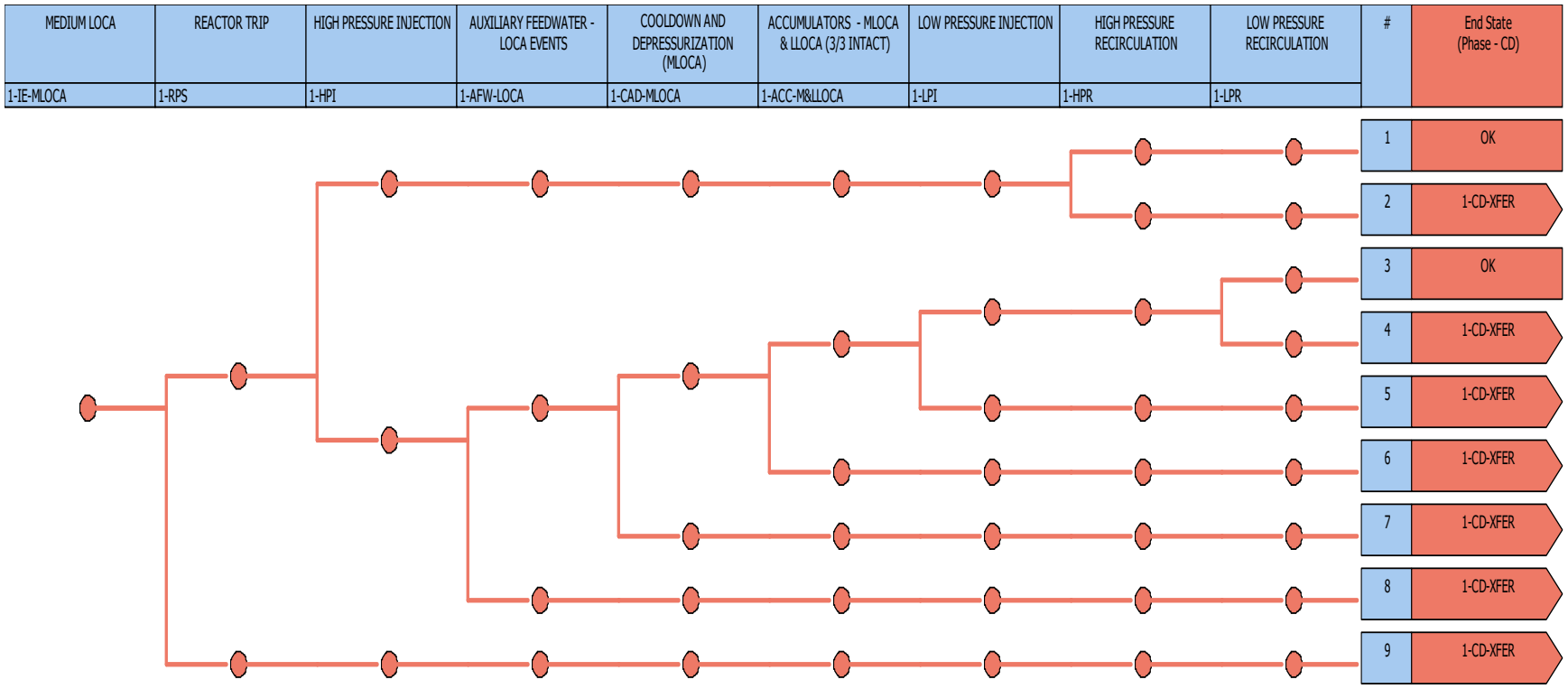


Figure 3-19 MLOCA Event Tree

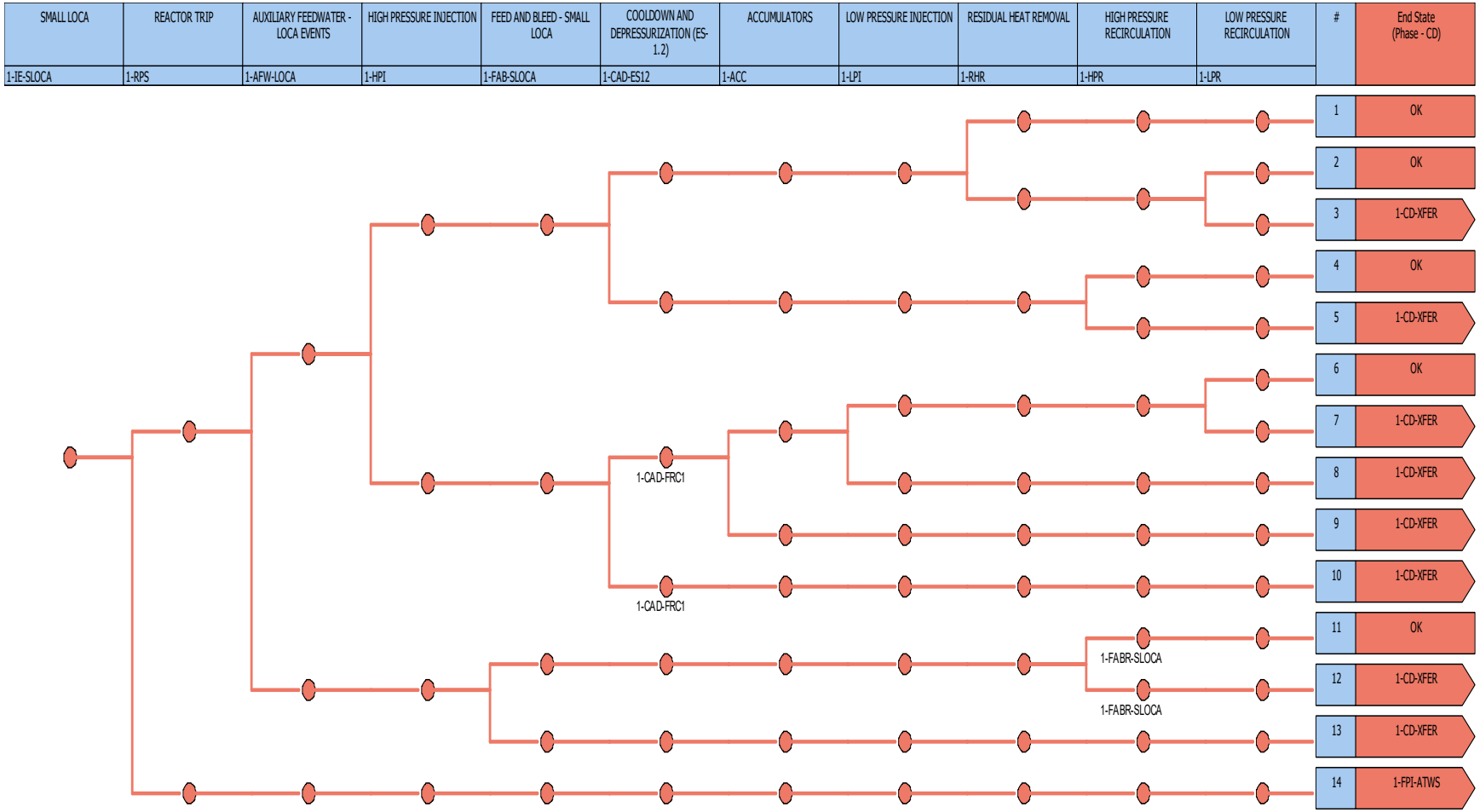


Figure 3-20 SLOCA Event Tree

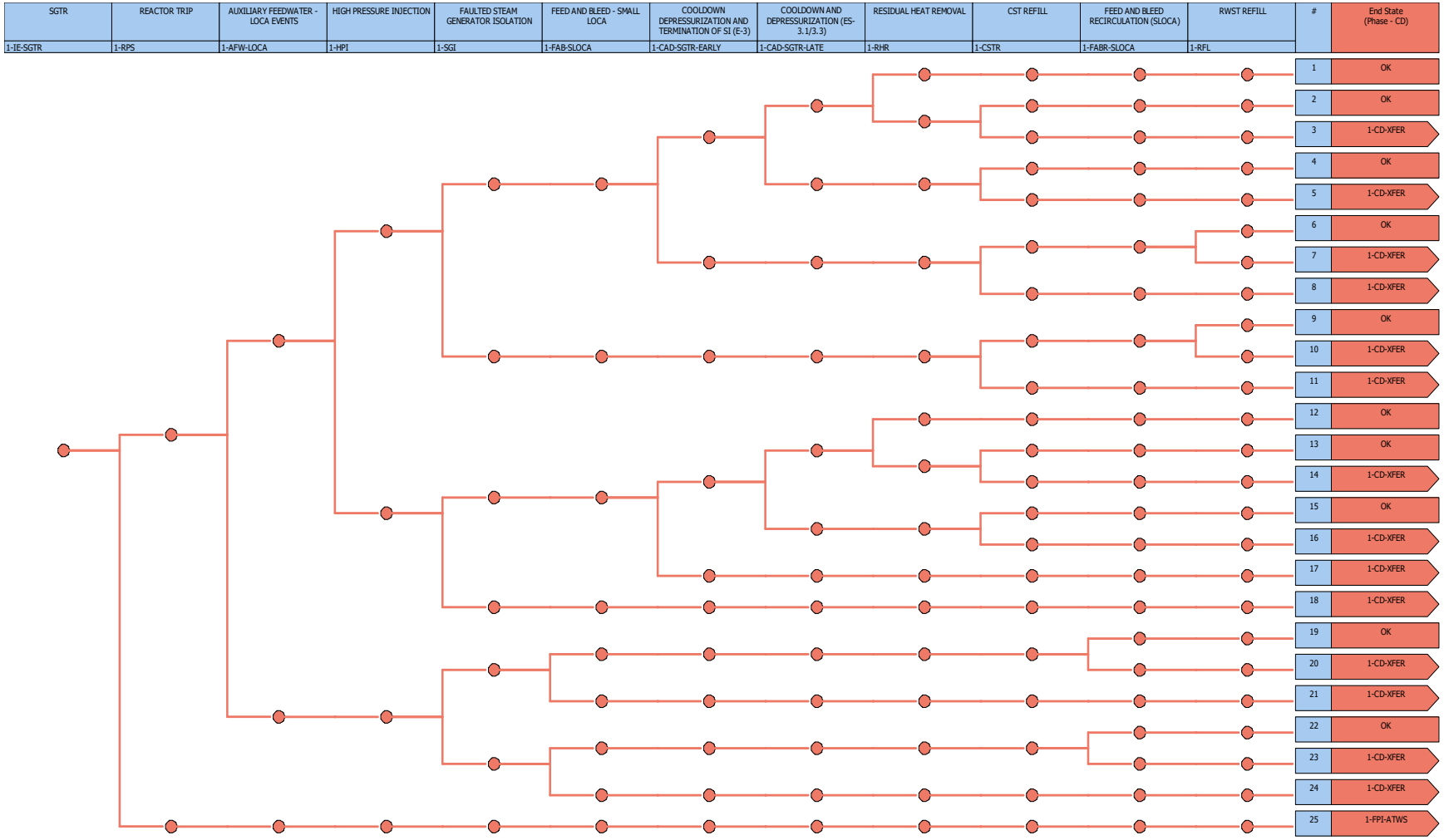


Figure 3-21 SGTR Event Tree

3.4 Transfer Event Trees for Transient Initiating Events

For the transient initiating events presented in Section 3.1, certain consequential events can occur that change the complexity of the transient progression. These consequential events include:

- ATWS – If the RPS fails, the transient sequence is transferred to the ATWS event tree.
- Consequential SSB – If the turbine fails to trip (i.e., the turbine stop or control valves fail to close) or the TBVs fail to reclose, the sequence is transferred to the CSSBO event tree. If the SG ARVs or SRVs are demanded and fail to reclose, the sequence is transferred to the CSSBI event tree.[85]
- Consequential SLOCA – If the PORVs or SRVs are demanded and fail to reclose, the RCP seals fail due to the loss of all seal injection and cooling, or operators fail to terminate SI (given an SI actuation), the sequence is transferred to the CSLOCA event tree.
- SBO – If a LOOP initiating event occurs and both EDGs fail or are unavailable, the sequence is transferred to the SBO event tree.

These consequential event trees are described in the following sections.

3.4.1 ATWS Event Tree

If the RPS fails to trip the reactor during the response to an initiating event, the sequences are transferred to the ATWS event tree. The structure of the ATWS event tree differs from other event trees due to the mitigation concerns in response to the large initial RCS pressure increase if MFW is lost. In addition, the higher RCS pressure and temperature require more stringent frontline system success criteria.

The loss of MFW is the limiting transient for ATWS. The MFW system will not be isolated by the P-4 interlock on a reactor trip, because during an ATWS the reactor fails to trip and the RCS temperature does not decrease sufficiently.[86] Therefore, only initiating events that result in unavailability of MFW (e.g., loss of MFW, loss of condenser, SLOCA, loss of a safety-related 4.16 kV AC bus, or loss of a safety-related 125 V DC bus) will experience an immediate MFW loss. If MFW is available during an ATWS, the RCS pressure increase will be limited, and only the ability to shut down the reactor by emergency boration is needed (given the pressurizer PORVs/SRVs reclose).[87]

If MFW is unavailable, RCS pressure relief is needed to prevent RCS pressure from increasing above 3200 psi, which leads to an RCS integrity breach beyond the capability of the ECCS to

---

[85] Core damage is assumed if both RPS fails to trip the reactor and secondary valves fail to close, due to the positive reactivity addition caused by increased cooling of the RCS.

[86] The P-4 interlock is activated when the reactor trip breakers (RTBs) are opened and low T_{avg} setpoint is reached. The P-4 interlock also provides the normal turbine trip signal.

[87] There are other procedure-based actions that can shut down the reactor, including: (1) manual control rod insertion, (2) local opening of reactor trip and bypass breakers, and (3) local opening of the control rod drive motor-generator breakers. None of these actions were considered in the L3PRA Level 1 model, since it was determined that there is insufficient time to perform these actions to mitigate the initial pressure transient.

mitigate and subsequent core damage.[88] The RCS integrity breach is assumed to include a consequential, pressure-induced SGTR, though this assumption does not affect the core damage frequency quantification. The success of primary pressure relief depends not only on the availability of the pressurizer PORVs and SRVs, but also the negative reactivity feedback. Unfavorable exposure time (UET) is defined as the time during the cycle when the reactivity feedback is not sufficient to prevent RCS pressure from exceeding 3200 psi. Many factors, such as initial power level, time in cycle when transient occurs, reactivity feedback as a function of the cycle life, the number of available relief valves, the failure or success of manually inserting the control rods, and AFW flow rates, affect UET.[89] Given the L3PRA project Level 1 model assumptions on initial power level (assumed to be 100 percent) and that no credit is given for insertion of the control rods, two cases exist in which the primary relief capacity is sufficient: (1) all PORVS and SRVs are available and successfully open or (2) one PORV is blocked during the transient, but the other PORV and all SRVs are available and successfully open. According to WCAP-15831, "WOG Risk-Informed ATWS Assessment and Licensing Implementation Process," Revision 2 (Westinghouse, 2007), the UETs for these cases are 0.11 and 0.32, respectively.[90]

Given the unavailability of MFW, maximum AFW flow (from both MDPs and the TDP) is needed to maintain inventory to SGs.[91] In addition, analyses show that a turbine trip is necessary (within 30 seconds) to maintain SG inventory.[92]

If the initial RCS pressure transient due to the ATWS is mitigated and no subsequent LOCA occurs, then negative reactivity must be added to shut down the reactor. If operators fail to trip the reactor prior to the pressure transient (assumed to be 90 seconds); operators will have additional time to trip the reactor if the pressure transient has been mitigated. If the reactor trip breakers have failed or the control rods are mechanically stuck, operators will enter the ATWS procedure (FR-S.1) and are directed to manually insert the control rods (if possible) and initiate emergency boration.[93, 94]

---

[88] Analyses performed in support of WCAP-8330, "Westinghouse Anticipated Transients without Trip Analysis," (Westinghouse, 1974) and WCAP-11992, "Joint Westinghouse Owners Group/Westinghouse Program: ATWS Rule Administration Process," (not publicly available) demonstrate that if reactor power is less than 70 percent at the time of the transient, RCS pressure will remain below 3200 psi following a loss of heat sink. The L3PRA project Level 1 model assumes that the plant is running at 100 percent power.

[89] The L3PRA Project Level 1 model does not credit manual insertion of control rods by the operators because it was determined that insufficient time was available. Therefore, the UET fractions used in the L3PRA Project Level 1 model assume the failure of manual insertion of control rods.

[90] These UETs were taken from Table 5-4 of WCAP 15831, and are weighted values (no rod insertion, 100 percent AFW flow) for a low reactivity core, equilibrium xenon, and reactor power greater than 40 percent.

[91] The L3PRA Project Level 1 model uses a simplifying assumption that failure of manual control rod insertion requires that all AFW pumps must provide flow to the SGs to prevent SG dry out and limit the RCS pressure increase; however, this may be conservative. According to WCAP-15831, core damage may be prevented with 50 percent AFW flow (i.e., both MDPs or the TDP) if manual insertion of the control rods fails.

[92] Unless the ATWS is due to the mechanical failure of the control rods to insert into the core, only the ATWS mitigation system actuation circuitry (AMSAC) will be available to trip the turbine, because the normal turbine trip signal is provided by the P-4 interlock when the RTBs open. Due to the time limitations for ATWS with MFW unavailable, no credit is given for operators to manually trip the turbine or close the MSIVs.

[93] As a modeling simplification and because they are successive steps in FR-S.1, the HFE to initiate emergency boration (OA-OBR-------H) is used to represent both manual rod insertion (if possible) and emergency boration.

[94] Operators can establish emergency boration using either the NCP or a CCP to inject borated water to the RCS through several different emergency boration pathways. However, the evaluation for OA-OBR-------H only includes the main procedural pathway via the normal charging line. Since the HEP dominates the failure of

If a LOCA initiating event (SLOCA or SGTR), a pressurizer PORV or SRV failure to close (as represented by the PVC-ATWS top event), or a RCP seal LOCA (due to the failure of RCP seal injection/cooling) has occurred, an SI actuation will occur and HPI can provide both RCS inventory makeup and negative reactivity to shut down the reactor.[95] If HPI is successful, HPR is needed for long-term cooling and to achieve a safe/stable end-state. Failure of either HPI or HPR is assumed to result in core damage.[96]

If the RCP seal injection is lost, but either seal cooling to the thermal barrier heat exchangers or RCP seal integrity is maintained, seal leakage is assumed to increase from a nominal leak rate to 21 gpm per RCP.[97] Therefore, operators must provide RCS inventory makeup by either aligning charging or depressurizing the plant (using the TBVs or SG ARVs to allow the accumulators to inject). Failure to align charging or initiate the cooldown and depressurization will result in core damage prior to 72 hours. Figure 3-22 shows the ATWS event tree.

The top events used in the ATWS event tree and their associated success criteria are provided below.

RPS — This top event signifies that a transient occurred, and the reactor protection system failed to trip the reactor.

MFW-ATWS — This top event represents the success or failure of the MFW system to remove decay heat via the SGs during an ATWS. If the transient initiating event does not render MFW unavailable (e.g., loss of MFW, loss of condenser heat sink, loss of instrument air, loss of safety-related AC/DC bus, or SLOCA), the system will not isolate because a reactor trip failed to occur and/or RCS temperature is expected to be above the P-4 (low T_{avg} setpoint) interlock. Success requires the use of both turbine-driven MFW pumps to provide flow to all four SGs.[98] In addition, sufficient steam removal is required by either: (1) three TBVs or (2) an ARV or 1 of 5 SRVs for 4 of 4 SGs. Additional information on the MFW-ATWS fault tree modeling is provided in Section 5.1.29.

PPR — This top event represents the success or failure of primary pressure relief after ATWS. If RCS pressure increases above 3200 psi, an RCS integrity breach (assumed here to also include a pressure-induced SGTR) beyond the capability of the ECCS to mitigate may occur and core damage is assumed to follow. The success of primary pressure relief depends not only on the pressurizer PORVs and SRVs but also the negative reactivity feedback. If the reactor cycle is in UET, pressure relief fails regardless of relief valve

---

emergency boration fault tree results, the L3PRA Project Level 1 model does not include the alternate pathways for emergency boration in the EBR fault tree, as a simplification.

[95] The RWST boron concentration is considered sufficient to shut down the reactor.

[96] The inclusion of only the HPI and HPR top events (given a SLOCA) is an ATWS modeling simplification due to the uncertainty of post-LOCA cooldown and depressurization given an ATWS has occurred. ATWS results indicate that this modeling approach has a negligible impact on the overall CDF.

[97] This assumption is conservative for scenarios with successful RCP seal cooling (via ACCW through the thermal barrier heat exchangers).

[98] The success criteria requiring both MFW pumps and 4 of 4 SGs is conservative; however, thermal hydraulic calculations to support reducing the criteria are not currently available. ATWS results indicate that this modeling assumption has a negligible impact on the overall CDF.

operation. In the L3PRA project Level 1 model, two different cases were analyzed to estimate the percentage values of UETs based on maximum AFW flow (both MDPs and the TDP): (1) all pressurizer PORVs and SRVs successfully open and (2) one PORV is blocked, but the other PORV and all SRVs successfully open. From WCAP-15831, the weighted UETs for these cases are 0.11 and 0.32, respectively. Additional information on the PPR fault tree modeling is provided in Section 5.1.33.

AFW-ATWS — This top event represents the success or failure of all three AFW pumps (both MDPs and the TDP) to provide makeup to the SGs after an ATWS. Success implies automatic actuation and operation of all three AFW pumps to supply sufficient cooling water to all four SGs.[99] The AMSAC system is credited to automatically start all AFW pumps given a loss of MFW with reactor power greater than 40 percent.[100] Additional information on the AFW-ATWS fault tree modeling is provided in Section 5.1.2.

TT-ATWS — This top event represents the success or failure of the turbine to trip after an ATWS. Success implies that the turbine automatically trips; and therefore, adequate SG inventory is available given a loss of MFW. The AMSAC system is credited to automatically trip the turbine given a loss of MFW with reactor power greater than 40 percent.[101] Additional information on the TT-ATWS fault tree modeling is provided in Section 5.1.46.

PVC-ATWS — This top event questions the primary system boundary integrity. Primary system breach occurs if the ATWS event was originated from a LOCA or SGTR, or if the pressurizer valves (PORVs/SRVs) fail to reclose after opening during the initial RCS pressure transient.[102] It is assumed that all pressurizer PORVs and SRVs open and must reclose to prevent a consequential LOCA.[103]

---

[99] Unlike the other initiating events that could render a SG unavailable (e.g., SLOCA, SGTR), if an ATWS occurs after one of these initiating events, it is assumed that a SG will not be rendered unavailable during the initial pressure transient of an ATWS and prior to reaching a quasi-equilibrium state based on engineering judgement. For a SLOCA initiating event, the loop in which the LOCA occurred will not render the SG unavailable for some time (i.e., after the applicable RCP is tripped), which will be when AFW success criteria on the number of required SGs will be less stringent. For a SGTR initiating event, the ruptured SG will not be isolated until after operators exit the ATWS procedures; and therefore, it would be available for the duration of the ATWS response.

[100] In addition, the low SG water level ESFAS signal and LOOP/SI sequencers can provide an automatic start signal for the AFW pumps. However, these signals are assumed to be failed if RPS failures are what caused the failure of the reactor trip. Therefore, these signals are only credited if reactor trip fails due to the mechanical failure of the control rods to insert into the core or due to the mechanical failure of the reactor trip breakers to open. Manual start of the AFW pumps is not credited due to insufficient time available for operators given an ATWS with MFW unavailable.

[101] If reactor trip fails due to the mechanical failure of the control rods to insert into the core, then the normal turbine trip signal will be available because the RTBs will open. Due to trip signal failures dominating the results (as shown by the TT fault tree), for simplification, the failure of the stop and control valves have not been included in the TT-ATWS fault tree.

[102] The ATWS event tree uses a simplified LOCA response modeling approach that only queries HPI and HPR, which does not properly account for SGTR scenarios in which no water will be available to bring the plant to safe/stable end state via HPR.

[103] This is potentially conservative if MFW is available; however, thermal hydraulic calculations to show how limited the pressure transient with MFW would be are not currently available.

RCPSI — This top event represents the success or failure of normal RCP seal injection via the NCP.[104] As discussed previously, alignment of the CCPs for alternate seal injection is only credited for the loss of ACCW and loss of RCP seal injection initiating events. If RCP seal injection fails, seal leakage is assumed to increase to at least 21 gpm per RCP (higher leakage rates may occur depending on the success or failure of RCP thermal barrier cooling—see RCPSC below). Additional information on the RCPSI fault tree modeling is provided in Section 5.1.36.

RCPSC — This top event represents the success or failure of RCP seal cooling from the thermal barrier heat exchangers (cooled via ACCW). If RCP seal cooling fails, the integrity of the seals is challenged. Per the WOG 2000 RCP seal model, given the loss of all RCP seal cooling and injection, RCP seals have an approximately 21 percent chance of failure. In addition, operator failure to trip the RCPs (RCS-XHE-XM-TRIP) will also result in failure of RCP seals. A failure of RCP seals is assumed to result in a consequential SLOCA; and therefore, the sequence is transferred to the consequential SLOCA event tree. Additional information on the RCPSC fault tree modeling is provided in Section 5.1.35.

HPI — This top event represents the success or failure of the HPI system to provide makeup water (and negative reactivity) to the RCS. Success implies automatic actuation and operation of 1 of 4 CCPs/SI pumps to take suction from the RWST and provide flow to 2 of 4 RCS cold legs. Additional information on the HPI fault tree modeling is provided in Section 5.1.12.

RXSD — This top event represents the success or failure to insert negative reactivity to shut down the reactor, bringing it to a safe and stable end-state. If the initial RCS pressure transient due to the ATWS is mitigated, then negative reactivity must be added to shut down the reactor. If the RTBs have failed or the control rods are mechanically stuck, operators will need to either manually insert control rods or initiate emergency boration. Successful emergency boration implies the operator starts and aligns a charging pump (NCP or CCP) to provide borated water from one of the borated water sources to the reactor core (OA-OBR-------H). If the RTBs have not failed and the control rods are not mechanically stuck, operators will be directed to manually trip the reactor.[105] The HFE RPS-XHE-TRIP-LT represents operator failure to manually trip the reactor after 90 seconds (given the initial failure to manually trip the reactor within 90 seconds to prevent the ATWS). Additional information is provided in Section 5.1.38.

HPR-ATWS — This top event represents the success or failure of HPR. Success requires 1 of 4 HPI pumps (CCPs or SI pumps) to take suction from the discharge of the RHR pumps and deliver the water to the RCS. HPR will provide long-term

[104] The RCPSI fault tree does not account for the potential loss of the NCP due to SI actuation caused by the opening of pressurizer relief valves to mitigate the initial pressure transient, which is potentially non-conservative. However, for these scenarios, the CCPs would provide alternate RCP seal injection (given the successful automatic start of at least one pump).

[105] Operators will not enter the ATWS procedure (FR-S.1) unless they attempt to manually trip the reactor, but the rods fail to insert.

cooling for the reactor given the HPI system was successful in supplying early makeup water to the reactor. HPR is required if RHR cannot be established. The decay heat will be removed from the containment sump by 1 of 2 RHR heat exchangers or 4 of 8 CCUs. Operator action (OAR_HPATA----H if CCUs are available or OAR_HPATB----H if CCUs are not available) is required to align the RHR pump discharge to the HPI pump suction and verify that the containment sump valves are open and the RWST suction valves are closed. Additional information on the HPR fault tree modeling is provided in Section 5.1.13.

CHG — This top event represents the success or failure of alternate charging to the RCS. In addition to providing the normal source of RCP seal injection, the NCP is also the source of normal charging to the RCS. For transients where the NCP fails after the reactor trip, operators are directed to align a CCP as an alternate source of charging. Given a loss of RCP seal injection, but with RCP seal integrity maintained (via thermal barrier cooling), seal leakage is assumed to increase from a nominal leak rate to 21 gpm per RCP. If AFW or MFW is providing long-term decay heat removal, charging via a CCP is required to provide makeup to the RCS to prevent core damage within 72 hours. An operator action (CHG-XHE-NORMAL) is required to start and align a CCP to provide makeup to the RCS. Additional information on the CHG fault tree modeling is provided in Section 5.1.5.

SAFE/STABLE — This top event represents the success or failure of cooldown and depressurization to allow the accumulators to provide makeup to the RCS. If the RCP seals are leaking at the assumed rate of 21 gpm per RCP due to lack of seal injection, core damage prior to 72 hours can occur if a source of inventory makeup to the RCS is not provided. If alternate charging fails, operators will eventually be directed by CSFST procedures to depressurize the SGs with a modeled minimal success criterion of 3 of 3 TBVs (to the condenser) or an ARV for 1 of 4 SGs. If successful, this depressurization will allow the accumulators (2 of 4 accumulators required for success) to inject into the RCS, thus providing makeup. An operator action (CAD-XHE-SAFESTABLE) is required. If the cooldown and depressurization or accumulators fail, core damage will occur prior to 72 hours. Additional information on the SAFE/STABLE fault tree modeling is provided in Section 5.1.41.

3.4.2 CSSB Event Trees

The consequential SSB event trees, CSSBO and CSSBI, apply to consequential over-cooling transients caused by failure of steam valves downstream of the MSIVs (the turbine stop/control valves and/or TBVs) or steam valves upstream of MSIVs (SG ARVs or SRVs) failing to reclose (if demanded), respectively.[106] The event progression for these two consequential events is very similar to that modeled for the SSBO and SSBI initiating events, respectively. The CSSBO and CSSBI event trees are identical in structure to each other and essentially identical to the

[106] The failure of only one secondary steam valve is assumed to result in a consequential SSB, which is likely a conservative assumption. Results indicate that this modeling assumption has only a minor impact on the overall CDF.

SSBO/SSBI event trees (as described in Section 3.2).[107] The main difference between the consequential SSBs and SSB initiating events is the valve closures and operator actions required for the isolation of the faulted SG, which is treated at the fault tree level. In the CSSBO event tree, the over-cooling transient can be terminated if all the MSIVs are closed by the main steam isolation signal.[108] In the CSSBI event tree, the faulted SG must be isolated in the same manner as required for the SSBI initiating event (i.e., closure of the applicable MSIV, MFIV, AFW injection valves, etc.). Figure 3-23 shows the CSSBI event tree.

3.4.3 CSLOCA Event Tree

A consequential SLOCA event occurs either when a pressurizer PORV or SRV fails to reseat after relieving an initial RCS pressure increase or if there is a failure of RCP seals (given a loss of all seal injection and cooling).[109] The structure of the consequential SLOCA event tree is essentially the same as that for the SLOCA event tree (as described in Section 3.3.4).[110] The impacts of initiating events involved in consequential SLOCA sequences on the SLOCA mitigating systems are reflected via fault tree logic of the related systems and their support systems. Figure 3-24 shows the CSLOCA event tree.

3.4.4 SBO Event Trees

The SBO event tree is a sub-tree that is linked to the LOOP event trees given the failure of onsite emergency power (i.e., the EDGs). During an SBO, both offsite and onsite power are unavailable; therefore, only secondary cooling via the turbine-driven AFW pump is available for decay heat removal. An increase in RCS pressure is expected to occur (due to the loss of condenser heat sink and loss of SG ARVs), which will require the pressurizer PORVs to open to relieve the pressure transient. If the PORVs fail to open, then the pressurizer SRVs will be demanded. After the pressure transient has been mitigated, the pressurizer PORVs or SRVs (if demanded), must reclose to prevent a consequential SLOCA. The LOOP and subsequent SBO will also cause the complete loss of RCP seal injection and cooling; therefore, the integrity of the RCP seals must be queried. If the RCP seals are still intact, then secondary cooling can place the plant in a stable condition once AC power is recovered. If one or both stages of the RCP seals fail, a consequential SLOCA occurs.[111] AC power recovery is required prior to battery depletion or core uncovery; whichever occurs first.[112] If the turbine-driven AFW pump fails or is

---

[107] The RPS top event is not included in the CSSB event trees because they were already addressed in the event tree for the original initiating event.

[108] Unlike the SSBO initiating event category that includes feedwater line ruptures, isolation of a CSSBO does not require the feedwater line valves to be closed.

[109] Stuck-open PORVs or SRVs, or RCP seal LOCA due to total loss of RCP injection/cooling during an SBO are treated in the SBO-1 event tree. In addition, mitigation of stuck-open PORVs or SRVs during an ATWS are modeled within the ATWS event tree.

[110] The RPS top event is not included in the CSLOCA event tree because it was already addressed in the event tree for the original initiating event.

[111] Unlike the other L3PRA Project Level 1 model event trees, the SBO tree has the stage 1 and stage 2 seal failures separated. Even though any combination of seal failures is assumed to result in a consequential SLOCA, the size of the LOCA could affect the time for AC power recovery. Currently, AC power recovery is limited to 2 hours (based on the battery depletion time of the turbine batteries); therefore, the fidelity of different RCP seal LOCAs is not needed. However, the separation of the RCP seal stages was kept in the L3PRA Project Level 1 model to support potential sensitivity studies.

[112] Restoration of AC power can be accomplished by recovery of offsite power or, for plant-centered and switchyard-related LOOPs, the alignment to the alternate switchyard. The recovery of AC power is assumed to occur for both

unavailable, operators will have approximately one hour to recover offsite power.[113] If the turbine-driven AFW pump successfully provides early decay heat removal, operators will have approximately two hours to recover AC power (based on the most limiting depletion time of the turbine building batteries required to realign offsite power to a safety-related bus).[114] Once the batteries are depleted, DC control power is lost; and therefore, it is assumed that the operation of breakers and switchers required to restore offsite power (or the alignment to an alternate switchyard) to the safety-related 4.16 kV AC buses cannot be performed.[115] As such, the L3PRA project Level 1 model assumes core damage if AC power is not recovered prior to two hours.[116] After AC power is recovered and given that no consequential SLOCA has occurred, the event progression is similar to that of a transient. Figure 3-25 shows the SBO event tree.

The top events used in the SBO event tree and their associated success criteria are provided below.

AFW-B — This top event represents the success or failure of the turbine-driven AFW pump to remove decay heat via the SGs.[117] Success requires the automatic actuation and operation of the turbine-driven AFW pump flow to 2 of 4 SGs. If the automatic AFW actuation signal (on low SG water level) fails, operator action (OA-START-AFW-H) is credited to manually start the turbine-driven AFW pump. If AFW fails, operators have approximately one hour to recover AC power and initiate either secondary cooling with the motor-driven AFW pumps or feed and bleed cooling. Additional information on the AFW-B fault tree modeling is provided in Section 5.1.2.

---

safety-related 4.16 kV buses. This may be non-conservative and is noted as a modelling uncertainty in Section 10.

[113] After AC power is recovered, operators will have an additional 30 minutes (approximately) to restore systems that were unavailable during the SBO. ECA-0.0 directs operators to place the hand switches to equipment rendered unavailable by the SBO (e.g., ECCS pumps, motor-driven AFW pumps, ACCW pumps, and CCUs) to the pull-to-lock position. These timings (1 hour to core uncovery and 30 additional minutes until core damage) may be conservative for some sequences (namely those with RCP seal leaks of 182 gpm per RCP and smaller). Plant-specific MELCOR calculations predicted time to core uncovery of 1.9 hours (182 gpm per RCP) and 2.4 hours (21 gpm per RCP), and time to core damage of 3 hours (182 gpm per RCP) and 3.9 hours (21 gpm per RCP). Results indicate that this modeling assumption has only a minor impact on the overall CDF.

[114] The L3PRA Project model includes three different sets of batteries: (1) the safety-related batteries (4-hour battery life) that supply DC power to the breakers/switchers downstream of the reserve auxiliary transformers (RATs); (2) the turbine building batteries (2-hour battery life) that supply DC power to circuit switchers directly upstream of the RATs; and (3) the switchyard batteries (4-hour battery life) that supply DC control power to the circuit breakers that are located in the high voltage switchyard (immediately downstream of 230kV bus 1 and bus 2). Therefore, the 2-hour battery life of the turbine batteries will be limiting.

[115] Some of these breakers may have the capability to be closed manually without DC power. No credit was given in the L3PRA Project Level 1 model to manually close breakers without DC power.

[116] Continued operation of the turbine-driven AFW pump after DC power is lost is possible, which could delay the time to when core damage occurs (or prevent it). However, with no reliable indication of SG water level (after the safety-related batteries are depleted at four hours), there is significant potential for unsustainable operation (e.g., the SGs may be overfilled, which would lead to flooding of the steam lines, including the AFW pump turbine). In addition, AC power recovery is needed to achieve a safe/stable end-state; therefore, continued operation of the turbine-driven AFW pump was not credited in the L3PRA Project Level 1 model. However, credit for continued operation of the turbine-driven AFW is provided in the L3PRA Project Level 2 PRA portion of the L3PRA model.

[117] The MFW system is unavailable due to the LOOP initiating event, and the motor-driven AFW pumps are unavailable due to the loss of all onsite emergency AC power.

PVC-B	This top event represents the success or failure of the PORVs or SRVs to reclose given a LOOP initiating event and subsequent SBO.[118] Success requires that no pressurizer PORVs or SRVs open given the transient or that all opened PORVs or SRVs reclose once RCS pressure is lower than the relief pressure set-points. If a PORV or SRV sticks open, a consequential SLOCA occurs. If operators successfully restore AC power, the sequence is transferred to the SBO-1 event tree. Additional information on the PVC-B fault tree modeling is provided in Section 5.1.32.
BP1	This top event represents the probability of the binding or popping failure of the stage 1 RCP seals, given the complete loss of RCP seal injection and cooling that occurs during a SBO. A failure probability of 0.0125 is taken from the WOG 2000 RCP seal model. If the stage 1 RCP seal fails, RCP seal leakage will increase from 21 gpm per RCP to 76 or 480 gpm per RCP, depending on the integrity of the stage 2 seal. Additional information on the BP-1 fault tree modeling is provided in Section 5.1.3.
BP2	This top event represents the probability of the binding or popping failure of the stage 2 RCP seals, given the complete loss of RCP seal injection and cooling that occurs during a SBO. A failure probability of 0.2 is taken from the WOG 2000 RCP seal model. If the stage 2 RCP seal fails, RCP seal leakage will increase from 21 gpm per RCP to 182 or 480 gpm per RCP, depending on the integrity of the stage 1 seal. Additional information on the BP-2 fault tree modeling is provided in Section 5.1.3.
OPR	Success or failure to recover AC power (via offsite power or an alternate switchyard) within two hours or less is represented by this top event.[119] Success implies the operators were able to restore offsite AC power to both safety-related 4.16 kV AC buses prior to battery depletion. Depending on the success of the turbine-driven AFW pump, operators will have 1 or 2 hours to recover AC power, based on the time to core uncovery or battery depletion (whichever comes first). If AC power is successfully recovered, given a consequential SLOCA, then the sequence transfers to the SBO-1 event tree. Additional information on the OPR fault tree modeling is provided in Section 5.1.30.
AFW-ACR	This top event represents the success or failure of the AFW system (after AC power recovery from a SBO) to remove decay heat via the SGs. This will require the use of 1 of 2 motor-driven AFW pumps or the turbine-driven AFW pump to provide flow to 2 of 4 SGs. Operator action (OA-ORS-------H) is needed to restore the AFW system to operation after AC power recovery.[120] All other modeling assumptions are identical to those

[118] Since both a total loss of condenser heat sink occurs and the SG ARVs are rendered unavailable due to the LOOP and subsequent SBO, it is assumed that RCS pressure will increase causing a demand on the PORVs. The failure of the pressurizer SRVs to reclose is only queried if the PORV(s) fail to open.

[119] The alternate switchyard is assumed to be available only during plant-centered and switchyard-related LOOPs.

[120] This operator action may not be needed if the turbine-driven AFW pump was successfully providing makeup to the SGs prior to AC power recovery. However, since top events needed to reach a safe/stable end-state contain this same HFE, no increase in CDF occurs due to this modeling simplification.

of the AFW top event (as described in Section 3.1.2). Additional information on the AFW-ACR fault tree modeling is provided in Section 5.1.2.

FAB-ACR — This top event represents the success or failure of feed and bleed cooling (after AC power recovery from an SBO). Feed and bleed cooling is required given secondary cooling (AFW) is unavailable. Operator action (OA-ORS-------H) is needed to restore the applicable SSCs for feed and bleed cooling (e.g., CCPs, DC power to PORVs) after AC power recovery. In addition, the operator action (OAB-SBOACR---H) to initiate feed and bleed cooling is conditioned on AC power recovery after an SBO. All other modeling assumptions are identical to that of the FAB top event (as described in Section 3.1.2). If feed and bleed cooling fails, core damage is assumed to occur. Additional information on the FAB-ACR fault tree modeling is provided in Section 5.1.8.

FABR-ACR — This top event represents the success or failure of long-term feed and bleed operation (after AC power recovery from an SBO). The operator action (OA-LTFB-ACRA-H if CCUs are available or OA-LTFB-ACRB-H if CCUs are not available) for alignment of feed and bleed recirculation is conditioned given AC power recovery after an SBO. In addition, the AC power support logic is specialized for conditions following successful AC power restoration. All other modeling assumptions are identical to that of the FABR top event (as described in Section 3.1.2). If feed and bleed recirculation fails, core damage is assumed to occur. Additional information on the FABR-ACR fault tree modeling is provided in Section 5.1.9.

CHG-ACR — This top event represents the success or failure of alternate charging to the RCS (after AC power recovery from an SBO). This fault tree is a duplicate of the CHG fault tree that is needed for the deactivation of the EDG dependencies after AC power recovery. All modeling assumptions are identical to that of the CHG top event (as described in Section 3.1.2). Additional information on the CHG-ACR fault tree modeling is provided in Section 5.1.5.

SAFE/STABLE-ACR — This top event represents the success or failure of cooldown and depressurization to allow the accumulators to provide makeup to the RCS (after AC power recovery from an SBO). This fault tree is a duplicate of the SAFE/STABLE fault tree that is needed for the deactivation of the EDG dependencies after AC power recovery. All modeling assumptions are identical to that of the SAFE/STABLE top event (as described in Section 3.1.2). Additional information on the SAFE/STABLE-ACR fault tree modeling is provided in Section 5.1.41.

3.4.5 SBO-1 Event Tree

The SBO-1 event tree is used to model the response to a consequential SLOCA (either from a pressurizer PORV or SRV failing to reclose, or a failure of RCP seals) after the restoration of AC power (either from the recovery of offsite power or the alignment of an alternate switchyard) following an SBO. The CSLOCA event tree (as described in Section 3.4.3) cannot be used

because the transition from the LOOP event tree to the SBO event tree, and then subsequently to the SBO-1 event tree, requires the activation and deactivation of the EDG dependencies of applicable SSCs. The structure of the SBO-1 event tree is the same as that for the CSLOCA event tree. However, the SBO-1 event tree uses "-ACR" versions for applicable top event fault trees that deactivates the EDG dependencies for electrical power. In addition, the "-ACR" fault trees for AFW-LOCA-ACR and FAB-SLOCA-ACR have an operator action (OA-ORS-------H) representing the need to restore the systems after recovery of AC power. Figure 3-26 shows the SBO-1 event tree.

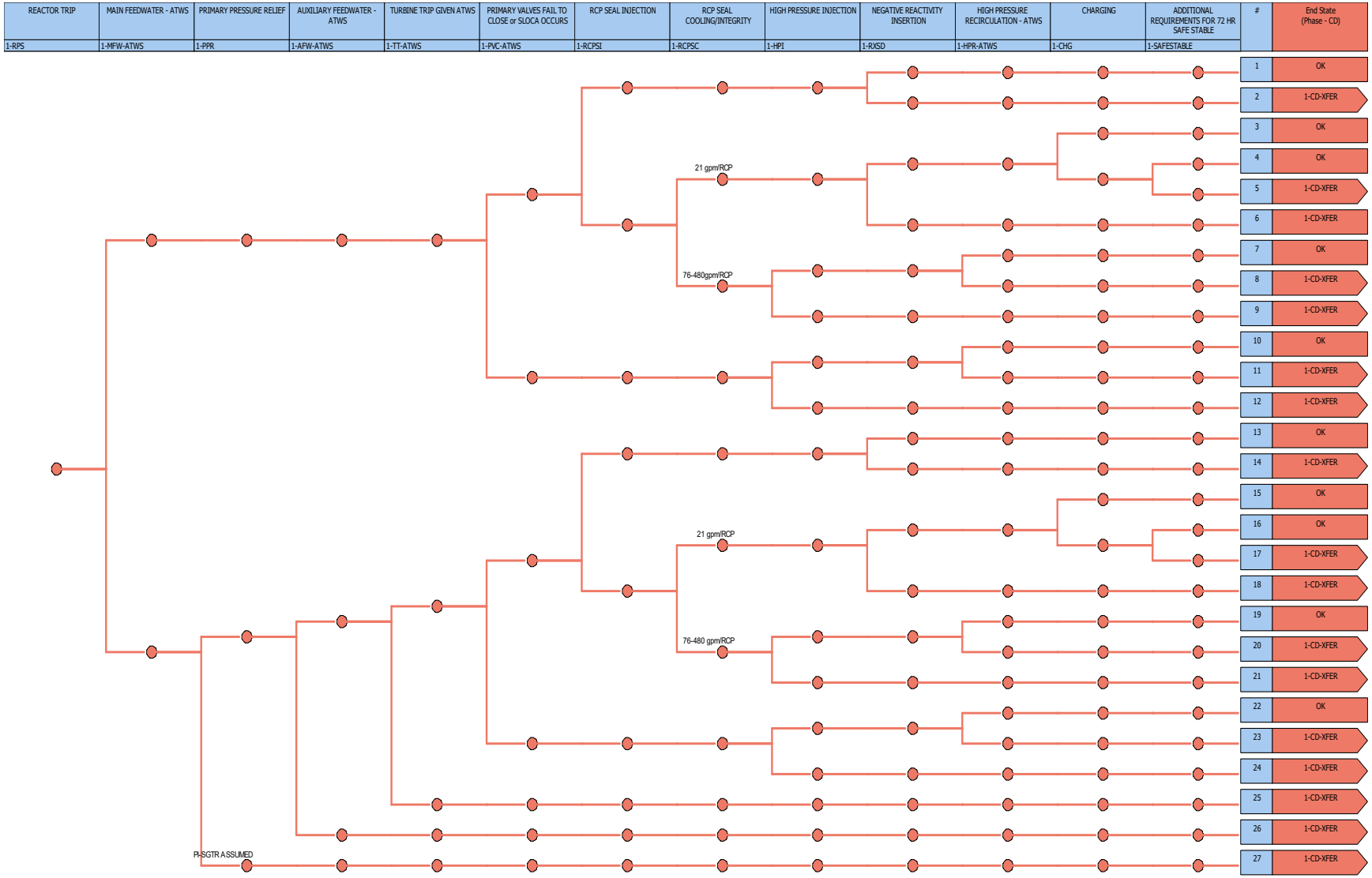


Figure 3-22 ATWS Event Tree

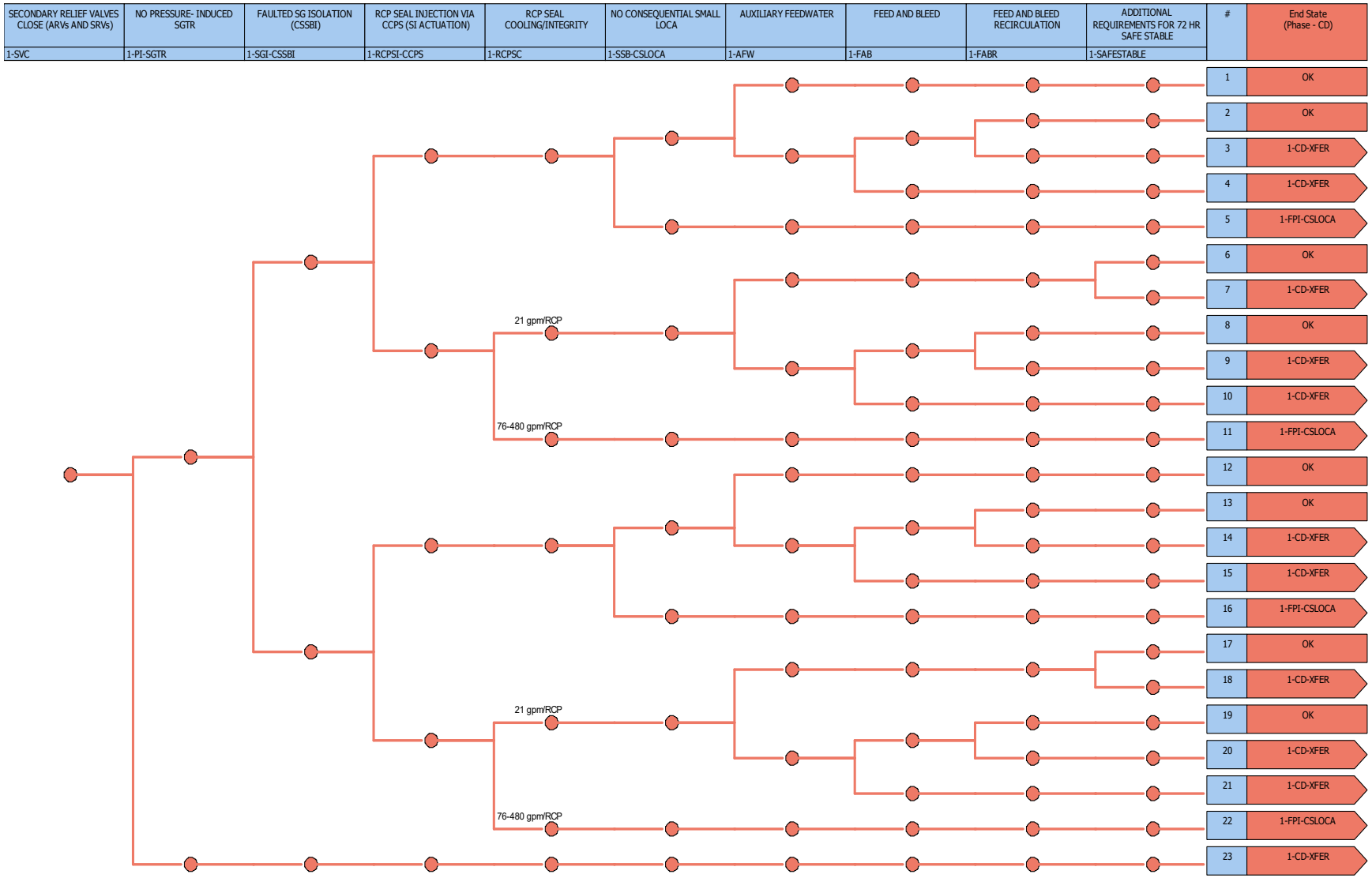


Figure 3-23 CSSBI Event Tree

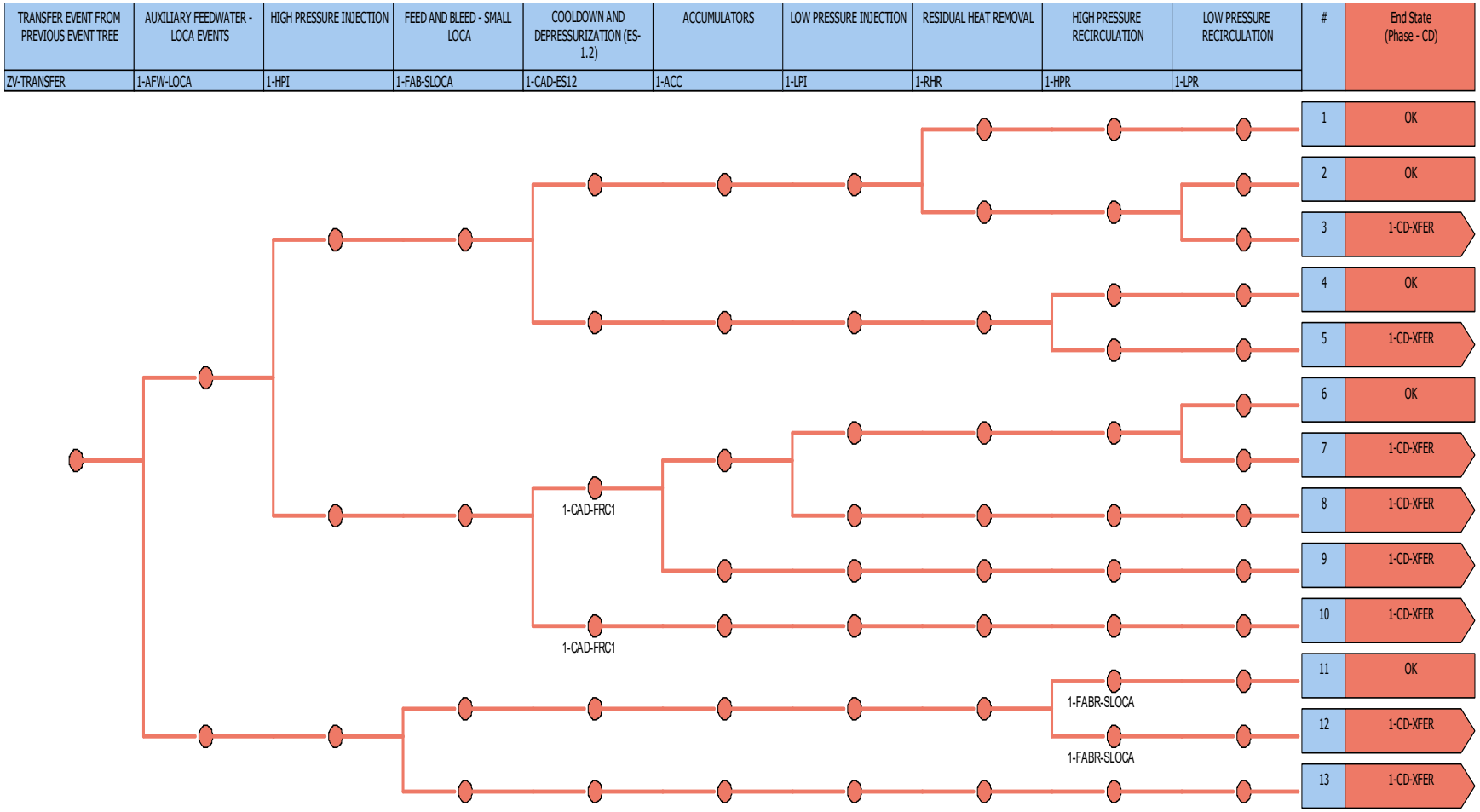


Figure 3-24 Consequential SLOCA Event Tree

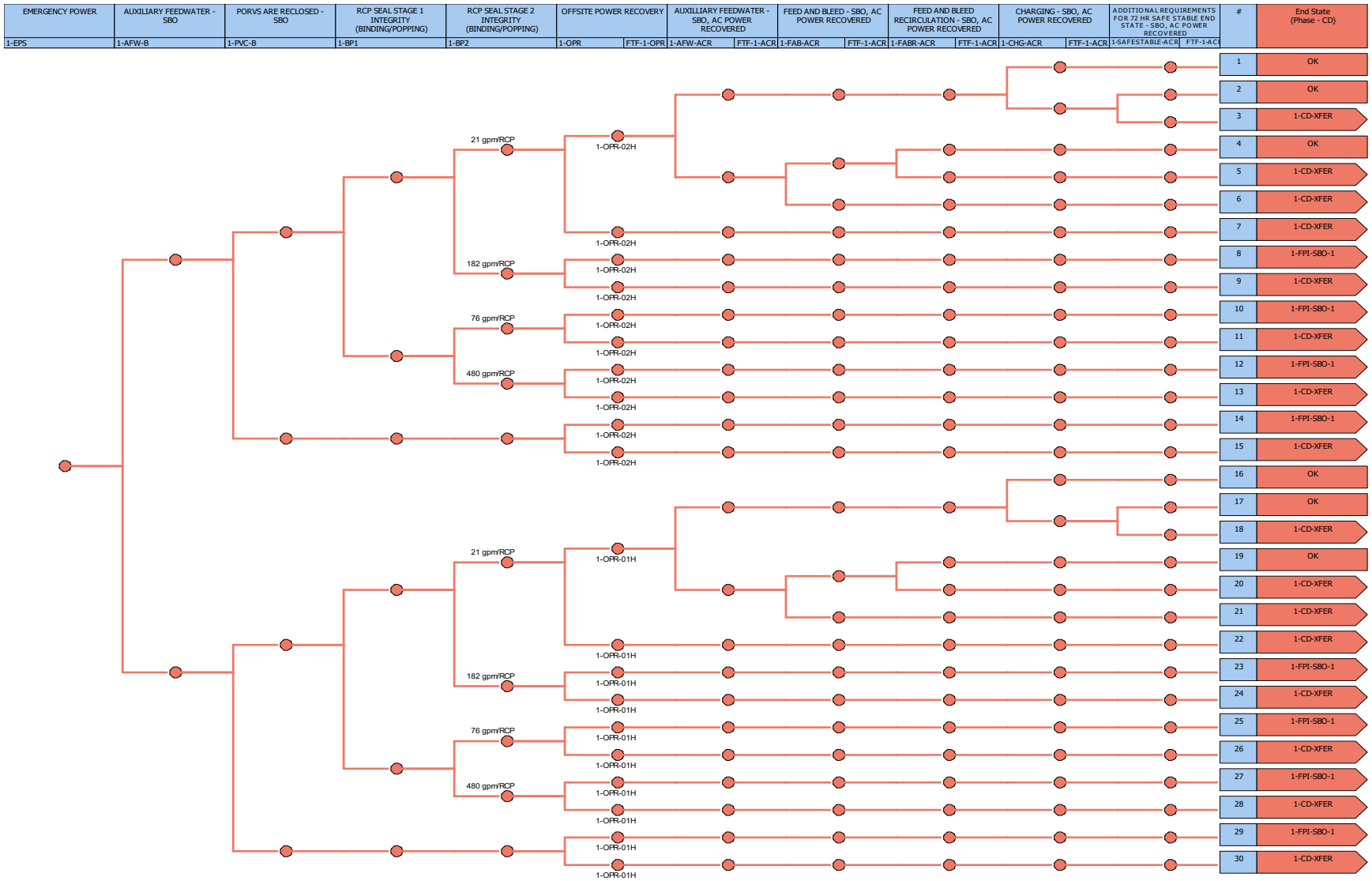


Figure 3-25 SBO Event Tree

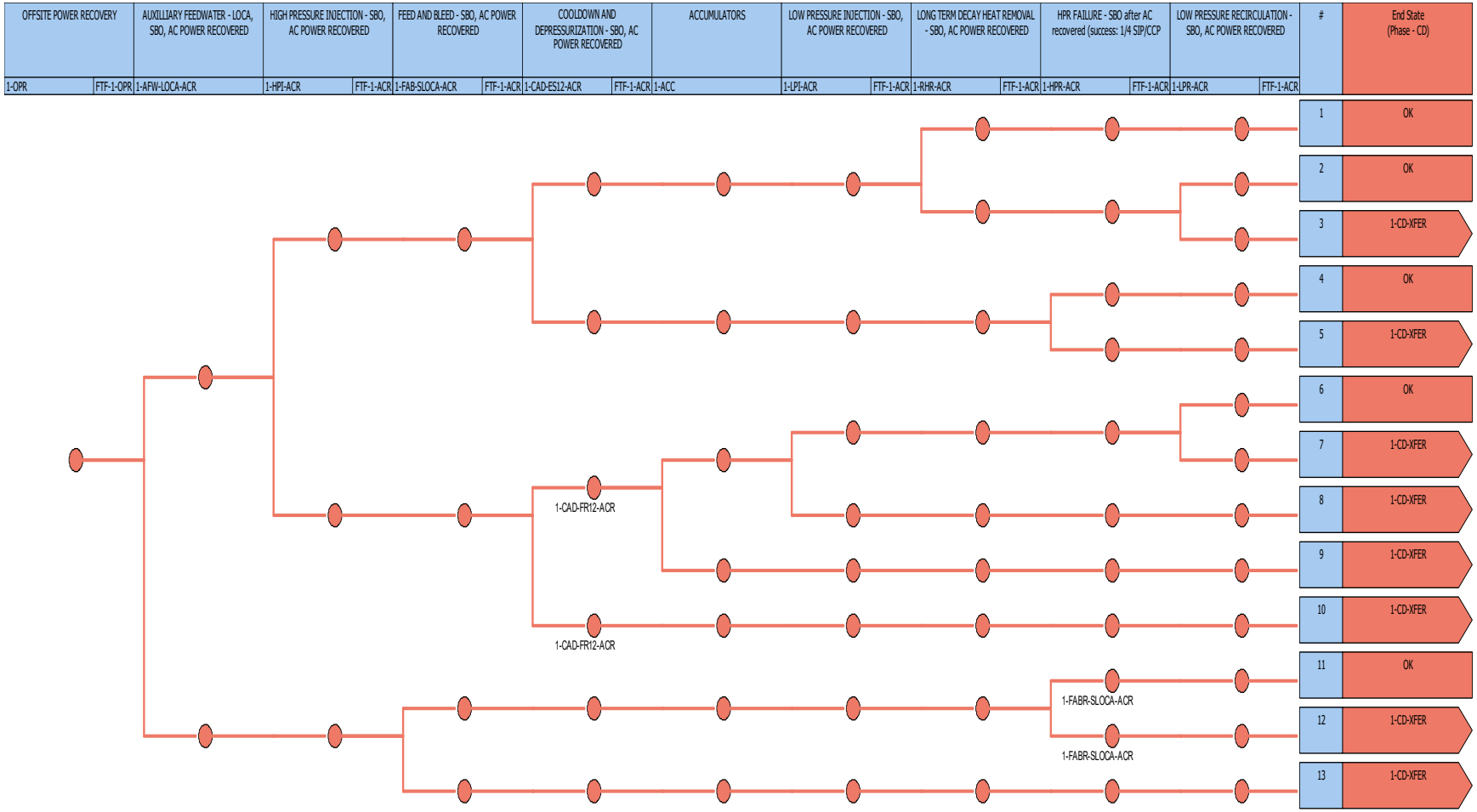


Figure 3-26 SBO-1 Event Tree

3.5 Interfacing System LOCA Events

This class of accidents consists of failures of RCS pressure isolation valves such that high pressure and high temperature primary coolant can enter lower pressure rated components in a connected system, possibly resulting in the rupture of those components that may be outside the containment structure. This would result in a LOCA that releases primary coolant outside of the containment structure and preclude coolant from reaching the emergency containment sump. Long term recirculation of emergency core coolant is not possible (since no coolant reaches the emergency sump) and the accident is assumed to result in core damage.

The NRC sponsored research on ISLOCA risk in the late 1980's and early 1990's. Based on this work, the following observations were made on ISLOCA risk:

- Postulating the catastrophic failure of two (or more) pressure isolation valves that have been verified, as part of a plant's normal startup procedure, to be fully closed and leak-tight, is speculative. No instances of this happening have been found in the operating experience data.

- Even relatively low-pressure (e.g., 300 psi) rated pipe has a significant probability of surviving intact when pressurized to full RCS operating pressure and temperature.

- Even if a rupture in a lower-pressure rated system were to occur, valves are typically in place to potentially isolate the rupture.

As part of the L3PRA project, issues were identified pertaining to modeling and quantifying RCS/ECCS ISLOCA sequences. Some very limited data was identified in the 2010 update of NUREG/CR-6928 (NRC, 2007) that implied the potential for CCF of isolation valves (i.e., large internal leakage) that could result in an ISLOCA. Due to the large uncertainty related to this data, and the risk-significance associated with ISLOCAs, an expert elicitation was performed to address these issues. A brief overview of the ISLOCA expert elicitation is provided in Section 3.5.1.

Based on the general ISLOCA insights provided above and insights from the reference plant model ISLOCA analysis and the ISLOCA expert elicitation, a three-valve failure screening criterion was applied to determine which ISLOCA pathways would be included in the L3PRA project Level 1 model. This criterion simply states that if three or more valves need to fail to lead to an ISLOCA, then the applicable ISLOCA pathways screen out from further consideration. The application of this criterion resulted in the inclusion of four ISLOCA pathways in the L3PRA project Level 1 model:

- RHR system via hot leg suction lines from the RCS

- RHR system via the cold leg injection lines to the RCS

- ACCW system via the RCP thermal barrier heat exchangers

- RCP stage 1 seal leak-off

Descriptions of the L3PRA project Level 1 event tree modeling of these four ISLOCA pathways is presented in Sections 3.5.2 through 3.5.5.

3.5.1 ISLOCA Expert Elicitation

As mentioned previously, issues were identified pertaining to the modeling and quantification of RCS/ECCS ISLOCA sequences. Specifically, some very limited data was identified that implied the potential for CCF of isolation valves (i.e., large internal leakage) that could result in an ISLOCA. Due to the large uncertainty related to this data, and the risk-significance associated with ISLOCAs, an expert elicitation was performed to address these issues. The focus of the expert elicitation was on ISLOCA sequences in the portions of the ECCS consisting of the RHR system and SI system for a Westinghouse four-loop PWR.

The elicitation process essentially employed a simplified form of the Senior Seismic Hazard Analysis Committee (SSHAC) guidance for probabilistic seismic hazard analysis as described in NUREG/CR-6372, "Recommendations for Probabilistic Seismic Hazard Analysis: Guidance on Uncertainty and Use of Experts," (LLNL, 1997) and NUREG-2117, "Practical Implementation Guidelines for SSHAC Level 3 and 4 Hazard Studies," (NRC, 2012). SSHAC defines a formal, structured, interactive process for conducting expert judgment on complex technical issues.

The elicitation consisted of a combination of group and individual interviews using video conferences to: (1) train the experts, (2) familiarize the experts with the plant systems, and (3) perform initial individual elicitations to gather preliminary data. The results of the initial sessions were aggregated into a detailed summary of the information generated during the elicitation. The elicitation process concluded with a group meeting to review and refine the results of the initial elicitation.

The following three types of experts were required to perform the ISLOCA elicitation:

- Experts in probabilistic risk assessment and the facilitation of expert elicitations
- Experts experienced in component (valve or piping) failures, seal leakage, and modeling of common-cause failures
- Experts on RHR and SI systems, who are familiar with system design, operation, and maintenance, and possible maintenance errors that could cause component and/or system failures

Information elicited from the expert panel included: (1) large internal leakage failure rates for isolation valves, (2) conditional failure probabilities for isolation valves in series, (3) failure to close probabilities for MOVs when exposed to large differential pressures, and (4) location of external break of pipe or other components due to over pressurization.[121, 122]

[121] The expert elicitation did not consider leakages of less than or equal to 0.8-inch that could result in core damage in less than 72 hours.

[122] The L3PRA Level 1 model does not consider the conditional failure of the 2nd valve in series failing prior to the 1st valve.

3.5.2 ISLOCA from RHR Hot Leg Suction Lines

The ISL-RHR-HLS event tree represents a RHR system ISLOCA due to the failure of the hot leg suction valves from the RCS. This event tree is shown in Figure 3-27 and has the following events arranged in the approximate order in which they would be expected to occur.

IE-ISL-RHR-HLS The plant is in an operating mode in which a RHR system ISLOCA can occur via the hot leg suction lines.

IEFT-ISL-RHR-HLS This top event represents the fault tree logic that can lead to an RHR system ISLOCA via the hot leg suction lines. This fault tree is used to develop the RHR system ISLOCA frequency based on failures of the RHR hot leg suction MOVs for hot leg 1 or hot leg 4 that can lead to RCS pressure being experienced by low-pressure RHR system piping and components (e.g., RHR heat exchangers, pump suction piping, and pump seals).[123] Additional information on the IEFT-ISL-RHR-HLS fault tree modeling is provided in Section 5.1.16.

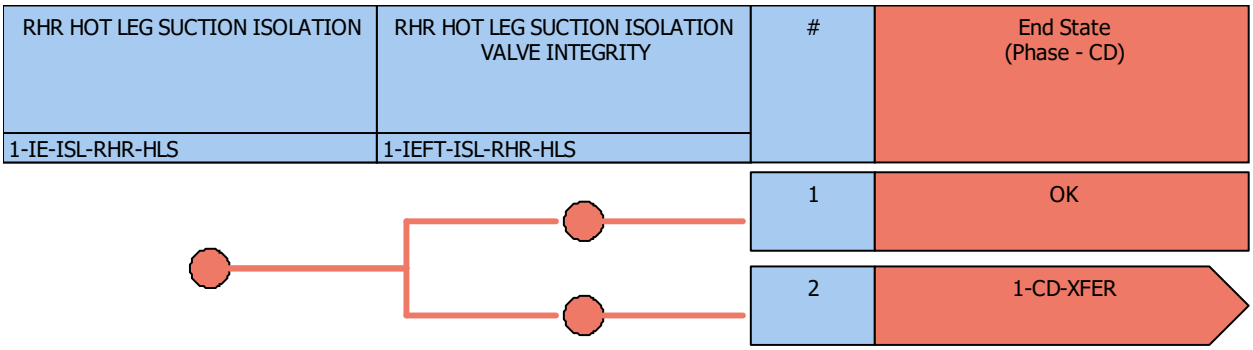


Figure 3-27 RHR Hot Leg Suction Line ISLOCA Event Tree

No isolation is possible for this ISLOCA path (~12-inch diameter break), because there are no isolation valves rated for full RCS pressure downstream of hot leg suction MOVs for hot leg 1 or hot leg 4. Therefore, core damage is assumed to occur if an ISLOCA via this pathway occurs.

3.5.3 ISLOCA from RHR Cold Leg Injection Lines

The ISL-RHR-CLI-A and ISL-RHR-CLI-B event trees represent an RHR system ISLOCA due to the failure of the cold leg injection valves to the RCS. These event trees are identical in structure (shown in Figure 3-28 for cold legs 1 and 2) and have the following events arranged in the approximate order in which they would be expected to occur.

IE-ISL-RHR-CLI-A
IE-ISL-RHR-CLI-B The plant is in an operating mode in which an RHR system ISLOCA can occur via the cold leg injection lines.

[123] SSIE fault trees allow for the calculation of plant-specific initiating event frequencies for system failures that are so rare they are not observed in failure data sets. In addition, by using the fault tree logic, the individual component importance measures can be captured versus rolling up the RHR valve failures into a single initiating event.

IEFT-ISL-RHR-CLI-A This top event represents the fault tree logic that can lead to a

IEFT-ISL-RHR-CLI-B RHR system ISLOCA via the cold leg injection lines. This fault tree is used to develop the RHR system ISLOCA frequency based on failures of the RHR cold leg injection check valves for cold legs 1–4that can lead to RCS pressure being experienced by low-pressure RHR system piping and components (e.g., RHR heat exchangers, pump suction piping, and pump seals). Additional information on the IEFT-ISL-RHR-CLI-A and IEFT-ISL-RHR-CLI-B fault tree modeling is provided in Section 5.1.15.

ISL-RHR-CLI-A-REC This top event represents the failure to isolate the RHR system

ISL-RHR-CLI-B-REC ISLOCA via the cold leg injection lines. The RHR ISLOCA break size from the cold leg injection lines will be limited by the size of the RHR cold injection line piping diameter. This results in a MLOCA that can be mitigated by injection via the CCPs or SI pumps until the depletion of the RWST. Operator action (OA-IS-ISLRHR-H) can terminate the RHR system ISLOCA by manually closing valves in the affected cold legs. If the ISLOCA is not isolated (due to operator or hardware failures), core damage is assumed. Additional information on the ISL-RHR-CLI-A-REC and ISL-RHR-CLI-B-REC fault tree modeling is provided in Section 5.1.26.

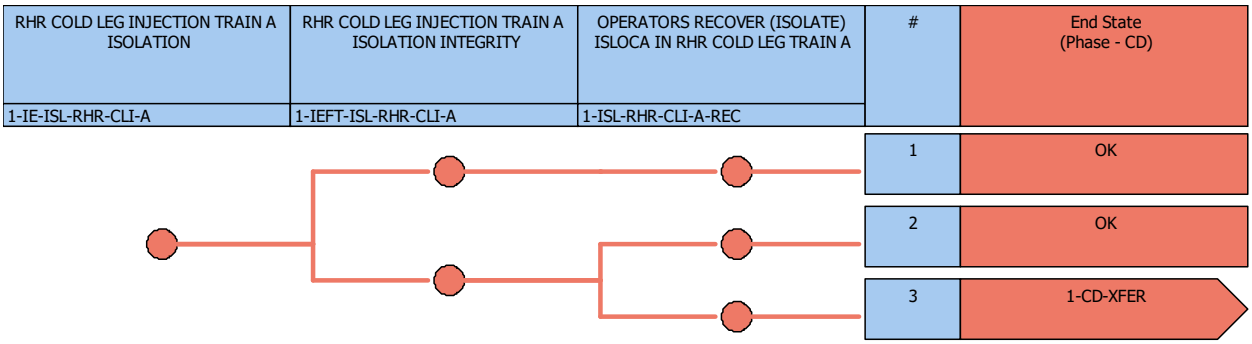


Figure 3-28 RHR Cold Leg Injection Line ISLOCA Event Tree

ISLOCA from RCP Thermal Barrier Heat Exchangers Tube Rupture

The ISL-RCP-TBHX event tree represents an ACCW system ISLOCA from a tube rupture from any of the four RCP thermal barrier heat exchangers. Two different ISLOCA pathways exist for this event tree: (1) upstream of the RCP thermal barrier heat exchangers and (2) downstream of the RCP thermal barrier exchangers. The ISL-RCP-TBHX event tree (shown in Figure 3-29) has the following events arranged in the approximate order in which they would be expected to occur.

IE-ISL-RCP-TBHX The top event represents the rupture of a RCP thermal barrier heat exchanger tube. The reference plant model rupture frequency was multiplied by four to represent the frequency of tube rupture from any of the RCP thermal barrier heat exchangers. This initiating event is limited to a rupture of one

tube of one RCP thermal barrier heat exchanger (i.e., the concurrent rupture of more than one heat exchanger or more than one tube is not considered in the L3PRA project Level 1 model).

ISL-RCP-TBHX-UPSTREAM This top event represents the potential for an ACCW system ISLOCA upstream of the RCP thermal barrier heat exchangers. Given rupture of a RCP thermal barrier heat exchanger tube, directly upstream is a check valve.[124] If the applicable check valve re-seats, no ISLOCA will occur. If the applicable check valve fails, an ISLOCA occurs. Additional information on the ISL-RCP-TBHX-UPSTREAM fault tree modeling is provided in Section 5.1.25.

ISL-RCP-TBHX-DNSTREAM This top event represents the potential for an ACCW system ISLOCA downstream of the ruptured RCP thermal barrier heat exchanger. Two MOVs are available to prevent an ISLOCA downstream of the RCP thermal barrier heat exchangers. The first MOV is unique to each individual RCP. The second MOV is common to all four RCPs. These MOVs receive an automatic closure signal on high flow. If either of these MOVs close, the ISLOCA will be prevented. If both MOVs fail, a subsequent ISLOCA occurs. Additional information on the ISL-RCP-TBHX-DNSTREAM fault tree modeling is provided in Section 5.1.21.

ISL-RCP-TBHX-RPT This top event represents the potential for relief valves to prevent the failure of ACCW piping, thereby limiting the SLOCA to inside containment. If the isolation by the upstream check valves or the downstream MOVs fail, the ACCW supply and return lines will be pressurized. Relief valves are located on the ACCW RCP motor cooling water return line of each RCP. Since the rupture is limited to a single tube, these relief valves could prevent over pressurization of ACCW system outside containment. If all four relief valves open, a SLOCA inside the containment occurs.[125] If these valves fail to open, ACCW piping (both inside and outside containment) will be pressurized.[126] Additional information on the ISL-RCP-TBHX-RPT fault tree modeling is provided in Section 5.1.24.

ISL-RCP-TBHX-HV1974 This top event represents the failure to isolate the ACCW system ISLOCA downstream of the ruptured RCP thermal barrier heat exchanger. Operator action (OA-IS-ISLACC-H) can limit the RCP thermal barrier heat exchanger rupture to a SLOCA inside containment by manually closing HV1974. If HV1974 is not closed, the ISLOCA continues and core damage is assumed. Additional information on the ISL-RCP-TBHX-HV1974 fault tree modeling is provided in Section 5.1.22.

ISL-RCP-TBHX-HV1978 This top event represents the failure to isolate the ACCW system ISLOCA upstream of the ruptured RCP thermal barrier heat exchanger. Operator action (OA-IS-ISLACC-H) can limit the RCP thermal barrier heat exchanger rupture to a SLOCA inside containment by manually closing HV1978. If HV1978 is not closed, the ISLOCA continues and core damage is

[124] Since this event tree represents the failure of any of the four RCP thermal barrier heat exchanger and a single event tree is used, the RCP specific valves are represented by a single basic event.

[125] An OK end-state is used if the LOCA inside containment occurs, because these scenarios are already accounted for in the LOCA initiating event data.

[126] The success criteria requiring all four relief valves to open is potentially conservative.

assumed. Additional information on the ISL-RCP-TBHX-HV1978 fault tree modeling is provided in Section 5.1.23.

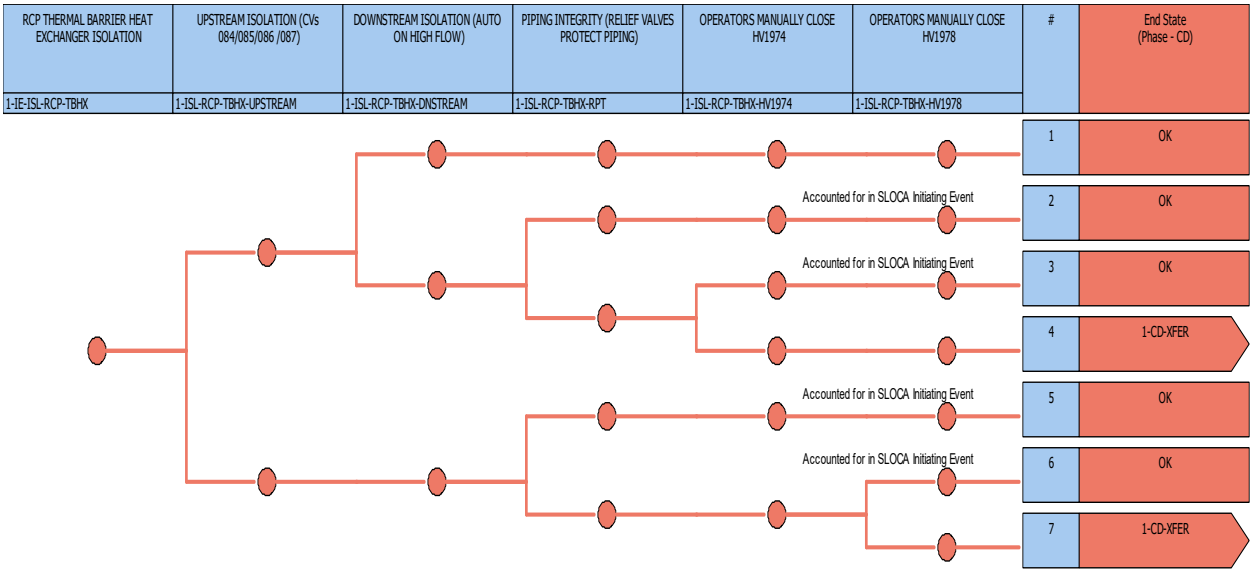


Figure 3-29 RCP Thermal Barrier Heat Exchanger Tube Rupture ISLOCA Event Tree

3.5.4 ISLOCA from RCP Seal Leak-Off

The ISL-RCP-S1LO event tree represents an ISLOCA from a RCP seal leak-off return line. A failure of RCP seals (resulting in a SLOCA) occurs only when there is a total loss of both RCP seal injection and ACCW flow to the RCP thermal barrier heat exchangers. Initiating events or initiating events with concurrent system failures that result in the loss of both RCP seal injection and cooling are:

- LOOP with subsequent SBO
- Total loss of NSCW
- Loss of ACCW followed by loss of seal injection via the NCP.[127]
- Loss of seal injection via the NCP followed by loss of ACCW

For an ISLOCA via the RCP seal leak-off return line to occur, in addition to the complete loss of RCP injection and cooling, the RCP stage 1 seals must fail, while the integrity of the stage 2 seals must be maintained. If the stage 2 RCP seals fail, a SLOCA inside containment will occur. The ISL-RCP-S1LO event tree (shown in Figure 3-30) has the following events arranged in the approximate order in which they would be expected to occur.

[127] The alignment of a CCP to supply RCP seal injection is credited during loss of ACCW and loss of RCP seal injection initiating events.

IE-ISL-RCP-S1LO The plant is in an operating mode in which an ISLOCA can occur via the seal leak-off return line.

IEFT-ISL-RCP-S1LO This top event represents the fault tree logic that can lead to an ISLOCA via the RCP seal leak-off return line. This fault tree is used to develop the RCP seal leak-off return line ISLOCA frequency based on initiating events (combined with subsequent system failures and unavailabilities) that can lead to the complete failure of RCP seal injection and cooling.[128] In addition, the stage 1 RCP seals need to fail while the integrity of the stage 2 seals is maintained for an ISLOCA via this pathway to occur. Additional information on the IEFT-ISL-RCP-S1LO fault tree modeling is provided in Section 5.1.14.

ISL-RCP-S1LO-HV8141 This top event represents the failure to terminate the ISLOCA by the closure of RCP seal leak-off return line isolation valves for each of the four RCPs. If RCP leakage through a RCP seal leak-off line increases, operators will receive a control room alarm on high flow.[129] Operator action (OA-IS-ISLLKF-H) is required to manually close all four valves. Additional information on the ISL-RCP-S1LO-HV8141 fault tree modeling is provided in Section 5.1.19.

ISL-RCP-S1LO-AUTO This top event represents the failure to limit the SLOCA to inside the containment by the closure of RCP seal leak-off return line containment isolation valves. These valves will close automatically due to a containment isolation signal given a SI actuation. During a SBO, automatic closure of RCP seal leak-off return line containment isolation valves is not possible because 480 V AC power is lost; therefore, operator action (OA-IS-ISLSEALSBO) is required to manually close the isolation valve (located outside containment). Additional information on the ISL-RCP-S1LO-AUTO fault tree modeling is provided in Section 5.1.18.

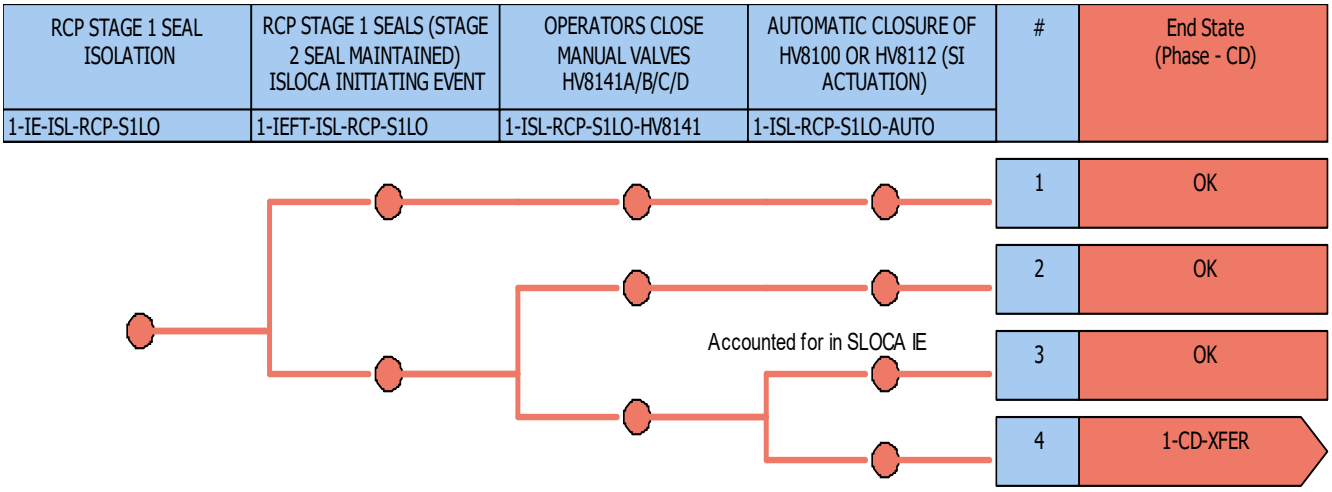


Figure 3-30 RCP Seal Leak-Off ISLOCA Event Tree

[128] The initiating events included in this initiating event fault tree are (1) LOOP with subsequent SBO, (2) total loss of NSCW, (3) loss of ACCW with the failure to align the CCPs for seal injection, and (4) the loss of the normal seal injection (i.e., the NCP) with subsequent failure to align the CCPs for alternate seal injection and loss of ACCW flow to the RCP thermal barrier heat exchangers.

[129] These valves cannot be isolated during an SBO due to the loss of instrument air.

4 SUCCESS CRITERIA ANALYSES

The term success criteria generally applies to both the minimal equipment needed to accomplish a safety function modeled in the probabilistic risk assessment (PRA) [e.g., one of two high-pressure injection (HPI) trains] and the sequence timing for key operator actions (e.g., feed and bleed operation must be initiated within four hours after loss of secondary-side cooling). The general approach for determining the success criteria for the L3PRA project Level 1 model mainly relies on the reference plant PRA model success criteria. Consistent with the overall project approach for leveraging the reference plant peer-reviewed PRA model, emphasis was placed on the facts and observations from the peer review of the reference plant PRA model, and an audit was performed of selected aspects of the reference plant PRA model success criteria. Specifically, the peer review of the reference plant PRA model had no findings nor unmet supporting requirements in the success criteria element. However, a cut set comparison between the reference plant PRA model and the plant-specific Standardized Plant Analysis Risk (SPAR) standardized plant analysis risk (associated SPAR) model revealed some differences in the success criteria. This comparison was the main means of identifying issues to resolve related to the success criteria used in the L3PRA project Level 1 PRA model. Other insights were developed by (1) reviewing the reference plant PRA event tree and fault tree modeling, (2) questions that arose during the development and improvements to the L3PRA project Level 1 model, or (3) questions from reviewers (e.g., Advisory Committee on Reactor Safeguards (ACRS), Westinghouse Owner's Group (WOG)-led peer review, and other internal reviews).

The identified success criteria issues were reviewed extensively and either the reference plant PRA model success criteria were adopted, or new criteria were selected for use in the L3PRA project Level 1 model based on NRC thermal hydraulic analyses using MELCOR. Table 4-1 provides the general success criteria for the events defined in Section 2 and Section 3.

One additional issue that arose during completion of the L3PRA project Level 1 internal event model involves event tree sequences that are safe (i.e., no core damage), but not stable, at 24 hours (i.e., they would result in core damage at some point after 24 hours). For these sequences, the L3PRA project Level 1 model generally extends the accident sequence to 72 hours. Additional information on how these sequences are addressed is provided in Section 3.1.1

Table 4-1 L3PRA Project Level 1 Model General Success Criteria

Initiator	Inventory Control		Decay Heat Removal		Notes
	Injection Phase	Recirculation Phase	Early	Late	
Transient Initiators with MFW Potentially Available ▪ Turbine Trip ▪ Reactor Trip ▪ Other Transients ▪ Loss of Two Safety-Related 120 V Alternating Current (AC) Panels ▪ Loss of NSCW ▪ Loss of ACCW ▪ Loss of RCP Seal Injection	1 HPI Train to 2 RCS Cold Legs[130]	1 HPR Train to 2 RCS Cold Legs[131]	1 AFW Train to 2 SGs or 1 MFW Train to 1 SG[132] or [1 PORV and 1 CCP Train to 2 RCS Cold Legs]	1 AFW Train to 2 SGs[133] or 1 MFW Train to 1 SG or [1 HPR Train to 2 RCS Cold Legs]	RCS inventory control is only needed if a consequential LOCA (RCP seal failure or stuck-open pressurizer PORV/SRV) occurs. For a loss of NSCW, core damage is assumed if an RCP seal LOCA occurs or a pressurizer PORV/SRV fails to reclose (if demanded).

[130] A HPI train consists of either a CCP or SI pump.

[131] The RHR pumps are used in HPR to provide suction to the HPI pumps in a piggy-back mode. The heat sink for the recirculation water should be provided either by the CCW to the RHR heat exchanger or by 4 of 8 CCUs.

[132] Successful AFW or MFW also requires steam removal for the SGs being fed. Steam removal for a SG requires either: (1) 3 of 3 TBVs, (2) the SG ARV, or (3) 1 of 5 SG SRVs.

[133] CST inventory makeup is needed to achieve a 72-hour safe/stable end state if AFW is used for long-term decay heat removal for transient initiating events and SGTR.

Table 4-1 L3PRA Project Level 1 Model General Success Criteria (cont.)

Initiator	Inventory Control		Decay Heat Removal		Notes
	Injection Phase	Recirculation Phase	Early	Late	
Transient Initiators with MFW Potentially Available ▪ Turbine Trip ▪ Reactor Trip ▪ Other Transients ▪ Loss of Two Safety-Related 120 V Alternating Current (AC) Panels ▪ Loss of NSCW ▪ Loss of ACCW ▪ Loss of RCP Seal Injection	1 HPI Train to 2 RCS Cold Legs[134]	1 HPR Train to 2 RCS Cold Legs[135]	1 AFW Train to 2 SGs or 1 MFW Train to 1 SG[136] or [1 PORV and 1 CCP Train to 2 RCS Cold Legs]	1 AFW Train to 2 SGs[137] or 1 MFW Train to 1 SG or [1 HPR Train to 2 RCS Cold Legs]	RCS inventory control is only needed if a consequential LOCA (RCP seal failure or stuck-open pressurizer PORV/SRV) occurs. For a loss of NSCW, core damage is assumed if an RCP seal LOCA occurs or a pressurizer PORV/SRV fails to reclose (if demanded).

[134] A HPI train consists of either a CCP or SI pump.

[135] The RHR pumps are used in HPR to provide suction to the HPI pumps in a piggy-back mode. The heat sink for the recirculation water should be provided either by the CCW to the RHR heat exchanger or by 4 of 8 CCUs.

[136] Successful AFW or MFW also requires steam removal for the SGs being fed. Steam removal for a SG requires either: (1) 3 of 3 TBVs, (2) the SG ARV, or (3) 1 of 5 SG SRVs.

[137] CST inventory makeup is needed to achieve a 72-hour safe/stable end state if AFW is used for long-term decay heat removal for transient initiating events and SGTR.

Table 4-1 L3PRA Project Level 1 Model General Success Criteria (cont.)

Initiator	Inventory Control		Decay Heat Removal		Notes
	Injection Phase	Recirculation Phase	Early	Late	
Transient Initiators that Result in MFW Failure ▪ Loss of MFW ▪ Loss of Condenser Heat Sink ▪ LOOP Initiating Events ▪ Loss of Safety-Related 125 Volt Direct Current (DC) Bus ▪ Loss of Safety-Related 4.16 Kilovolt AC Bus ▪ Secondary-Side Breaks ▪ Loss of Instrument Air ▪ Inadvertent SI Actuation	1 HPI Train to 2 RCS Cold Legs	1 HPR Train to 2 RCS Cold Legs	1 AFW Train to 2 SGs.[138] or [1 PORV and 1 CCP Train to 2 RCS Cold Legs]	1 AFW Train to 2 SGs or [1 HPR Train to 2 RCS Cold Legs]	RCS inventory control is only needed if a consequential LOCA (RCP seal failure or stuck-open pressurizer PORV/SRV) occurs.

[138] For SSBs upstream of the MSIVs or downstream of the main feedwater isolation valves (MFIVs), the faulted SG is assumed to be unavailable for decay heat removal. For SSBs downstream of the MSIVs, any SG in which the MSIVs are not closed is assumed to be unavailable for decay heat removal.

Table 4-1 L3PRA Project Level 1 Model General Success Criteria (cont.)

Initiator	Inventory Control		Decay Heat Removal		Notes
	Injection Phase	Recirculation Phase	Early	Late	
SLOCA	1 HPI Train or 1 LPI Train to 2 RCS Cold Legs[139, 140]	1 HPR Train or 1 LPR Train to 2 RCS Cold Legs[141]	1 AFW Train to 2 SGs or [2 PORVs and 1 SI Train or 1 PORV and 1 CCP Train to 2 RCS Cold Legs]	1 RHR Train and 3 CCUs[142] or 1 HPR Train or 1 LPR Train to 2 RCS Cold Legs	For LPI to provide inventory control in the injection phase, the operators must successfully perform a secondary-side cooldown and depressurization. In addition, at least two accumulators must provide initial inventory makeup to the RCS.

[139] The RHR pumps are used for low-pressure injection.

[140] For SLOCAs (including consequential SLOCAs), all four RCS cold legs are considered available for HPI, LPI, and recirculation.

[141] The RHR pumps are used in low pressure sump recirculation. The heat sink for the recirculation water should be provided either by the CCW to the RHR heat exchanger or by 4 of 8 CCUs.

[142] The RHR pumps are used in shutdown cooling mode. The heat sink is provided by the CCW to the RHR heat exchanger. However, 3 of 8 CCUs are needed to function to prevent the containment spray from actuating. If containment sprays are actuated, the RWST level will reach the recirculation switch-over level prior to reaching the entry conditions for shutdown cooling mode of RHR.

Table 4-1 L3PRA Project Level 1 Model General Success Criteria (cont.)

Initiator	Inventory Control		Decay Heat Removal		Notes
	Injection Phase	Recirculation Phase	Early	Late	
SGTR	1 HPI Train to 2 RCS Cold Legs[143]	1 HPR Train to 2 RCS Cold Legs[144]	1 AFW Train to 2 Intact SGs[145] or [2 PORVs and 1 SI Train or 1 PORV and 1 CCP Train to 2 RCS Cold Legs]	1 AFW Train to 2 Intact SGs or 1 RHR Train or 1 HPR Train to 2 RCS Cold Legs	

[143] As an SGTR event tree modeling simplification, the potential for RCS cooldown and depressurization to allow for LPI (given the failure of HPI and isolation of the faulted SG) is not credited in the L3PRA Project Level 1 model. The applicable SGTR sequence (sequence 18 in Figure 3-21) contributes approximately 6 percent of the total SGTR CDF (and less than 0.1 percent to the total CDF for internal events).

[144] Recirculation during SGTR is only possible if feed and bleed cooling was initiated. In addition, HPI can be used by itself if the RWST is successfully refilled.

[145] For SGTRs, the faulted SG is assumed to be unavailable for decay heat removal.

Table 4-1 L3PRA Project Level 1 Model General Success Criteria (cont.)

Initiator	Inventory Control		Decay Heat Removal		Notes
	Injection Phase	Recirculation Phase	Early	Late	
MLOCA	2 HPI Trains or 1 LPI Train to 2 Intact RCS Cold Legs	1 HPR Train or 1 LPR Train to 2 Intact RCS Cold Legs	2 HPI Trains to 2 Intact RCS Cold Legs	1 HPR Train or 1 LPR Train to 2 Intact RCS Cold Legs	For LPI to provide inventory control in the injection phase, the operators must successfully perform a secondary-side cooldown and depressurization. In addition, at least three accumulators must provide initial inventory makeup to the RCS.
LLOCA	1 LPI Train to 2 Intact RCS Cold Legs and 3 Accumulators to Intact RCS Cold Legs	1 LPR Train to 2 Intact RCS Cold Legs.[146]	1 LPI Train to 2 Intact RCS Cold Legs and 3 Accumulators to Intact RCS Cold Legs	1 LPR Train to 2 Intact RCS Cold Legs	

[146] Hot leg recirculation is also required.

5 FAULT TREES

This section presents the information on the key systems and their associated fault tree models required to support the event trees presented in Section 3.[147]

Section 5.1 and Section 5.2 provide brief system or function descriptions of top event fault trees and key support systems, respectively. Additional information provided in these sections includes:

- Identification of which event trees use the applicable fault trees
- Support systems required for system or function operation (if applicable)
- Associated support system initiating event (SSIE) fault tree modeling (if applicable)
- Identification of additional fault trees associated with the system/function (if applicable)

Table 5-1 provides a system dependency matrix, while Table 5-2 summarizes the system or function success criteria for top event fault trees.

5.1 Top Event Fault Tree Models

The fault tree model descriptions that follow are for the top events on the event trees described in Section 3 of this report. The top events on the event trees describe the general functions or system demands required to mitigate the initiating event. In some event trees [e.g., small loss-of-coolant accident (SLOCA), station blackout (SBO)], the logic for functions or system demands must be modified from the general case to reflect the impact of the initiating event or of other events occurring in a given sequence. The required modifications sometimes involve changes in success criteria, changes in support system requirements, or changes in a specific basic event probability (e.g., a human error probability for a specific function may differ depending on the sequence). To reduce the number of distinct fault trees that had to be developed, in many cases the specialized fault tree conditions were addressed using features of the SAPHIRE code that allow manipulation of (i.e., changes to) the fault tree logic based on specific conditions associated with a given initiating event or other events occurring in a given sequence. The following fault tree descriptions focus on the event tree top event but include a brief reference to any fault tree variations (i.e., modified fault trees needed for different initiating events or specific accident sequences).

5.1.1 Accumulator Injection (ACC-M&LLOCA)

Description. The accumulators provide a means for the passive injection of borated water into the reactor vessel to preserve fuel integrity in the event of a loss-of-coolant accident (LOCA). Each of the four accumulators discharges through a separate line into a cold leg of the reactor coolant system (RCS). Each discharge line contains two check valves and one motor-operated valves (MOV) that is normally open with power removed at the motor control center (MCC). Each MOV receives a confirmatory safety injection (SI) signal to open. Each accumulator

[147] Key systems (as defined in this section) are those that either lead to an initiating event or are top events in an event tree.

contains borated water and is pressurized with a nitrogen blanket. The nitrogen pressure is used to propel the accumulator contents into the cold leg when RCS pressure drops below the accumulator pressure [approximately 650 pounds per square inch (psi)].

Success implies that 3 of 3 accumulators inject their entire volume of water into the intact RCS cold legs during a medium loss-of-coolant accident (MLOCA) or large loss-of-coolant accident (LLOCA). It is assumed that for MLOCAs and LLOCAs, the RCS loop with the break cannot be used for either emergency core cooling system (ECCS) injection/recirculation or accumulator injection. For SLOCA initiating events, 2 of 3 accumulators need to inject into intact loops.[148] For cooldown and depressurization to reach a 72-hour safe/stable end-state when charging fails with elevated reactor coolant pump (RCP) seal leakage (21 gpm per RCP), 2 of 4 accumulators are needed.

ACC-M&LLOCA Fault Tree Use. This top event fault tree is used in the event trees involving the MLOCA and LLOCA event trees.

Additional System Fault Trees. The following fault tree for accumulator injection is also used in the L3PRA project Level 1 model.

5.1.1.1 Accumulators Fail to Inject during SLOCA or for 72-Hour Safe/Stable End-state (ACC)

Description. The success criterion for a SLOCA or for a 72-hour safe/stable end-state requires only two accumulators as compared to the requirement of three accumulators for a MLOCA and LLOCA. If the RCP seals are leaking at the assumed rate of 21 gpm per RCP due to lack of seal injection, core damage prior to 72 hours can occur if a source of inventory makeup to the RCS is not provided. If alternate charging fails, operators will eventually be directed by critical safety function status tree (CSFST) procedures to depressurize the steam generators (SGs) to 200 psi using the turbine bypass valves (TBVs) or the SG atmospheric relief valves (ARVs). This depressurization will allow the accumulators to inject into the RCS, thus providing makeup and preventing core damage within 72 hours.

ACC Fault Tree Use. This top event fault tree is used in the SLOCA, consequential SLOCA, and SBO-1, and most transient event trees.[149]

5.1.2 Auxiliary Feedwater System (AFW and AFW-LOCA)[150]

Description. The auxiliary feedwater (AFW) system is designed to supply feedwater from the condensate storage tanks (CSTs) to the SGs whenever the reactor coolant temperature is above 350°F and the main feedwater (MFW) system is not in operation (i.e., during startup, cooldown, or emergency conditions resulting in a loss of MFW).

The AFW system automatically provides feedwater for the removal of reactor core decay heat following a loss of MFW. Main feedwater may be lost due to a loss of offsite AC power, or a secondary-side piping or component failure. The AFW system prevents damage to the reactor core until the reactor coolant temperature is brought from a condition of full power to the

---

[148] For consequential SLOCAs due to either RCP seal failures or stuck open pressurizer relief valves, all four RCS loops are considered intact for all ECCS injection and recirculation functions.

[149] The ACC fault tree is not a top event in the transient event trees but is rather part of the SAFE/STABLE top event.

[150] The AFW and AFW-LOCA fault tree versions are identical.

condition at which the residual heat removal (RHR) system can be placed in operation. The AFW system supplies feedwater to the SGs at a flow rate sufficient to support normal low power transients such as startup, cooldown, and hot standby.

Each unit has two train-oriented motor-driven AFW pumps and one turbine-driven AFW pump that take suction from one of the two CSTs per unit. Either CST 1 or CST 2 can be used, but the pumps are normally aligned to CST 1 and only one CST is in service at a given time. Each motor-driven auxiliary feedwater pump is sized to supply the feedwater flow required for removal of 100 percent of the decay heat from the reactor. The turbine-driven pump is sized to supply up to twice the capacity of a motor-driven pump. The nominal success criteria for the AFW system is 1 of 2 motor-driven AFW pumps or the turbine-driven AFW pump delivers flow to at least 2 of 4 SGs that is adequate to remove decay heat. Steam removal from the SGs fed with AFW is required by either: (1) three TBVs or (2) an ARV or 1 of 5 safety relief valves (SRVs) for 2 of 4 SGs.[151]

The two motor-driven AFW pumps are automatically started by the reactor protection system (RPS), engineered safety features actuation system (ESFAS), anticipated transient without scram (ATWS) mitigation system actuation circuitry (AMSAC), or MFW upon receipt of the following signals:

- Two of four low-low level signals from any one SG (RPS)
- Any SI signal (ESFAS)
- Any loss of, or degraded, safety-related 4.16 kilovolt (kV) AC bus voltage signal (ESFAS)
- An AMSAC signal
- A signal resulting from the trip of both MFW pumps[152]

The two motor-driven pumps can also be started from the main control board and the remote shutdown panels.

The turbine-driven pump is automatically started by the RPS, ESFAS, or AMSAC upon receipt of the following signals:

- Two of four low-low level signals from any two SGs (RPS)
- Any loss of, or degraded, safety-related 4.16 kV AC bus voltage signal (ESFAS)
- An AMSAC signal

[151] For SLOCA and steam generator tube rupture (SGTR) initiating events, the success criterion for AFW flow and steam removal is 2 of 3 intact SGs.

[152] Due to the negligible effect on the results, this start signal was not included in the L3PRA Project Level 1 model.

The turbine-driven pump can also be started and controlled from the main control board and the remote turbine-driven pump AFW panel.[153] In addition, the motor operated valves in the steam supply line to the turbine can be operated from the main control board and the remote turbine-driven pump AFW panel.

AFW Fault Tree Use. This top event fault tree is used in most transient-type event trees.

Required Support Systems. The following support systems are required for successful operation of the AFW system:

- The AFW system is dependent upon the electric power system for the operation of the motor-driven pumps, the motor-operated valves, for instrument power for equipment control, and for monitoring and indication of system parameters. AC power is required for the motor-driven pumps and their associated suction and discharge valves. Each motor-driven pump and its associated motor-operated discharge valve are powered from the corresponding diesel generator. DC power is required for the motor-driven pump start control circuitry, the turbine-driven pump steam supply motor operated valves, and the turbine-driven pump discharge valves to each SG.

- The main steam system provides steam from the SG 1 and 2 steam lines to the turbine of the turbine-driven pump. The turbine can perform its intended function for steam inlet pressures ranging from 90 to 1130 psi.

- The AFW pumps are in separate rooms in the AFW pump house. The turbine-driven pump room is cooled by natural circulation with outside air for emergency conditions. The operation of the turbine-driven pump actuates a signal to open the engineered safety feature (ESF) damper allowing ventilation by natural circulation. However, the turbine-driven AFW pump does not need room heating, ventilating and air conditioning (HVAC) (including the opening of the ESF pneumatically operated damper) for its operation for at least 24 hours. Thus, the loss of turbine-driven AFW pump room cooling is not modeled in the L3PRA project Level 1 model. The motor-driven AFW pump rooms are cooled by outside air using a fan and a damper in each room. These are part of the ESF system. Based on room heat-up analysis, the motor-driven AFW pump rooms would not reach a temperature in 24 hours without room cooling that would result in failure of the pumps. Thus, the loss of motor-driven AFW room cooling is not modeled in the L3PRA project Level 1 model.

- The SG ARVs require 480 volt (V) AC supply power and 125 V DC control power to open.[154] The TBVs require 125 V DC control power and instrument air to open. In addition, the condenser heat sink must be available for the TBVs to be operable.

Additional System Fault Trees. The following fault trees for the AFW system are also used in the L3PRA project Level 1 model.

---

[153] The turbine-driven AFW pump can also be operated locally if DC power is unavailable; however, local operation is only credited in the Level 2 portion of the L3PRA Project model.

[154] The SG ARVs can also be operated using local manual operators. However, due to the negligible effect on results, this manual operation is not credited for cooldown and depressurization during non-SBO scenarios in the L3PRA Project Level 1 model.

5.1.2.1 Auxiliary Feedwater during ATWS (AFW-ATWS)

Description. During an ATWS and if negative reactivity insertion fails, the AFW success criteria changes to all three AFW pumps to deliver flow to all four SGs. In addition, steam removal from the SGs fed with AFW is required by either: (1) three TBVs or (2) an ARV or 1 of 5 SRVs for all four SGs.

AFW-ATWS Fault Tree Use. This top event fault tree is used in the ATWS event tree.

5.1.2.2 Auxiliary Feedwater during SBO (AFW-B)

Description. The AFW-B fault tree credits only the turbine-driven pump.

AFW-B Fault Tree Use. This top event fault tree is used in the SBO event tree.

5.1.2.3 Auxiliary Feedwater after AC Power Recovery during SBO (AFW-ACR and AFW-LOCA-ACR)

Description. This fault tree is a specialization of the AFW fault tree that is used following restoration of AC power from an SBO. It features an operator action (OA-ORS-------H) for failing to make the necessary restorations. The AC power support logic is specialized for conditions following successful AC power restoration.

AFW-ACR Fault Tree Use. This top event fault tree is used in the SBO event tree.

5.1.3 Binding-Popping Failures of RCP Seals (BP1 and BP2)

Description. If RCP seal injection and cooling fail, the RCP seals can potentially fail. One of the RCP seal failure mechanisms is the binding and popping of the seal. Based on the Westinghouse Owner's Group (WOG) 2000 RCP seal leakage model (Westinghouse, 2002), the stage 2 seal has a 20 percent chance of failing, while the stage 1 seal has 1.25 percent chance of failing.[155]

BP1 and BP2 Fault Trees Use. These top event fault trees are used in the SBO event tree.

Additional System Fault Trees. The following fault tree for the binding/popping failure of RCP seals is also used in the L3PRA project Level 1 model.

5.1.3.1 Binding/Popping Failure of RCP Seals – LOACCW (RCPS-BP)

Description. This fault tree represents the binding popping failure of either the stage 1 or stage 2 seals given a loss of auxiliary component cooling water (ACCW) or loss of nuclear service cooling water (NSCW) initiating event. Since the loss of ACCW initiating event causes the loss of RCP seal cooling via the thermal barrier heat exchangers, if RCP seal injection is lost, the

[155] These failure probabilities specified are per RCP. However, the WOG 2000 RCP seal leakage model (Westinghouse, 2002) assumes that all RCPs for the affected unit experience the same leakage scenario (i.e., given a failure in one RCP, the conditional common-cause failure (CCF) probability for the remaining pumps is 1.0).

integrity of the seals will be challenged. This fault tree also includes the operator action (RCS-XHE-XM-TRIP-LONSCW) to trip the RCPs (which does not apply for a SBO).[156]

RCP-BP Fault Tree Use. This top event fault tree is used in the LOACCW event tree.

5.1.4 Cooldown and Depressurization

Description. During a MLOCA, SLOCA (including SGTR) or consequential SLOCA (due to RCP seal failure or stuck-open PORV or SRV), operators can initiate secondary-side cooldown and depressurization to allow for the initiation of the shutdown cooling mode of RHR or low-pressure injection (LPI), given a failure of high-pressure injection (HPI). Success requires opening at least two SG ARVs to start the cooldown of the secondary side to use the RHR pumps.

Required Support Systems. The following support systems are required for successful cooldown and depressurization:

- The SG ARVs require 480 V AC supply power and 125 V DC control power to open.

Associated Fault Trees. The following fault trees for cooldown and depressurization are used in the L3PRA project Level 1 model.

5.1.4.1 Cooldown and Depressurization during MLOCA (CAD-MLOCA)

Description. This fault tree represents cooldown and depressurization given a MLOCA. During a MLOCA with the failure of HPI, operators will be directed by FR-C.1/C.2 to depressurize the SGs with the ARVs for 2 of 4 SGs. This depressurization will allow the accumulators to inject into the RCS, thus providing makeup until RCS pressure decreases below the shutoff head of the RHR pumps. Operator action (OAD_MLA------H) is required to initiate the depressurization of the SGs by opening the ARVs.

CAD-MLOCA Fault Tree Use. This top event fault tree is used in the MLOCA event tree.

5.1.4.2 Cooldown and Depressurization during SLOCA with successful HPI (CAD-ES12)

Description. This fault tree represents cooldown and depressurization given a SLOCA with successful HPI. During a SLOCA with successful HPI, operators will be directed by ES-1.2 to depressurize the SGs with the ARVs for 2 of 4 SGs. This depressurization will allow the accumulators to inject into the RCS, thus providing makeup until RCS pressure decreases below the shutoff head of the RHR pumps. Operator action (OAC_NC-------H) is required to initiate the depressurization of the SGs by opening the ARVs.

CAD-ES12 Fault Tree Use. This top event fault tree is used in the SLOCA and consequential SLOCA event trees.

5.1.4.3 Cooldown and Depressurization during SLOCA with HPI failed (CAD-FRC1)

Description. This fault tree represents cooldown and depressurization given a SLOCA with HPI failed. During a SLOCA and the failure of HPI, operators will be directed by FR-C.1/C.2 to

---

[156] The WOG 2000 RCP seal leakage models assumes that both stages of RCP seals will fail if the RCPs are not tripped when both RCP seal injection and cooling are lost.

depressurize the SGs with the ARVs for 2 of 4 SGs. This depressurization will allow the accumulators to inject into the RCS, thus providing makeup until RCS pressure decreases below the shutoff head of the RHR pumps. Operator action (OAC_AC-------H) is required to initiate the depressurization of the SGs by opening the ARVs.

CAD-FRC1 Fault Tree Use. This substitution fault tree is used in the SLOCA and consequential SLOCA event trees.

5.1.4.4 Cooldown and Depressurization (ES-1.2) after AC Power Recovery during SBO (CAD-ES12-ACR)

Description. This fault tree is a specialization of the CAD-ES12 fault tree that is used following AC power recovery from a SBO. The AC power support logic is specialized for conditions following successful AC power restoration.

CAD-ES12-ACR Fault Tree Use. This top event fault tree is used in the SBO-1 event tree.

5.1.4.5 Cooldown and Depressurization (FR-C.1/C.2) after AC Power Recovery during SBO (CAD-FRC1-ACR)

Description. This fault tree is a specialization of the CAD-FRC1 fault tree that is used following AC power recovery from a SBO. The AC power support logic is specialized for conditions following successful AC power restoration.

CAD-FRC1-ACR Fault Tree Use. This substitution fault tree is used in the SBO-1 event tree.

5.1.4.6 Cooldown and Depressurization during SGTR – Early (CAD-SGTR-EARLY)

Description. This fault tree represents the cooldown and depressurization of the RCS to stop primary-to-secondary leakage during a SGTR. Operator action (OAD_SGR------H) is required to use the TBVs or the ARVs for 2 of 3 intact SGs to depressurize the RCS to a pressure less than that of the ruptured SG to prevent overfilling. The E-3 procedure also directs operators to use pressurizer sprays or PORVs to restore pressurizer level. In addition, operators must terminate SI, align normal charging, and establish letdown to stop the primary-to-secondary leakage.

CAD-SGTR-EARLY Fault Tree Use. This top event fault tree is used in the SGTR event tree.

5.1.4.7 Cooldown and Depressurization during SGTR – Late (CAD-SGTR-LATE)

Description. This fault tree represents the depressurization via the SGs to decrease RCS pressure to allow for the shutdown cooling mode of RHR to be initiated. If the ruptured SG is isolated and primary-to-secondary leakage has been stopped, operators will transition from E-3 to ES-3.1 or ES-3.3, which will direct operators to cooldown and depressurize the RCS by dumping steam using the TBVs or ARVs for 2 of 3 intact SGs (CAD-XHE-SGTR--LT).

CAD-SGTR-LATE Fault Tree Use. This top event fault tree is used in the SGTR event tree.

5.1.5 Charging (CHG)

Description. If RCP seal injection via the normal charging pump (NCP) is lost, but either seal cooling to the thermal barrier heat exchangers or RCP seal integrity is maintained, seal leakage

is assumed to increase from its nominal leak rate to 21 gpm per RCP.[157] At this leakage rate, core damage could occur prior to 72 hours unless other mitigation (in addition to long-term decay heat removal) is successful. Even though there is insufficient time available for operators to align the centrifugal charging pumps (CCPs) to provide alternate RCP seal injection for most transient initiating events, operators are procedurally directed to align a CCP to provide alternate charging to the RCS (as represented by HFE CHG-XHE-NORMAL). If charging is successful, core damage will not occur prior to 72 hours.

CHG Fault Tree Use. This top event fault tree is used in most transient event trees.

Required Support Systems. The same support systems required for CCPs (HPI) are needed for charging; see Section 5.1.12 for further information.

Additional System Fault Trees. The following fault tree for charging is also used in the L3PRA project Level 1 model.

5.1.5.1 Charging after AC Power Recovery from a SBO (CHG-ACR)

Description. This fault tree is a specialization of the CHG fault tree that is used following AC power recovery from a SBO. The AC power support logic is specialized for conditions following successful AC power restoration.

CHG-ACR Fault Tree Use. This top event fault tree is used in the SBO event tree.

5.1.6 Condensate Storage Tank Refill (CSTR)

Description. CST inventory makeup is required for scenarios in which the in-service CST inventory would be depleted within the PRA mission time of 24 hours (e.g., given a SGTR) and where CST makeup is needed for 72 hours to reach a safe/stable end sate (i.e., scenarios with elevated RCP seal leakage). Upon depletion of the in-service CST, the alternate CST can be manually aligned to the suction of the pumps (OA-ALTAFW----H). Each AFW pump has a suction line from each CST. An additional source of water is available from the demineralized water tank, which is automatically used for makeup to the CSTs, if available. Automatic makeup from the demineralized water system requires instrument air to open the supply valve.[158, 159]

CSTR Fault Tree Use. This top event fault tree is used in the SGTR event tree and the SAFE/STABLE fault trees.

Required Support Systems. The following support systems are needed to provide additional water for AFW:

- Automatic makeup from demineralized water system requires instrument air to open the supply valve.

---

[157] This assumption is conservative for scenarios with successful RCP seal cooling (via ACCW through the thermal barrier heat exchangers).

[158] Fault tree modeling of automatic CST makeup represented using an undeveloped basic event. Instrument air dependency was included in the model.

[159] The fire water system could also be connected to the CSTs to refill them; however, it was not credited in the model as an AFW source (for simplicity).

- Manual alignment of the second CST requires DC power (i.e., opening the motor-operated valves that connect to the pump suction paths).

5.1.7 Emergency Power System (EPS)

Description. After a loss of offsite power (LOOP), the emergency diesel generators (EDGs) start and supply power for the mitigating systems. If at least one AC emergency bus is energized with an EDG supplying power, the event progression would be like a transient. If both EDGs fail to start or run after a LOOP event, an SBO occurs.

The EDGs provide standby onsite power required by the safety-related AC power systems in the event of a loss of preferred power sources, for powering the essential loads necessary to safely shut down the reactor under any operating and accident condition.

The system has two independent trains for each unit. Each train has an EDG connected exclusively to a single safety-related 4.16 kV AC bus of a load group. Each safety-related 4.16 kV AC bus has similar safety-related equipment on it. One bus is adequate to satisfy minimum ESF demands caused by a LOCA and a simultaneous loss of offsite power supply. Power and control cables for the EDGs and associated switchgear are routed to maintain physical separation.

The EDG fuel oil storage and transfer system is used to transfer diesel fuel oil from the DG fuel oil storage tank using pumps to replenish the EDG day tank as fuel oil is being consumed. The EDG fuel oil day tanks each contain enough fuel to provide approximately 2.6 hours of operation for its associated diesel engine at the maximum operating load without resupply from an EDG fuel oil storage tank. The design of the diesel fuel oil storage system allows replenishment of fuel oil without interrupting operation of the EDG. Should continuous operation of the generator for more than 7 days be required, it will be necessary to refill the diesel fuel oil storage tank. A fuel oil transfer pump is automatically started and stopped by a day tank level switch. The second pump is started automatically in the event of low discharge pressure from the lead pump or day tank low-low level. Should a pump be run continuously or fail to stop, any overflow is returned to the storage tank via the recirculation line.

The EDG building ESF HVAC system is required for EDG operation. Each EDG has two fans along with their associated dampers. Failures of both fans (or their associated dampers) will cause the EDG to fail.

EPS Fault Tree Use. This top event fault tree is used in the LOOP event trees.

Required Support Systems. The NSCW provides cooling water for the EDG jacket water cooling system, which also removes heat from the lube oil system.

5.1.8 Feed and Bleed (FAB)

Description. The feed and bleed mode of reactor cooling is needed if AFW and MFW are unavailable and requires successful HPI to provide flow to the RCS cold legs and opening of the PORV(s) to remove RCS decay heat. Operators must initiate feed and bleed cooling by manually initiating an SI signal (if an automatic SI actuation has not already been generated). After initiation of the SI signal, the operator will then open the PORV(s). In addition, operators

must trip all the RCPs before initiating feed and bleed. These operator actions are accounted for in the HFE OAB_TR-------H.[160]

The success criteria for feed and bleed cooling change depending on the type of initiating event. If a transient-type initiating event occurs, successful feed and bleed requires 1 of 2 CCPs and 1 of 2 PORVs. However, if an initiating event involves a SLOCA, successful feed and bleed cooling can also be provided by 1 of 2 SI pumps and both PORVs.

FAB Fault Tree Use. This top event fault tree is used in most transient event trees and the secondary-side break (SSB) event trees (including consequential SSB).

Required Support Systems. The same support systems required for HPI and operation of the PORVs are needed for feed and bleed; see Section 5.1.12 and Section 5.1.32 for additional information.

Additional System Fault Trees. The following fault trees for feed and bleed cooling are also used in the L3PRA project Level 1 model.

5.1.8.1 Feed and Bleed during SLOCA (FAB-SLOCA)

Description. This fault tree is a SLOCA specialization of the FAB fault tree that changes the success criterion to allow 1 of 2 SI pumps and both PORVs (in addition to 1 of 2 CCPs and 1 of 2 PORVs) to provide feed and bleed cooling. In addition, the operator action (OAB_SI-------H) for initiation of feed and bleed is conditioned on the presence of an SI signal.

FAB-SLOCA Fault Tree Use. This top event fault tree is used in the SLOCA, consequential SLOCA, and SGTR event trees.

5.1.8.2 Feed and Bleed after AC Power Recovery from an SBO (FAB-ACR)

Description. This fault tree is a specialization of the FAB fault tree that is used following AC power recovery from an SBO. It features an operator action (OA-ORS-------H) for failing to make the necessary restorations. In addition, the operator action (OAB-SBOACR---H) for initiating feed and bleed cooling is conditioned on AC power recovery after an SBO. The AC power support logic is specialized for conditions following successful AC power restoration.

FAB-ACR Fault Tree Use. This top event fault tree is used in the SBO event tree.

5.1.8.3 Feed and Bleed during a SLOCA after AC Power Recovery from an SBO (FAB-SLOCA-ACR)

Description. This fault tree is a specialization of the FAB-SLOCA fault tree that is used to represent feed and bleed cooling during a consequential SLOCA following AC power recovery

---

[160] If the failure of AFW is due to the long-term loss of makeup inventory due to the failure of manual alignment of AFW to the second CST or automatic makeup from the demineralized water system, more time is available to operators to initiate feed and bleed. For these cases a new HFE OAB_TR-------H-LT was created and inserted via post-processing rules for the dominant contributor to failure of long-term AFW inventory (OA-ALTAFW----H). Because detailed calculations were not available to determine reliable time estimates, only the additional time for recovery credit was used to modify the human error probability (HEP) for this new HFE (as compared to OAB_TR------H). See Section 6.5.5 for additional information.

from an SBO. Besides the change in pump and PORV success criteria (as discussed in Section 5.1.8.1), it also features an operator action (OA-ORS-------H) for failing to make the necessary restorations after the recovery of AC power. In addition, the operator action (OAB-SBOACR---H) for initiating feed and bleed cooling is conditioned on AC power recovery after a SBO.[161] The AC power support logic is specialized for conditions following successful AC power restoration.

FAB-SLOCA-ACR Fault Tree Use. This top event fault tree is used in the SBO-1 event tree.

5.1.9 Feed and Bleed Recirculation (FABR)

Description. If the feed and bleed mode of reactor cooling is successfully initiated and the RWST contents have been reduced to the low-low level alarm set-point, the suction of the HPI pumps (SI pumps or CCPs) must be switched to the containment sump.[162] One of two RHR pumps is required to supply the fluid suction head to the HPI pumps. The change from the injection phase to the cold leg recirculation phase of feed and bleed cooling is a manual/automatic process. When the water in the RWST reaches the low-low level alarm set-point, the two RHR sump isolation valves automatically open and the RHR pumps and HPI pumps are sequentially shifted to the cold leg recirculation phase of operation. Operators are required to manually (OAR_LTFB-TRA-H if CCUs are available or OAR_LTFB-TRB-H if CCUs are not available) align the RHR pump discharge to the suction of the SI pumps or CCPs and isolate RWST from all three sets of pumps.[163] The heat sink for the recirculation water is provided by either CCW to one of two RHR heat exchangers (associated with a running RHR pump) or by 4 of 8 CCUs.

FABR Fault Tree Use. This top event fault tree is used in most transient event trees and the SSB event trees (including consequential SSB).

Required Support Systems. The same support systems required for HPR are needed for feed and bleed recirculation; see Section 5.1.13 for additional information.[164]

Additional System Fault Trees. The following fault trees for the feed and bleed recirculation are also used in the L3PRA project Level 1 model.

5.1.9.1 Feed and Bleed Recirculation during an SLOCA (FABR-SLOCA)

Description. This fault tree is an SLOCA specialization of the FABR fault tree that changes the success criterion to allow 1 of 2 SI pumps (as an alternative to 1 of 2 CCPs) to provide feed and

---

[161] As a modeling simplification, a new HFE to cover initiation of feed and bleed cooling given AC power recovery after an SBO during a consequential SLOCA was not created. Instead, the HFE (OAB-SBOACR---H) for initiation of feed and bleed cooling given AC power recovery after an SBO (with no consequential SLOCA), is used. This HFE has a more limiting (higher) HEP than the HFE for initiation of feed and bleed cooling conditioned on the presence of an SI signal.

[162] The pump success criterion for feed and bleed recirculation is assumed to be the same as the pump success criterion for feed and bleed in the injection mode. This is potentially conservative because no credit is given for the SI pumps for feed and bleed in the injection mode, while it is possible that an SI pump may provide adequate flow in the recirculation mode.

[163] If at least 3 of 8 CCUs are available, containment spray is assumed to not actuate resulting in more time before the RWST reaches its low-low level alarm set-point.

[164] Note that PORVs are required for feed and bleed recirculation; however, the PORV fault tree logic is not included in the FABR fault trees because it is already included in the FAB fault trees.

bleed recirculation. In addition, the operator action (OAR_LTFB-SLA-H if CCUs are available or OAR_LTFB-SLB-H if CCUs are not available) for alignment of feed and bleed recirculation is conditioned given a SLOCA has occurred.

FABR-SLOCA Fault Tree Use. This top event/substitution fault tree is used in the SLOCA, consequential SLOCA, and SGTR event trees.

5.1.9.2 Feed and Bleed Recirculation after AC Power Recovery from an SBO (FABR-ACR)

Description. This fault tree is a specialization of the FABR fault tree that is used following AC power recover from an SBO. The operator action (OA-LTFB-ACRA-H if CCUs are available or OA-LTFB-ACRB-H if CCUs are not available) for alignment of feed and bleed recirculation is conditioned given AC power recovery after a SBO. In addition, the AC power support logic is specialized for conditions following successful AC power restoration.

FABR-ACR Fault Tree Use. This top event fault tree is used in the SBO event tree.

5.1.9.3 Feed and Bleed Recirculation during a SLOCA after AC Power Recovery from an SBO (FABR-SLOCA-ACR)

Description. This fault tree is a specialization of the FABR-SLOCA fault tree that is used to represent feed and bleed recirculation during a consequential SLOCA following AC power recovery from an SBO. This fault tree is an SLOCA specialization of the FABR fault tree that changes the success criterion to allow 1 of 2 SI pumps (as an alternative to 1 of 2 CCPs) to provide feed and bleed recirculation. In addition, the operator action (OA-LTFB-ACRA-H if CCUs are available or OA-LTFB-ACRB-H if CCUs are not available) for alignment of feed and bleed recirculation is conditioned given AC power recovery after an SBO.[165] The AC power support logic is specialized for conditions following successful AC power restoration.

FABR-SLOCA-ACR Fault Tree Use. This substitution fault tree is used in the SBO-1 event tree.

5.1.10 Feedwater (FW)

Description. The FW fault tree is composed of both AFW and MFW fault trees. The description of the AFW system and fault tree logic is described in Section 5.1.2. The MFW feedwater system consists of two turbine-driven MFW pumps, feedwater regulating valves, feedwater isolation valves, piping, and other supporting instrumentation. The system receives condensate from the condensate system and pumps the water to the SGs. It also provides additional preheating of the water and regulates feedwater flow to the SGs.

Two identical turbine-driven MFW pumps are provided for normal plant operation. Each pump is designed to provide 50 percent of required MFW flow. From the MFW pump, the MFW flows either through the main feed pump recirculation valves or to the MFW pump discharge isolation valves. Feedwater flow to each SG is automatically controlled by the feedwater regulating valve (or its associated feedwater regulating valve bypass valve). The bypass valve is used during

[165] As a modeling simplification, a new HFE to cover feed and bleed recirculation given AC power recovery after an SBO during a consequential SLOCA was not created. Instead, the HFEs (OA-LTFB-ACRA-H and OA-LTFB-ACRB-H) for feed and bleed recirculation given AC power recovery after an SBO (with no consequential SLOCA), are used. This modeling simplification has a negligible impact on the results.

plant startup and up to approximately 15 percent power; the feedwater regulating valve is used above this power level.

MFW is automatically isolated on a low T_{avg} signal following a reactor trip by closing the MFW isolation valves, the bypass feedwater isolation valves, and the feedwater regulating and bypass valves. If AFW fails, operators are instructed (via the loss of secondary heat sink emergency operating procedure) to restart MFW with the corresponding valve alignments. Operators must re-establish MFW flow to at least one SG from 1 of 2 MFW pumps (at least one condensate pump must be running to provide suction to the MFW pumps). Steam removal from the SGs fed with MFW is required by either: (1) three TBVs or (2) an ARV or 1 of 5 SRVs for 2 of 4 SGs.

FW Fault Tree Use. This top event fault tree is used in the reactor trip, turbine trip, other transients, loss of ACCW, loss of NSCW, loss of RCP seal injection, and loss of two safety-related 120 V AC panel event trees.

Required Support Systems. The following support systems are required for successful operation of the MFW:

- The plant electrical power systems are required for the operation of MFW. AC power is required for turbine lube oil system pumps, while DC power is required for steam supply valves and the emergency oil pump.

- The turbine plant cooling water (TPCW) system provides cooling water to the lube oil cooler.

5.1.11 Hot Leg Recirculation (HLR)

Description. Hot leg recirculation prevents flow path blockage within the reactor vessel due to boron precipitation and is initiated following cold leg recirculation during a LLOCA. The success of hot leg recirculation requires 1 of 2 RHR pumps to inject to hot leg 1 or hot leg 4. The RHR trains remain lined up to the containment recirculation sump through their respective sump suction valves. Orifices in each hot leg branch limit pump run out. Operator action (OAL_LPLL-----H) is required to establish low-pressure hot leg recirculation.

HLR Fault Tree Use. This top event fault tree is used in the LLOCA event tree.

Required Support Systems. The same support systems required for low-pressure recirculation (LPR) are needed for hot leg recirculation; see Section 5.1.28 for further information.

5.1.12 High-Pressure Injection (HPI)

Description. The high-pressure injection function essentially combines two separate systems: the charging system (two CCPs) and SI system (two SI pumps). When an SI signal is generated, all four pumps start and take suction from the RWST and provide flow to the RCS cold legs. An SI signal is generated by any of the following conditions:

- High containment pressure

- Low pressurizer pressure

- Low pressure in any main steam line

- Manual SI actuation

The two motor-driven CCPs are mechanically arranged in parallel flow paths. The CCPs are normally aligned to receive water from the volume control tank (VCT) through two remotely operated valves installed in series. An SI signal will close these valves and open two parallel valves to align the CCP suction to the RWST for the injection phase of operation. Two valves in parallel are used to isolate the high-pressure injection common discharge header during normal plant conditions. These normally closed valves receive an SI signal to open, thereby aligning the CCP discharge to the RCS cold legs. Simultaneously, the normal charging flow discharge valves are closed by the SI signal, thereby assuring injection flow to the cold legs.

Associated with the CCPs are minimum flow recirculation lines to the seal water heat exchanger and back to the pumps' suction manifold. These minimum flow lines are provided to prevent pump deadheading and to permit pump testing during power operations. Each minimum flow bypass line contains an isolation valve that closes automatically upon receipt of an SI signal. A third isolation valve is provided in the common header downstream of the two pump minimum flow lines. These are referred to as the normal minimum flow lines. An alternate minimum flow line is provided for each pump to prevent pump deadheading should RCS pressure rise following isolation of the normal minimum flow lines. An isolation valve in each of these lines opens upon receipt of an SI signal. Each of these alternate minimum flow lines contains a relief valve, with flow being discharged to the RWST.

There are two motor-driven SI pumps that provide intermediate pressure injection flow to the RCS cold (or hot) legs during accident conditions. These pumps are mechanically arranged in redundant flow paths. Associated with the SI system are isolation valves that must be positioned to initiate injection flow during an accident. The SI pumps are aligned to receive water from the RWST through multiple valves for the injection phase of operation.

Each of the SI pumps uses a minimum flow recirculation line to maintain a sufficient pump flow rate to prevent over-heating during accidents or until RCS pressure is below the shutoff pressure of the pumps. The pump minimum flow recirculation flows through normally open bypass valves and then through an isolation valve back to the RWST.

The nominal success criteria for the HPI fault tree is 1 of 4 SI pumps/CCPs injecting RWST water to any 2 of 4 cold legs for all SLOCAs. The success criteria for MLOCA shifts to 2 of 4 SI pumps/CCPs to 2 of 3 intact cold legs.

HPI Fault Tree Use. This top event fault tree is used in the ATWS event tree and most event trees involving LOCAs (i.e.., SGTR, SLOCA, MLOCA, and consequential SLOCA).[166]

Required Support Systems. The following support systems are required for successful operation of HPI:

- The plant electrical power systems are required for the operation of HPI. AC power is required for motive power to pump motors and for motive and control power to MOV operators, while DC power is required for control power to the pump motors and circuit

[166] High-pressure injection is not modeled in the LLOCA event tree.

breakers. All pumps, valves, and other equipment that are required for cooling of safety-related components are supplied from safety-related buses. These safety-related buses are supplied by emergency power if primary power sources are lost.

- The ESFAS sends start signals to SI pumps, CCPs, and several valves for safety injection. In addition, it starts the CCPs on a loss of power signal.[167]

- NSCW provides cooling water to the CCPs and SI pump motor coolers and lube oil coolers.

- Each pump room is cooled by an auxiliary building room cooler that has essential chilled water supplied to its coil (the CCP coolers also have a normal chilled water system coil). However, room cooling is not required based on a room heat-up analysis.

Additional System Fault Trees. The following fault tree for the HPI system is also used in the L3PRA project Level 1 model.

5.1.12.1 High-Pressure Injection after AC Power Recovery from a SBO (HPI-ACR)

Description. This fault tree is a specialization of the HPI fault tree that is used following AC power recovery from a SBO. The AC power support logic is specialized for conditions following successful AC power restoration.

HPI-ACR Fault Tree Use. This top event fault tree is used in the SBO-1 event tree.

5.1.13 High-Pressure Recirculation (HPR)

Description. When the RWST contents have been reduced to the low-low level alarm set-point either during HPI or feed and bleed, the suction of the HPI pumps (SI pumps or CCPs) must be switched to the containment sump. One of two RHR pumps is required to supply the fluid suction head to the SI pumps or the CCPs. The change from the injection phase to the cold leg recirculation phase is a manual/automatic process. When the water reaches the low-low level alarm point the RHR sump isolation valves automatically open and the RHR pumps, the SI pumps, and the CCPs are sequentially shifted to the cold leg recirculation phase of operation. Operators are required to manually (OAR_HPSLA----H if CCUs are available or OAR_HPSLB----H if CCUs are not available) align the RHR pump discharge to the suction of the SI pumps or CCPs and isolate RWST from all three sets of pumps. The heat sink for the recirculation water is provided by either CCW to one of two RHR heat exchangers (associated with a running RHR pump) or by 4 of 8 CCUs.

HPR Fault Tree Use. This top event fault tree is used in MLOCA, SLOCA, SGTR, and consequential SLOCA event trees.

Required Support Systems. The following support systems are required for successful operation of HPR:

- The plant electrical power systems are required for the operation of HPR. AC power is required for motive power to pump motors and for motive and control power to MOV

[167] If the HPI pumps fail to automatically start during an SI actuation, operators can manually start the pumps.

operators, while DC power is required for control power to the pump motors and circuit breakers. All pumps, valves, and other equipment that are required for cooling of safety related components are supplied from safety-related buses. These safety-related buses are supplied by emergency power if primary power sources are lost.

- The ESFAS sends start signals to all ECCS pumps and several valves for safety injection and starts the CCPs on a loss of power signal. In addition, ESFAS sends the signals to open the RHR sump isolation valves at the RWST low-low level alarm set-point.

- In addition to providing cooling water to the CCPs and SI pump motor coolers and lube oil coolers, NSCW also provides cooling water to the RHR pump motor coolers. The NSCW provides the path to the ultimate heat sink for the ECCS system via the RHR heat exchanger and the CCW system.

- The CCW system cools the shell side of the RHR heat exchangers. In addition, CCW supplies cooling water to the RHR pump seals. However, this dependency is not modeled in the PRA based on manufacturer test results that indicate the seals will remain operable under worst case operating temperature and pressure conditions without CCW cooling to the seals.

- The CCUs provide the ultimate heat sink if CCW to the RHR heat exchangers is not available.

- The RHR pump room is cooled by an auxiliary building room cooler that has essential chilled water supplied to its coil. The RHR pump room coolers also have a normal chilled water system coil. However, room cooling is not required based on a room heat-up analysis.

Additional System Fault Trees. The following fault trees for high-pressure recirculation are also used in the L3PRA project Level 1 model.

5.1.13.1 High-Pressure Recirculation after AC Power Recovery from an SBO (HPR-ACR)

Description. This fault tree is a specialization of the HPR fault tree that is used following AC power recovery from an SBO. The operator action (OA-HPR-ACRA--H if CCUs are available or OA-HPR-ACRB--H if CCUs are not available) for alignment of high-pressure recirculation is conditioned given AC power recovery after an SBO. In addition, the AC power support logic is specialized for conditions following successful AC power restoration.

HPR-ACR Fault Tree Use. This top event fault tree is used in the SBO-1 event tree.

5.1.13.2 High-Pressure Recirculation during an ATWS (HPR-ATWS)

Description. This fault tree is a specialization of the HPR fault tree that is used following an ATWS given a consequential LOCA occurs. The operator action (OAR_HPATA----H if CCUs are available or OAR_HPATB----H if CCUs are not available) for alignment of high-pressure recirculation is conditioned on the occurrence of the ATWS.

HPR-ATWS Fault Tree Use. This top event fault tree is used in the ATWS event tree.

5.1.14 RCP Stage 1 Seals Fail with Integrity of Stage 2 Seals Maintained (IEFT-ISL-RCP-S1LO)

Description. This fault tree is used to develop the RCP seal leak-off return line interfacing-systems loss-of-coolant accident (ISLOCA) frequency based on initiating events (combined with subsequent system failures and unavailabilities) that can lead to the complete failure of RCP seal injection and cooling. The initiating events included in this initiating event fault tree are LOOP with subsequent SBO (as represented by the LOOP initiating events and the EPS fault tree), total loss of NSCW (as represented by the IEFT-LONSCW fault tree), loss of ACCW with the failure to align the CCPs for seal injection (as represented by the IEFT-LOACCW and RCPSI-LOACCW fault trees), and the loss of normal seal injection (i.e., the NCP) with subsequent loss of ACCW flow to the RCP thermal barrier heat exchangers (as represented by the IEFT-LOSINJ fault tree and a sub-fault tree within the RCPSC fault tree representing the subsequent loss of ACCW). In addition, the stage 1 RCP seals (BP1 fault tree) need to fail while the integrity of the stage 2 seals (BP2 fault tree) is maintained for an ISLOCA via this pathway to occur.[168] If the stage 2 RCP seals fail, then a SLOCA inside containment occurs.

IEFT-ISL-RCP-S1LO Fault Tree Use. This fault tree is the SSIE fault tree for the frequency of an ISLOCA from the RCP seal leak-off lines and is used in the ISL-RCP-S1LO event tree.

Required Support Systems. The same support systems required for the EPS (Section 5.1.7), RCPSI-LOACCW (Section 5.1.36), and ACCW (Section 5.2.5) fault trees are needed for this fault tree.

5.1.15 RHR Cold Leg Injection Train A(B) Isolation Integrity (IEFT-ISL-RHR-CLI-A, IEFT-ISL-RHR-CLI-B)

Description. An RHR ISLOCA can occur from one of the four RCS cold leg injection lines if two isolation check valves in series fail. If an ISLOCA occurs in any of these paths, RCS pressure can cause the failure of RHR piping that is not rated to handle this pressure. This SSIE fault tree includes the failure of four primary-side cold leg check valves and the subsequent, dependent failures of the four system-side check valves. In addition, the random (i.e., independent) failure of the system-side check valves is also included. These check valve failure frequencies/probabilities were taken from the ISLOCA expert elicitation discussed previously in Section 3.5. If the ISLOCA occurs from one of the RHR cold-leg injection lines, operators can terminate the ISLOCA by closing an MOV for the applicable cold legs.

IEFT-ISL-RHR-CLI-A(B) Fault Tree Use. This fault tree is the SSIE fault tree for the frequency of an ISLOCA in one of the RHR system cold leg injection lines and is used in the ISL-RHR-CLI-A(B) event trees.

Required Support Systems. AC power is required for motive and control power to MOV operators.

[168] If the operators fail to trip the RCPs given the complete loss of RCP seal injection/cooling, then both stages of RCP seals are assumed to fail resulting in a SLOCA inside containment, and therefore, an ISLOCA would not occur.

5.1.16 RHR Hot Leg Suction Isolation Integrity (IEFT-ISL-RHR-HLS)

Description. An RHR ISLOCA can occur from either of the two RCS hot leg suction lines if the two normally-closed MOVs in series for hot leg 1 or hot leg 4 fail. If an ISLOCA occurs in either of these paths, RCS pressure can cause the failure of RHR piping that is not rated to handle this pressure. This SSIE fault tree includes the failure of the two primary-side hot leg MOVs and the subsequent, dependent failures of the two system-side MOVs. The random (i.e., independent) failure of the system-side MOVs is also included. In addition, transfer (open) failures for both the primary- and system-side MOVs are included; these frequencies/probabilities are from the Reliability and Availability Data System (RADS) calculator.

IEFT-ISL-RHR-HLS Fault Tree Use. This fault tree is the SSIE fault tree for the frequency of an ISLOCA in one of the RHR system hot leg suction lines and is used in the ISL-RHR-HLS event tree.

5.1.17 Loss of RCP Seal Injection (IEFT-LOSINJ)

Description. If the NCP or its associated charging flow control valves, seal injection filters, or suction/discharge isolation valves fail, a loss of seal injection flow to all RCPs occurs. Loss of RCP seal injection flow from the NCP would not directly cause a reactor trip given the availability of ACCW.[169] After verifying ACCW operation, operators are directed to establish safety grade charging using the CCPs. If safety grade charging is established, the plant may continue its operation and no initiating event (reactor trip) would occur. Otherwise, operators would trip the reactor, resulting in a plant transient.

IEFT-LOSINJ Fault Tree Use. This fault tree is the SSIE fault tree for the frequency of a loss of all RCP seal injection and is used in the LOSINJ event tree.

Required Support Systems. The same support systems required for CCPs (HPI) are needed for safety grade charging; see Section 5.1.12 for further information. In addition, the following support systems are also needed for normal charging:

- The NCP is powered by nonsafety-related 4.16 kV AC power.
- The NCP motor coolers require ACCW for adequate pump cooling.

5.1.18 Automatic Closure of RCP Seal Leak-off MOVs Given an SI Actuation (ISL-RCP-S1LO-AUTO)

Description. During an ISLOCA from the RCP seal leak-off lines, the closure of one of two MOVs in series will limit the SLOCA to inside of containment. These valves will close automatically due to a containment isolation signal given an SI actuation. During an SBO, automatic closure of these two MOVs is not possible because 480 V AC power is lost; therefore, operator action (OA-IS-ISLSEALSBO) is required to manually close the MOV that is outside containment.

[169] The loss of ACCW is modeled as a separate initiating event; therefore, the loss of RCP seal injection event tree does not include the loss of seal injection due to the impacts from loss of ACCW.

ISL-RCP-S1LO-AUTO Fault Tree Use. This top event fault tree is used in the ISL-RCP-S1LO event tree.

Required Support Systems. The following support systems are required for successful closure of at least one of the two MOVs in series on the RCP seal leak-off lines:

- 480 V AC power is required for motive and control power to the MOV operators.
- The ESFAS sends signals for the automatic closure of the RCP seal leak-off line MOVs due to a containment isolation signal given an SI actuation.

5.1.19 Operators Fail to Manually Close HV8141A/B/C/D (ISL-RCP-S1LO-HV8141)

Description. During an ISLOCA from the RCP seal leak-off lines, operators can limit the SLOCA to inside containment by manually closing an air-operated valve on each of the four RCP seal leak-off lines. If RCP leakage through the RCP seal leak-off line increases, operators will receive a control room alarm on high flow. Operator action (OA-IS-ISLLKF-H) is required to manually close all four of these valves.

ISL-RCP-S1LO-HV8141 Fault Tree Use. This top event fault tree is used in the ISL-RCP-S1LO event tree.

Required Support Systems. The following support systems are required for successful closure of the air-operated valves on each of the four RCP seal leak-off lines:

- 125 V DC power is required for control power for these valves.
- Instrument air is needed to close these valves.

5.1.20 PSV8121 Protects Piping Integrity (ISL-RCP-S1LO-RPT)

Description. During an ISLOCA from the RCP seal leak-off lines, line pressure will increase above the set-point of the leak-off line relief valve. If the relief valve opens, RCP seal leak-off return piping will not fail; and therefore, the SLOCA will be limited to inside of containment. The relief valve is common to all RCPs and when opened directs its flow to the pressure relief tank. Analysis has shown that this relief valve can relieve the pressure of stage 1 RCP seal failures of all four RCPs. If this relief valve fails to open, RCP seal leak-off return piping (both inside and outside containment) will be pressurized.

ISL-RCP-S1LO-RPT Fault Tree Use. This top event fault tree is used in the ISL-RCP-S1LO event tree.

5.1.21 SLOCA Downstream of RCP Thermal Barrier Heat Exchanger (ISL-RCP-TBHX-DNSTREAM)

Description. If an RCP thermal barrier heat exchanger ruptures, there is the potential for a downstream ACCW system ISLOCA. Two MOVs are available to prevent an ISLOCA downstream of the RCP thermal barrier heat exchangers for each of the RCPs. The first of these MOVs is associated with the individual RCP thermal barrier heat exchanger that could rupture. The second MOV is common to all four RCPs. These MOVs will receive an automatic closure signal on high flow. If either the individual MOV associated with the RCP or the

common MOV close, the ISLOCA will be prevented. If both MOVs that could prevent the ISLOCA fail, a subsequent ISLOCA occurs.[170]

ISL-RCP-TBHX-DOWNSTREAM Fault Tree Use. This top event fault tree is used in the ISL-RCP-TBHX event tree.

Required Support Systems. For these valves to automatically close on high flow, 480 V AC power is needed. In addition, safety-related 120 V AC power is needed for the high flow valve closure signal.

5.1.22 Operators Fail to Close HV1974 (ISL-RCP-TBHX-HV1974)

Description. During an ACCW system ISLOCA downstream of the ruptured RCP thermal barrier heat exchanger, HV1974 can be closed to limit the SLOCA to inside the containment. Operator action (OA-IS-ISLACC-H) is required to manually close HV1974. If HV1974 is not closed, the ISLOCA continues and core damage is assumed.

ISL-RCP-TBHX-HV1974 Fault Tree Use. This top event fault tree is used in the ISL-RCP-TBHX event tree.

Required Support Systems. 480 V AC power is needed for operators to manually close HV1974.

5.1.23 Operators Fail to Close HV1978 (ISL-RCP-TBHX-HV1978)

Description. During an ACCW system ISLOCA upstream of the ruptured RCP thermal barrier heat exchanger, HV1978 can be closed to limit the SLOCA to inside the containment. Operator action (OA-IS-ISLACC-H) is required to manually close HV1978. If HV1978 is not closed, the ISLOCA continues and core damage is assumed.

ISL-RCP-TBHX-HV1978 Fault Tree Use. This top event fault tree is used in the ISL-RCP-TBHX event tree.

Required Support Systems. 480 V AC power is needed for operators to manually close HV1978.

5.1.24 Relief Valves Protect Piping Integrity (ISL-RCP-TBHX-RPT)

Description. During a rupture of a RCP thermal barrier heat exchange with the failure of the upstream check valves or the downstream MOVs to close, the ACCW supply and return lines will be pressurized. Relief valves are located on the ACCW RCP motor cooling water return line of each RCP. Since the rupture is limited to a single 0.75-inch diameter tube, these relief valves could prevent over pressurization of the ACCW system outside containment. If all four relief valves open, a SLOCA inside the containment occurs. If any of these valves fail to open, ACCW piping (both inside and outside containment) will be pressurized.[171]

---

[170] Fault tree modeling of control logic for these MOVs is represented using an undeveloped basic event. This modeling simplification has a negligible effect on the results.

[171] The success criteria requiring all four relief valves to open is potentially conservative.

ISL-RCP-TBHX-RPT Tree Use. This top event fault tree is used in the ISL-RCP-TBHX event tree.

5.1.25 ISLOCA Upstream of RCP Thermal Barrier Heat Exchanger (ISL-RCP-TBHX-UPSTREAM)

Description. If a RCP thermal barrier heat exchanger ruptures, there is the potential for an upstream ACCW system ISLOCA. Directly upstream of the RCP thermal barrier heat exchangers is a check valve, on for each RCP. Since the ISL-RCP-TBHX event tree represents the failure of any of the four RCP thermal barrier heat exchangers, the RCP specific valves are represented by a single basic event (ACW-CKV-OO-084_____). If the applicable check valve reseats, no ISLOCA will occur. If the applicable check valve fails, an ISLOCA occurs.

ISL-RCP-TBHX-UPSTREAM Fault Tree Use. This top event fault tree is used in the ISL-RCP-TBHX event tree.

5.1.26 Operators Recover (Isolate) ISLOCA in RHR Cold Leg Train A or B (ISL-RHR-CLI-A-REC, ISL-RHR-CLI-B-REC)

Description. The ISLOCA break size from the RHR cold leg injection lines will be limited by the size of the RHR cold leg injection line piping. This results in a MLOCA that can be mitigated by injection via 2 of 4 CCPs or SI pumps to 2 of 3 intact RCS loops until the depletion of the RWST. Operator action (OA-IS-ISLRHR-H) is required to terminate the RHR system ISLOCA by manually closing an MOV for cold legs 1 and 2 or an MOV cold legs 3 and 4. If the ISLOCA is not isolated (due to operator or hardware failures), core damage is assumed.

ISL-RHR-CLI-A(B)-REC Fault Tree Use. This top event fault tree is used in the ISL-RHR-CLI-A and ISL-RHR-CLI-B event trees.

Required Support Systems. The same support systems required for CCPs and SI pumps (HPI) are needed; see Section 5.1.12 for further information. In addition, 480 V AC power is required for motive and control power to MOV operators for the cold leg valves.

5.1.27 Low-Pressure Injection (LPI)

Description. One of the functions of the RHR system is to provide the long-term cooldown requirements of the ECCS. In this function, the RHR system provides a low-pressure, high-volume water source to the RCS by supplying water from the RWST during the injection phase and from the containment sump during the recirculation phase. When an SI signal is generated, both RHR pumps start. While in standby mode, most of the RHR valves required for LPI are already open. The RWST suction valves, the pump flow control valves, and the pump discharge isolation valves are open. The only RHR valves that receive an SI signal are the sump isolation valves, which open given a concurrent low-low RWST level signal. An SI signal is generated by any of the following conditions:

- High containment pressure
- Low pressurizer pressure
- Low pressure in any main steam line

- Manual SI actuation

Two RHR pumps are installed in parallel flow paths in the RHR system. To ensure that the RHR pumps do not overheat when the discharge line is closed, or discharge is prevented by high RCS pressure, a minimum flow line from the downstream side of each RHR heat exchanger to the pump suction line is provided. A control valve located in each minimum flow line, controlled by the flow switch at the RHR pump discharge, opens to maintain a minimum of flow to protect the pump and closes when the RHR pump discharge flow exceeds about twice the minimum flow.

When the RCS pressure drops below the RHR pump shutoff head, water from the RWST is pumped into cold leg branch lines 1 and 2 by RHR pump A, and into cold leg branch lines 3 and 4 by RHR Pump B. The branch lines contain orifices that limit pump run out and equalize flow through the branch lines such that the amount of coolant leakage is minimized if one of the injection lines spills into the containment.

Train A and train B injection flow paths are cross-connected during the injection phase through two open cross-connect valves, one associated with each train. Injection flow from the SI pumps discharges between the check valves in the branch lines leading to the cold legs. Flow control valves automatically recirculate flow back to the suction of the respective RHR pump until injection flow increases to about twice the minimum flow required for pump protection.

LPI Fault Tree Use. This top event fault tree is used in the LLOCA, MLOCA, SLOCA, and consequential SLOCA event trees.

Required Support Systems. The following support systems are required for successful operation of the LPI:

- The plant electrical power systems are required for the operation of LPI. AC power is required for motive power to pump motors and for motive and control power to MOV operators, while DC power is required for control power to the pump motors and circuit breakers. All pumps, valves, and other equipment that are required for cooling of safety-related components are supplied from safety-related buses. These safety-related buses are supplied by emergency power if primary power sources are lost.

- The ESFAS sends start signals to the RHR pumps.

- The NSCW system cools the RHR pump motors and lube oil.

- The CCW system cools the RHR pump seals. However, this dependency is not modeled in the PRA based on manufacturer test results that indicate the seals will remain operable under worst case operating temperature and pressure conditions without CCW cooling to the seals.

- The RHR pumps receive room cooling that is provided by the normal chilled water system and the essential chilled water system but is not required based on a room heat-up analysis.

Additional System Fault Trees. The following fault tree for LPI is also used in the L3PRA project Level 1 model.

5.1.27.1 Low-Pressure Injection after AC Power Recovery from an SBO (LPI-ACR)

Description. This fault tree is a specialization of the LPI fault tree that is used following AC power recovery from an SBO. The AC power support logic is specialized for conditions following successful AC power restoration.

LPI-ACR Fault Tree Use. This top event fault tree is used in the SBO-1 event tree.

5.1.28 Low-Pressure Recirculation (LPR)

Description. When the RWST contents have been reduced to the low-low level alarm set-point during LPI, the suction for LPI must be switched to the containment sump. One of two RHR pumps is required to supply at least one intact cold leg. The change from the injection phase to the cold leg recirculation phase is a manual/automatic process. When the water level reaches the low-low level alarm point in the RWST, the two RHR sump isolation valves automatically open and the RHR pumps (along with the SI pumps and CCPs) are sequentially shifted to the cold leg recirculation phase of operation. Operators are required to manually isolate the RWST from the RHR pumps.[172] The heat sink for the recirculation water is provided either by CCW to the RHR heat exchanger associated with a running RHR pump, or by 4 of 8 CCUs.

LPR Fault Tree Use. This top event fault tree is used in LLOCA, MLOCA, SLOCA, and consequential SLOCA event trees.

Required Support Systems. The following support systems are required for successful operation of the LPR:

- The plant electrical power systems are required for the operation of LPR. AC power is required for motive power to pump motors and for motive and control power to MOV operators, while DC power is required for control power to the pump motors and circuit breakers. All pumps, valves, and other equipment which are required for cooling of safety-related components are supplied from safety-related buses. These safety-related buses are supplied by emergency power if primary power sources are lost.

- The ESFAS sends start signals to the RHR pumps. In addition, ESFAS sends signals to open the two RHR sump isolation valves at the RWST low-low level alarm set-point.

- The NSCW system cools the RHR pump motors and lube oil. The NSCW system provides the path to the ultimate heat sink during LPR via the RHR heat exchangers and the CCW system.

- The CCW system cools the shell side of the RHR heat exchangers. In addition, the CCW system cools the RHR pump seals. However, this dependency is not modeled in the PRA based on manufacturer test results that indicate the seals will remain operable under worst case operating temperature and pressure conditions without CCW cooling to the seals.

---

[172] The HFE(s) used depend on the size of the LOCA, which affects the time to recirculation switch-over (i.e., low RWST level). For a LLOCA, the HFE OAR_LPLL-----H is used, while for a MLOCA OAR_LPML-----H is used. A SLOCA or consequential SLOCA uses either OAR_LPSL-----H or OAR_LPSL2----H, depending on whether at least 3 of 8 CCUs are running (which prevents containment spray actuation).

- The CCUs provide the ultimate heat sink if CCW to the RHR heat exchangers is not available.

- The RHR pumps receive room cooling that is provided by the normal chilled water system and the essential chilled water system but is not required based on a room heat-up analysis.

Additional System Fault Trees. The following fault tree for the low-pressure recirculation is also used in the L3PRA project Level 1 model.

5.1.28.1 Low-Pressure Recirculation after AC Power Recovery from an SBO (LPR-ACR)

Description. This fault tree is a specialization of the LPR fault tree that is used following AC power recovery from an SBO. The AC power support logic is specialized for conditions following successful AC power restoration.

LPR-ACR Fault Tree Use. This top event fault tree is used in the SBO-1 event tree.

5.1.29 Main Feedwater during ATWS (MFW-ATWS)

Description. During an ATWS, the MFW system will not be isolated by the P-4 interlock on a reactor trip, because during an ATWS the reactor fails to trip, and the RCS temperature does not decrease sufficiently. Therefore, only initiating events that result in unavailability of MFW (e.g., loss of MFW, loss of condenser, SLOCA, loss of safety-related 4.16 kV bus, or loss of safety-related 125 V DC bus) will experience an immediate MFW loss. If MFW is available during an ATWS, the RCS pressure increase will be limited; and only the ability to shut down the reactor by emergency boration is needed (given the pressurizer PORVs and SRVs reclose). Success of MFW during an ATWS requires the use of both turbine-driven MFW pumps to provide flow to all four SGs. In addition, sufficient steam removal is required by either: (1) three TBVs or (2) an ARV or 1 of 5 SRVs for 4 of 4 SGs.

MFW-ATWS Fault Tree Use. This top event fault tree is used in the ATWS event tree.

Required Support Systems. The same support systems required for MFW as part of the FW fault tree (see Section 5.1.10 for additional information) are needed for MFW during an ATWS.

5.1.30 Offsite Power Recovery (OPR)

Description. This function represents restoration of offsite power, or power from an alternate switchyard, to both safety-related 4.16 kV AC buses.[173] Different versions of this fault tree are available for recovery of offsite power at 1 and 2 hours because AC power recovery is required prior to battery depletion or core uncovery; whichever occurs first. If the turbine-driven AFW pump fails or is unavailable, operators will have approximately one hour to recover offsite

[173] Restoration of AC power can be accomplished by recovery of offsite power for plant-centered and switchyard-related LOOPs or the alignment an alternate switchyard. The recovery of AC power is assumed to occur for both safety-related 4.16 kV AC buses (AA02 and BA03). This may be non-conservative (especially for an alternate switchyard that can only be aligned to a single safety-related 4.16 kV AC bus. Model changes to credit only a single safety-related 4.16 kV AC bus would be extensive and were not pursued).

power.[174] If the turbine-driven AFW pump successfully provides early decay heat removal, operators will have approximately two hours to recover AC power (based on the most limiting depletion time of the plant batteries). Once the batteries are depleted, DC control power is lost; and therefore, it is assumed that the operation of breakers and switches required to restore offsite power (or the alignment to the alternate switchyard) to the safety-related 4.16 kV AC buses cannot be performed.[175] As such, the L3PRA project Level 1 model assumes core damage if AC power is not recovered prior to two hours.[176] The OPR fault tree logic is structured such that AC power credit is not applied to SBO cut sets (that result from LOOP initiating events) in which each safety-related train is failed due to either: (1) reserve auxiliary transformer (RAT) output breaker failure to open, (2) sequencer failure, (3) NSCW failure with subsequent RCP LOCA, or (4) unavailabilities of the safety-related batteries (see Section 8.1.1 for additional information). The failure probability for AC power recovery is calculated using the formulation for power recovery detailed in Section 7.4.

OPR Fault Tree Use. This top event fault tree is used in the SBO event tree.[177]

Additional System Fault Trees. The following fault trees for offsite power recovery are also used in the L3PRA project Level 1 model.

5.1.30.1 Offsite Power Recovery in 1 Hour (OPR-01H)

Description. During a SBO, if the turbine-driven AFW pump is unavailable, then operators have one hour to restore offsite power or align the alternate switchyard to the safety-related 4.16 kV AC buses.

OPR-01H Fault Tree Use. This substitution fault tree is used in the SBO event tree.

5.1.30.2 Offsite Power Recovery in 2 Hours (OPR-02H)

Description. During a SBO, if the turbine-driven AFW pump successfully provides early decay heat removal, operators have two hours to restore offsite power or align the alternate switchyard to the safety-related 4.16 kV AC buses.

OPR-02H Fault Tree Use. This substitution fault tree is used in the SBO event tree.

---

[174] After AC power is recovered, operators will have an additional 30 minutes (approximately) to restore systems that were unavailable during the SBO. ECA-0.0 directs operators to place the hand switches to equipment rendered unavailable by the SBO (e.g., ECCS pumps, motor-driven AFW pumps, ACCW pumps, and CCUs) to the pull-to-lock position.

[175] Some of these breakers may have the capability to be closed manually without DC power. However, there is no procedural guidance to implement this action and, therefore, it is not modeled in the L3PRA Project Level 1 model.

[176] Continued operation of the turbine-driven AFW pump after DC power is lost is possible (and proceduralized) that could delay the time to when core damage occurs (or prevent it). However, with no reliable indication of SG water level (after the safety-related batteries are depleted at four hours), there is significant potential for unsustainable operation (e.g., overfilling the SGs and flooding the steam lines, including the AFW pump turbine). In addition, AC power recovery is needed to achieve a safe/stable end-state; therefore, continued operation of the turbine-driven AFW was not credited in the L3PRA Level 1 model. However, credit for continued operation of the turbine-driven AFW is provided in the Level 2 portion of the L3PRA model.

[177] This top event fault tree is always substituted either with the OPR-1H or OPR-2H fault trees, depending on the accident sequence.

5.1.31 Pressure-Induced SGTR (PI-SGTR)

Description. During a SSB (initiating event or consequential), a pressure-induced SGTR may result from a pressure differential across the tubes that exceeds the design limit. If the secondary-side pressure drops suddenly to atmospheric pressure, the pressure difference across the tubes can significantly exceed this design limit. Such a pressure difference can occur with larger size SSBs. Even then, without the existence of deep existing flaws (beyond the tube plugging criteria), this pressure difference is not expected to cause a consequential SGTR. This fault tree captures the probability of having a sufficiently deep flaw, along with the probability that the ensuing tube rupture will proceed to core damage (using a fault tree representation of the relevant top event fault trees from the SGTR event tree). See Section 8.5 for additional information.

PI-SGTR Fault Tree Use. This top event fault tree is used in the SSB event trees.

Required Support Systems. The support systems for the following functions are needed to mitigate a pressure-induced SGTR:

- AFW (Section 5.1.2) or feed and bleed cooling (Section 5.1.8)
- HPI (Section 5.1.12)
- SG Isolation (Section 5.1.42)
- Early and late cooldown and depressurization (Section 5.1.4)
- Shutdown cooling mode of RHR (Section 5.1.39)
- CST makeup (Section 5.1.6)
- Feed and bleed recirculation (Section 5.1.9)

5.1.32 Primary Relief Valves (PORVs/SRVs) Reclose (PVC)

Description. There are two PORVs on the pressurizer, each having the capacity to relieve steam flow to prevent over-pressurization of the RCS. One of the PORVs is set at a slightly higher relief pressure than the other as sensed by the pressurizer pressure instrumentation. These valves may also be opened by remote manual control. They close when pressure decreases below the pressure reset limit. During power operation, they prevent excessive pressure increases in the RCS, while minimizing the actuation of the safety valves. The PORVs are solenoid-operated and fail closed.

Each PORV has a normally open and remotely motor-operated isolation block valve located upstream of the PORV that provides a positive shutoff capability should the PORV become inoperable. The PORVs and their associated block valves are interlocked by a pressurizer low-pressure interlock. Actuation of the interlock prevents the relief valves from opening and closes the block valves at set point pressure. Manual control may override this interlock.

The pressurizer also has three spring-loaded, self-actuated, code safety valves that operate to prevent RCS pressure from exceeding 110 percent of system design pressure.

If challenged during an initiating event, the PORV(s) should reclose if opened.[178] If the PORV(s) fail to reclose, the associated block valve is designed to auto-close to isolate the relief path.[179] The pressurizer SRVs are required to open only when the PORVs fail to open (except for ATWS sequences). If the pressurizer SRVs are demanded to open, all SRVs should reclose after opening. If the PORV(s) or the SRVs stick open, a consequential SLOCA occurs.

PVC Fault Tree Use. This top event fault tree is used in most transient event trees.

Required Support Systems. The following support systems are required for successful operation of the PORVs:

- AC power is required to operate the block valves, while DC power is required to operate the PORVs (the SRVs are spring-loaded, self-actuated, code safety valves with no required support).

Additional System Fault Trees. The following fault trees for the modeling of the PORVs/SRVs challenged are also used in the L3PRA project Level 1 model.

5.1.32.1 Primary Relief Valves (PORVs/SRVs) Reclose during SBO (PVC-B)

Description. This fault tree is the same as the PVC fault tree above, except that it uses a fault tree flag set to fail both offsite and emergency AC power to the valve supports.

PVC-B Fault Tree Use. This top event fault tree is used in the SBO event tree.

5.1.32.2 Primary Relief Valves (PORVs/SRVs) Reclose during ATWS (PVC-ATWS)

Description. During an ATWS and given the failure of MFW, all (unisolated) PORVs and SRVs will be challenged to mitigate the pressure transient. In addition, this fault tree includes whether a SLOCA or SGTR initiating event occurred.

PVC-ATWS Fault Tree Use. This top event fault tree is used in the ATWS event tree.

5.1.33 Primary Pressure Relief (PPR)

Description. If MFW is unavailable during an ATWS, RCS pressure relief is needed to prevent RCS pressure from increasing above 3200 psi, which leads to an RCS integrity breach beyond the capability of the ECCS and subsequent core damage. The success of primary pressure relief depends not only on the availability of the pressurizer PORVs and SRVs, but also the negative reactivity feedback [i.e., unfavorable exposure time (UET)]. Many factors, such as initial power level, time in cycle when transient occurs, reactivity feedback as a function of the cycle life, the number of available relief valves, the failure or success of manually inserting the control rods, and AFW flow rates, affect UET. Given the L3PRA project Level 1 model

---

[178] The L3PRA Project Level 1 model includes this potential for most transient initiating events and incorporates specialized conditional PORV failure to close on demand probabilities depending on which initiating event occurred. These probabilities were taken from Table 11 of NUREG/CR-7037, "Industry Performance of Relief Valves at U.S. Commercial Nuclear Power Plants through 2007" (NRC, 2011).

[179] The PORV block valves can also be manually closed; however, credit for this action is not included in the L3PRA Project Level 1, internal event model.

assumptions on initial power level (assumed to be 100 percent) and that no credit is given for insertion of the control rods, two cases exist in which the primary relief capacity is sufficient:

- Case 1 – all PORVS/SRVs are available.
- Case 2 – one PORV is blocked during the transient, but the other PORV and all SRVs available.

For either case, all available relief valves must open to prevent RCS pressure from exceeding 3200 psi. According to WCAP-15831 (Westinghouse, 2007), the UETs for these cases are 0.11 and 0.32, respectively.

PPR Fault Tree Use. This top event fault tree is used in the ATWS event tree.

5.1.34 Pressurizer Valves Reseat (PZRR)

Description. This top event represents the success or failure of the pressurizer valves (PORVs and SRVs) to reclose after SI is terminated following an inadvertent SI actuation. Failure of one or more valves to reclose results in a consequential SLOCA. During an inadvertent SI actuation, it is mostly likely that either two-phase flow or liquid would pass through the pressurizer valves. The failure probability of the PORVs was not modified for this case, since they are designed for passing either steam or water. However, the SRVs are not designed for passing two-phase flow. Therefore, a higher failure probability (0.1 was used based on recommendations from subject matter experts during peer review of the reference plant PRA) was used for the probability of a failure of a SRV to reclose.

PZRR Fault Tree Use. This fault tree is a top event in the inadvertent SI event tree.

5.1.35 Reactor Coolant Pump Seal Cooling (RCPSC)

Description. The ACCW system provides RCP seal cooling via the thermal barrier heat exchangers. If RCP seal injection fails, RCP seal cooling prevents the integrity of RCP seals from being challenged. Successful RCP seal cooling to the RCP thermal barrier heat exchangers requires 1 of 2 ACCW pump and 1 of 2 ACCW heat exchangers (cooled by NSCW). According to the WOG 2000 RCP seal leakage model, if a loss of both seal injection and RCP thermal barrier cooling occurs, the RCP seal leakage would be 21 gpm per pump, initially. After 13 minutes, RCP seal leakage could increase to 76 gpm, 182 gpm, or 480 gpm per pump, depending on whether stage 1 fails, stage 2 fails, or both stages fail. The seal failure probabilities for binding/popping failure mode events are 0.0125 (stage 1) and 0.2 (stage 2). In addition, operator action (RCS-XHE-XM-TRIP) is required to trip the RCPs to prevent the failure of both RCP seals.

RCPSC Fault Tree Use. This top event fault tree is in most transient event trees.

Required Support Systems. The same support systems required for ACCW are needed for RCP seal cooling; see Section 5.2.5 for further information.

5.1.36 Reactor Coolant Pump Seal Injection (RCPSI)

Description. RCP seal injection is normally provided by the NCP.[180] If RCP seal injection fails, seal leakage is assumed to increase to at least 21 gpm per RCP.[181].

RCPSI Fault Tree Use. This top event fault tree is in most transient event trees.

Required Support Systems. The following support systems are needed for normal RCP seal injection:

- Nonsafety-related 4.16 kV AC power for the NCP.
- ACCW for adequate cooling of the NCP motor coolers.

Additional System Fault Trees. The following fault trees for the modeling of RCP seal injection are also used in the L3PRA project Level 1 model.

5.1.36.1 RCP Seal Injection during LOACCW (RCPSI-LOACCW)

Description. This fault tree models the operator action (OA-CCP-ALIGN---H) and applicable charging system structures, systems, and components (SSCs) required to align the CCPs to provide alternate RCP seal injection after a loss of ACCW. A loss of ACCW renders the NCP unavailable due to lack of pump cooling. In addition, RCP seal cooling provided by the thermal barrier heat exchangers is also lost. The failure to align the CCPs to provide seal injection will challenge the integrity of the RCP seals.

RCPSI-LOACCW Fault Tree Use. This top event fault tree is used in the loss of ACCW event tree.

Required Support Systems. The same support systems required for CCPs (HPI) are needed for charging; see Section 5.1.12 for further information.

5.1.36.2 RCP Seal Injection during Inadvertent SI Actuation (RCPSI-CCPs)

Description. A SI actuation results in the trip of the NCP and the starting of the CCPs; therefore, this fault tree addresses RCP seal injection using only the CCPs. If the CCPs start, RCP seal injection will be automatically restored. If the CCPs fail to start, RCP seal injection is unavailable; therefore, RCP seal cooling via the thermal barrier heat exchangers is the only means to prevent the seals from being challenged.

---

[180] If the NCP fails or is rendered unavailable (e.g., due to loss of nonsafety-related 4.16 kV AC power cause by a LOOP), the CCPs can be aligned for alternate seal injection. However, due to the limited time window (13 minutes) and the time required for operators to get to the procedure steps for this action, it is only credited in the loss of ACCW and loss of RCP seal injections initiating events. If either of these two initiating events occur, operators are directed almost immediately by procedures to align the CCPs for alternate RCP seal injection.

[181] Elevated RCP seal leakage rates are conservatively assumed regardless of the success or failure of RCP thermal barrier cooling.

RCPSI-CCPs Fault Tree Use. This top event fault tree is used in the SSB event trees, since they involve an SI actuation. However, for the inadvertent safety injection initiating event, it is assumed that at least one CCP is injecting into the RCS, so this fault tree is not needed.

Required Support Systems. The same support systems required for CCPs (HPI) are needed for charging; see Section 5.1.12 for further information.

5.1.37 Reactor Protection System (RPS)[182]

Description. The reactor protection system automatically keeps the reactor operating within a safe region by shutting down the reactor whenever the limits of the region are approached. The safe operating region is defined by several considerations, such as mechanical/hydraulic limitations on equipment and heat transfer phenomena. Therefore, the reactor protection system keeps surveillance on process variables that are directly related to equipment mechanical limitations, such as pressure and pressurizer water level (to prevent water discharge through safety valves and uncovering heaters), and on variables that directly affect the heat transfer capability of the reactor (e.g., flow and reactor coolant temperatures). Other parameters used in the reactor protection system are calculated from various process variables. In any event, whenever a direct process or calculated variable exceeds a set-point, the reactor will be shut down to protect against either gross damage to fuel cladding or loss of system integrity that could lead to release of radioactive fission products into the containment.

The following systems make up the reactor protection system:

- Process instrumentation and control system
- Nuclear instrumentation system
- Solid-state logic protection system
- Reactor trip switchgear
- Manual actuation circuit

The reactor protection system consists of sensors that monitor various plant parameters when connected with analog circuitry consisting of two to four redundant channels, and of digital circuitry, consisting of two redundant logic trains that receive inputs from the analog protection channels to complete the logic necessary to automatically open the reactor trip breakers (RTBs).

Either of the two trains, A or B, is capable of opening separate and independent RTBs, A and B, respectively. The two RTBs, in series, connect three-phase AC power from the rod drive motor-generator sets to the rod drive power cabinets. During plant power operation, a DC under-voltage coil on each RTB holds a trip plunger out against its spring, allowing the power to be available at the rod control power supply cabinets. For reactor trip, a loss of DC voltage to the under-voltage coil, as well as energization of the shunt trip coils, trips open the breaker. When

[182] The RPS fault tree in the L3PRA Project Level 1 model is based on the RPS modeling described in NUREG/CR-5500, "Reliability Study: Westinghouse Reactor Protection System, 1984-1985," Volume 2 (NRC, 1999b). The primary reason for using the NUREG/CR-5500 modeling approach is to use two separate events for failure to manually trip the reactor, conditional on the presence or absence of the RPS signal.

either RTB opens, power is interrupted to the rod drive power supply, and the control rods drop into the core. The control rods cannot be withdrawn until the RTBs are manually reset. The RTBs cannot be reset until the abnormal condition that initiated the trip is corrected.

A successful reactor trip requires a sufficient number of control rods to be inserted into the reactor core to stop the nuclear chain reaction. If the reactor trip is unsuccessful due to electrical failures, operators can manually scram the reactor. The L3PRA project Level 1 model considers two operator actions for scramming the reactor, depending on whether an RPS signal is available as a cue to the operators (OA------MANRTH or RPS-XHE-XE-NSGNL). However, RPS unreliability is dominated by failures of the RTBs and mechanically stuck control rods, for which manual scram is not effective. The plant response given RPS failure is modeled in the ATWS event tree.

RPS Fault Tree Use. This top event fault tree is used in most event trees.

5.1.38 Reactor Shutdown (ATWS) – Late (RXSD)

Description. If the initial RCS pressure transient due to the ATWS is mitigated, then negative reactivity must be added to shut down the reactor to bring the plant to a safe and stable end-state. This can be accomplished by manual trip of the reactor, manual rod insertion, or emergency boration, depending on what RPS failures have occurred. If the RTBs have failed or the control rods are mechanically stuck, operators will need to either manually insert control rods or initiate emergency boration.[183] Success implies the operator starts and aligns a charging pump (NCP or CCP) to provide borated water from one of the borated water sources to the reactor core (OA-OBR-------H).

If the RTBs have not failed and the control rods are not mechanically stuck, operators are procedurally directed to manually trip the reactor.[184] In the L3PRA project Level 1 model, for an ATWS to occur, operators would have already failed to manually trip the reactor within 90 seconds.[185] Also, due to the pressure transient caused by the power mismatch with the failure of MFW, operators have new cues that an ATWS has occurred. This provides additional time for operators to manually trip the reactor (represented by HFE RPS-XHE-TRIP-LT[186]).

RXSD Fault Tree Use. This fault tree is a top event in the ATWS event tree.

Required Support Systems. The same support systems required for CCPs (HPI) are needed for emergency boration; see Section 5.1.12 for further information. In addition, the following support systems are needed for emergency boration using the NCP:

---

[183] As a modeling simplification, the L3PRA Level 1 model only includes emergency boration to credit shutting down the reactor, even though procedures have diverse steps to shut down the reactor. This modeling simplification has a negligible effect on the overall core damage frequency (CDF).

[184] Operators will not enter the ATWS procedure (FR-S.1) unless they attempt to manually trip the reactor, but the rods fail to insert.

[185] It was determined by NRC staff that 90 seconds was insufficient time to insert control rods enough to prevent the pressure excursion given a failure of MFW (see Table 6-2 for additional information).

[186] A post-processing rule is used to delete the initial failure to trip the reactor HFEs (OA------MANRTH or RPS-XHE-XE-NSGNL) in cut sets that also include RPS-XHE-TRIP-LT. The HFE RPS-XHE-TRIP-LT represents operator failure to manually trip the reactor after 90 seconds (given the initial failure).

- The NCP is powered by nonsafety-related 4.16 kV AC power.

- The NCP motor coolers require ACCW for adequate pump cooling.

5.1.39 Residual Heat Removal (RHR)

Description. During an SLOCA, SGTR, or consequential SLOCA (RCP seal failure or stuck-open PORV/SRV), the shutdown cooling mode of RHR may be used once RCS pressure and hot-leg temperatures have been lowered to satisfy RHR design entry conditions. Success requires 1 of 2 trains of RHR to operate and remove decay heat for 24 hours. In addition, at least 3 of 8 CCUs need to be successfully running to prevent high containment pressure actuation of the containment spray system.[187] If six or more CCUs fail, the actuation of containment spray will cause the rapid depletion of RWST inventory, leaving insufficient time for operators to reach entry conditions for the shutdown cooling mode of RHR.

RHR Fault Tree Use. This top event fault tree is in the SLOCA, SGTR, and consequential SLOCA event trees.

Required Support Systems. The following support systems are required for successful operation of the RHR system in shutdown cooling mode:

- The plant electrical power systems are required for operation of the RHR system for shutdown cooling. AC power is required for motive power to pump motors and for motive and control power to MOV operators, while DC power is required for control power to the pump motors and circuit breakers. All pumps, valves, and other equipment that are required for cooling of safety-related components are supplied from safety-related buses. These safety-related buses are supplied by emergency power if primary power sources are lost.

- The NSCW system cools the RHR pump motors and lube oil.

- The CCW system cools the RHR pump seals. However, this dependency is not modeled in the PRA based on manufacturer test results that indicate the seals will remain operable under worst case operating temperature and pressure conditions without CCW cooling to the seals.

- The RHR pumps receive room cooling provided by the normal chilled water system and the essential chilled water system but is not required based on room heat-up analysis.

Additional System Fault Trees. The following fault tree for the shutdown cooling mode of RHR is also used in the L3PRA project Level 1 model.

[187] During a SGTR, containment spray will not actuate; therefore, the CCUs are not required to operate to allow for sufficient time to reach entry conditions for shutdown cooling.

5.1.39.1 RHR after AC Power Recovery from a SBO (RHR-ACR)

Description. This fault tree is a specialization of the RHR fault tree that is used following AC power recovery from an SBO. The AC power support logic is specialized for conditions following successful AC power restoration.

RHR-ACR Fault Tree Use. This top event fault tree is used in the SBO-1 event tree.

5.1.40 RWST Refill (RFL)

Description. If primary-to-secondary leakage is not terminated during a SGTR, the RCS inventory will continue to be lost out the open ARV/SRVs of the ruptured SG. Thus, makeup to the RWST is needed to reach a 72-hour safe and stable end-state. Operator action (RFL-XHE-REFILL-LT) is required to refill the RWST.[188]

RFL Fault Tree Use. This top event fault tree is used in the SGTR event tree.

5.1.41 Additional Requirements for 72-Hour Safe/Stable End-state (SAFE/STABLE)

Description. Given a failure of RCP seal injection with the integrity of RCP seals maintained, the RCP seals are assumed to leak at a rate of 21 gpm per RCP due to lack of seal injection.[189] In this case, core damage prior to 72 hours can occur if a source of inventory makeup to the RCS is not provided. If alternate charging fails, operators will eventually be directed by CSFST procedures to depressurize the SGs with a modeled minimal success criterion of 3 of 3 TBVs (to the condenser) or an ARV for 1 of 4 SGs. If successful, this depressurization will allow the accumulators (2 of 4 accumulators required for success) to inject into the RCS, thus providing makeup. An operator action (CAD-XHE-SAFESTABLE) is required. If the cooldown and depressurization, or accumulators fail, core damage will occur prior to 72 hours. Note that CST inventory makeup is also required to maintain AFW flow for these scenarios; see Section 5.1.6 for additional information.

SAFE/STABLE Fault Tree Use. This top event fault tree is in most transient event trees.

Required Support Systems. The same support systems required for cooldown and depressurization are needed for this fault tree; see Section 5.1.4 for additional information.

Additional System Fault Trees. The following fault tree for additional requirements for a 72-hour safe/stable end-state is also used in the L3PRA project Level 1 model.

5.1.41.1 Additional Requirements for 72-Hour Safe/Stable End-state after AC Power Recovery from a SBO (SAFE/STABLE-ACR)

Description. This fault tree is a specialization of the SAFE/STABLE fault tree that is used following AC power recovery from an SBO. The AC power support logic is specialized for conditions following successful AC power restoration.

---

[188] The fault tree modeling for refilling the RWST only includes the HFE, and does not include hardware failures, as it is expected that the HFE will likely dominate the failure to accomplish this action.

[189] This assumption is conservative for scenarios with successful RCP seal cooling (via ACCW through the thermal barrier heat exchangers).

SAFE/STABLE-ACR Fault Tree Use. This top event fault tree is used in the SBO event tree.

5.1.42 Steam Generator Isolation (SGI)

Description. During a SGTR, procedures direct operators to isolate the faulted SG. Operators must diagnose the LOCA as a SGTR, identify which SG has the tube rupture, and isolate the SG to prevent overfill (as represented by the HFE OAI_SG-------H). Successful SG isolation requires operators to close at least one MSIV on the affected SG and the associated MSIV bypass valve. If SG 1 or 2 is the affected SG, then operators must also close the steam supply valve to the turbine-driven AFW pump. Operators can also prevent SG overfill by closing the MSIVs and associated bypass valves on the other three (intact) SGs and stopping feed flow to the affected SG.

SGI Fault Tree Use. This top event fault tree is used in the SGTR event tree.

Additional System Fault Trees. The following fault trees for the modeling of SG isolation are also used in the L3PRA project Level 1 model.

5.1.42.1 Steam Generator Isolation during SSBI (SGI-SSBI)

Description. During an SSB upstream of the MSIVs and downstream of the main MFIVs, the MSIVs will close on low steam line pressure. In addition, an SI actuation will occur that closes MFIVs and MFRVs, including bypass valves. Operator action (SSB-XHE-ISOLATION) is required to isolate AFW flow to the faulted SG. Operators can also isolate the faulted SG by closing the MSIVs and MFW valves on all other three intact SGs and terminating AFW flow to the faulted SG.

SGI-SSBI Fault Tree Use. This top event fault tree is used in the SSBI and CSSBI event trees.

5.1.42.2 Steam Generator Isolation during SSBO (SGI-SSBO)

Description. During an SSB downstream of the MSIVs and upstream of the MFIVs, the MSIVs and MFIVs (including bypasses) for all four SGs must be closed to terminate the leak. These valves will close automatically due to low steam line pressure and SI actuation. AFW flow does not need to be isolated for these SSBs.

SGI-SSBO Fault Tree Use. This top event fault tree is used in the SSBO event tree.

5.1.42.3 Steam Generator Isolation during Consequential SSBO (SGI-CSSBO)

Description. A consequential SSB downstream of the MSIVs only requires that the MSIVs (including bypasses) for all four SGs be closed to terminate the leak.[190]

SGI-CSSBO Fault Tree Use. This top event fault tree is used in the CSSBO event tree.

---

[190] Unlike an SSB (downstream of the MSIVs) initiating event, a consequential SSB downstream of the MSIVs does not consider MFW line breaks; therefore, feedwater isolation (i.e., closure of MFIVs and bypass valves) is not needed to terminate the leak.

5.1.43 Consequential SLOCA during SSB (SSB-CSLOCA)

Description. During an SSB, an SI actuation is assumed to occur. Since the head of the CCPs is higher than the set-points of the pressurizer PORVs and SRVs, these valves will open.[191] If the CCPs are not stopped, the pressurizer PORVs or SRVs will remain open, resulting in a consequential SLOCA. Operator action (OAT----------H) is required to terminate SI, align a single CCP for normal charging, and establish letdown. This fault tree is composed of the TSI and PZRR fault trees (see Section 5.1.45 and Section 5.1.34 for additional information).

SSB-CSLOCA Fault Tree Use. This top event fault tree is used in the SSB event trees.

5.1.44 Secondary Relief Valves Close (SVC)

Description. During a reactor trip with the TBVs unavailable, the SG ARVs will open to relieve SG pressure. If the SG ARVs are unavailable, then the SG SRVs will be demanded. If these valves are challenged, they need to reclose after SG pressure falls below their set-points. A stuck open ARV or SRV will result in a consequential secondary-side break upstream of the MSIVs.[192]

SVC Fault Tree Use. This top event fault tree is used in most transient event trees.

5.1.45 Terminate Safety Injection (TSI)

Description. Since the pump head for CCPs is higher than the set-points of the pressurizer PORVs and SRVs, the CCPs will pressurize the RCS after inadvertent SI actuation. If the CCPs are not stopped by the operators, the pressurizer PORVs will open. If the PORVs fail to open, the SRVs will open. Operator action (OAT----------H) is required to terminate SI (especially the tripping of the CCPs) to prevent loss of RCS inventory through the pressurizer valves. If the operators successfully terminate SI, the pressurizer PORVs and SRVs should reclose (if they had opened). If a PORV or SRV does not reclose, a consequential LOCA occurs.

TSI Fault Tree Use. This top event fault tree is used in the inadvertent SI event tree.

5.1.46 Turbine Trip (TT)

Description. After reactor trip, the main turbine should be tripped to prevent overcooling of the RCS. For successful turbine trip, all four steam supply lines to the high-pressure turbine need to be isolated after the reactor trip by closing either the control valve or the main stop valve in each line. The failure of the turbine to trip leads to a consequential SSB downstream of the MSIVs. If the turbine successfully trips, the TBVs will be demanded (if available). The failure of a TBV to reclose also results in a consequential SSB downstream of the MSIVs.[193]

---

[191] The SRVs will open if the PORVs fail to open.

[192] The modeling of consequential SSB due to the failure of a single SG ARV or SRV to reclose is potentially conservative. Results indicate that this modeling assumption has only a minor impact on the overall CDF.

[193] The modeling of consequential SSB due to the failure of a single TBV to reclose is potentially conservative. Results indicate that this modeling assumption has only a minor impact on the overall CDF.

TT Fault Tree Use. This top event fault tree is used in most transient-type event trees.

Additional System Fault Trees. The following fault tree for turbine trip is also used in the L3PRA project Level 1 model.

5.1.46.1 Turbine Trip during ATWS (TT-ATWS)

Description. If an ATWS occurs with failure of MFW, the turbine must trip to prevent SG dry out. The AMSAC system is credited to automatically trip the turbine given a loss of MFW with reactor power greater than 40 percent.[194] In addition, if the reactor trip failure is due to the mechanical failure of the control rods to insert into the core, then the normal turbine trip signal is also assumed to be available because the RTBs will be open. Since trip signal failures dominate the results (as shown by the TT fault tree), the failure of the stop and control valves has not been included in the TT-ATWS fault tree.

TT-ATWS Fault Tree Use. This top event fault tree is used in the ATWS event tree.

5.2 Key Support Systems

The fault tree descriptions that follow are for key systems that provide support (e.g., electrical power, cooling water, service air, etc.) to systems described in Section 5.1 of this report. The support systems that result in an immediate or subsequent reactor trip are modeled as top event SSIE fault trees (though some of these support system failures may not result in a reactor trip for some time after the failure (e.g., operators have until battery depletion to restore a safety-related 4.16 kV AC bus prior to reactor trip). The support system aspects of these key systems (i.e., the use of these systems to support plant response to an initiating event) are modeled in fault trees that are not event tree top events and are linked to the system fault trees they support.

5.2.1 125 V DC Power

Description. The 125 V DC power system is required to start various equipment, open/close circuit breakers, and control and operate various valves. There are four safety-related 125 V DC systems per unit (A, B, C, and D). Each system has a lead-calcium battery, switchgear, two redundant battery chargers, two inverters, and 125 V DC distribution panels (molded case circuit breakers). Systems A, B, and C each have a 125 V DC motor control center for MOVs. There is no capability to connect the four DC systems between themselves, between Units 1 and 2, or between the safety-related and nonsafety-related systems.

The safety-related 125 V DC systems A, B, C, and D supply DC power to channels 1, 2, 3, and 4, respectively, and are designated as Class 1E equipment in accordance with the applicable sections of Institute of Electrical and Electronic Engineers (IEEE) 308-2012, “Standard Criteria for Class 1E Power Systems for Nuclear Power Generating Stations,” (IEEE, 2013). They are designed so that no single failure in any 125 V DC system will result in conditions that will prevent the safe shutdown of the reactor plant. All the components of the safety-related 125 V DC systems are housed in category 1 structures.

[194] The AMSAC system is credited in the TT-ATWS fault tree, but not credited in the TT fault tree as a modeling simplification.

The safety-related batteries have sufficient capacity to supply the required loads for 4 hours in a SBO following shedding of non-essential loads.[195] Each safety-related 125 V DC battery is provided with two battery chargers, each of which is sized to supply the continuous (long-term) demand on its associated DC system while providing sufficient power to replace 110 percent of the equivalent ampere-hours removed from the battery during a design basis battery discharge cycle within a 12-hour period after charger input power is restored. A single battery charger can handle the loads if the battery and the other battery charger are unavailable.

Each 125 V DC MCC supplies power to safety-related MOVs. The safety-related 125 V DC distribution panels supply power for ESF control, switching, and field flashing for the EDGs. The safety-related 125 V DC bus C provides all power required for successful operation of the turbine-driven AFW pump, except for the SG-to-AFW turbine MOVs (redundant valves) that are provided power from the DC system A and B MCCs.

The loss of safety-related 125 V DC bus A or B causes a main steam line and MFW line isolation; therefore, they are modeled as special initiating events. The loss of safety-related DC bus C or D does not lead to a reactor trip; therefore, they are not included as special initiating events.

SSIE Fault Trees. The following SSIE fault trees for the special initiating events associated with the 125 V DC power system are used in the L3PRA project Level 1 model:

5.2.1.1 Loss of Safety-Related 125 V DC Bus A (IEFT-LO125AD1)

Description. Loss of safety-related 125 V DC bus A will cause a reactor trip when train A MSIVs and MFIVs fail closed due to loss of their control power.

IEFT-L0125AD1 Fault Tree Use. This fault tree is the SSIE fault tree for the frequency of loss of safety-related 125 V DC bus A.

5.2.1.2 Loss of Safety-Related 125 V DC Bus B (IEFT-LO125BD1)

Description. Loss of safety-related 125 V DC bus B will cause a reactor trip when train B MSIVs and MFIVs fail closed due to loss of their control power

IEFT-L0125BD1 Fault Tree Use. This fault tree is the SSIE fault tree for the frequency of loss of safety-related 125 V DC bus B.

Key Support System Fault Trees. The following key support system fault trees associated with the 125 V DC system are used in the L3PRA project Level 1 model:[196]

---

[195] In the L3PRA Level 1 model, the time available for AC power recovery is limited by the 2-hour depletion time of the nonsafety-related turbine building batteries. Therefore, it is assumed that operator action is not required to shed non-essential loads from the safety-related batteries.

[196] The loss of the safety-related 125 V DC bus D is not described in this section because it was not determined to be a key system.

5.2.1.3 Loss of Safety-Related 125 V DC Bus A (DC-125VSWG-AD1)

Description. In addition to causing a reactor trip (due to the main steam line and MFW line isolation), a loss of safety-related 125 V DC bus A will cause the loss of power to two safety-related train A power 125 V DC supply panels and one safety-related Train B MCC.

DC-125VSWG-AD1 Fault Tree Use. This support system fault tree models the loss of safety-related 125 V DC bus A.

5.2.1.4 Loss of Safety-Related 125 V DC Bus B (DC-125VSWG-BD1)

Description. In addition to causing a reactor trip (due to the main steam line and MFW line isolation), a loss of safety-related 125 V DC bus B will cause the loss of power to two safety-related train B power 125 V DC supply panels and one safety-related train B MCC.

DC-125VSWG-BD1 Fault Tree Use. This support system fault tree models the loss of safety-related 125 V DC bus B.

5.2.1.5 Loss of Safety-Related 125 V DC Bus C (DC-125VSWG-CD1)

Description. The loss of safety-related 125 V DC bus C will not cause a reactor trip; however, the loss of bus C will cause the loss of its associated inverter, resulting in the unavailability of the turbine-driven AFW pump (due to loss of several turbine-driven AFW valves) and an RHR loop isolation MOV.

DC-125VSWG-CD1 Fault Tree Use. This support system fault tree models the loss of safety-related 125 V DC bus C.

5.2.2 120 V AC Power

Description. The 120 V AC distribution system provides instrument and control power for the RPS, ESF system controls and indication, and the process instrumentation and control system. Four independent safety-related 120 V AC power supplies are provided to supply the four channels of the protection systems and reactor control systems. Each safety-related instrument AC power supply consists of an inverter and a distribution panel. Trains A and B are provided with two inverters and two distribution panels. Each distribution panel has two incoming breakers that are interlocked so that only one breaker can be closed at a time. The normally closed breaker is the inverter supply. The normally open breaker is the backup supply from a 480/120 V regulated transformer. Normally, the inverter is operating to supply the safety-related AC bus. Each inverter is supplied by the 125 V DC system. If an inverter is inoperable or is to be removed from service, the safety-related AC bus can be supplied from the backup supply (480/120 V regulated transformer) associated with the same load group by the operator repositioning the distribution panel input breakers.

The loss of a single safety-related 120 V AC panel will require the operators to perform a controlled manual shutdown if it cannot be reenergized within 2 hours. Manual shutdowns of this nature are not included in the L3PRA project Level 1 model.[197] Loss of two safety-related

[197] Events that lead to the need for operators to initiate a manual reactor trip (as opposed to a controlled manual shutdown), such as a loss of ACCW or NSCW are included in the L3PRA Project Level 1 model.

120 V AC panels will cause a reactor trip due to the loss of 2 of 4 solid state protection system (SSPS) channels. The most severe initiating event occurs if the panels A and B fail because all ESFAS slave relays are lost.

SSIE Fault Trees. The following SSIE fault trees for the special initiating events associated with the loss of two safety-related 120 V AC panels are used in the L3PRA project Level 1 model:

5.2.2.1 Loss of Safety-Related 120 V AC Panels A and B (IEFT-LO120VAB)

Description. The loss of safety-related 120 V AC panels A and B will cause a reactor trip due to the loss of 2 of 4 SSPS channels (channels 1 and 2). Loss of panels A and B will also cause loss of power to the ESFAS train A and B slave relays; nuclear instrumentation system (NIS) channels 1 and 2 instrumentation and control; and process rack protection sets 1 and 2.

IEFT-LO120VAB Fault Tree Use. This fault tree is the SSIE fault tree for the frequency of the loss of safety-related 120 V AC panels A and B.

5.2.2.2 Loss of Safety-Related 120 V AC Panels A and C (IEFT-LO120VAC)

Description. The loss of safety-related 120 V AC panels A and C will cause a reactor trip due to the loss of 2 of 4 SSPS channels (channels 1 and 3). Loss of panels A and C will also cause loss of power to the ESFAS train A; NIS channels 1 and 3 instrumentation and control; process rack protection sets 1 and 3; and the turbine-driven AFW pump speed controller.

IEFT-LO120VAC Fault Tree Use. This fault tree is the SSIE fault tree for the frequency of the loss of safety-related 120 V AC panels A and C.

5.2.2.3 Loss of Safety-Related 120 V AC Panels A and D (IEFT-LO120VAD)

Description. The loss of safety-related 120 V AC panels 1AY1A and 1DY1B will cause a reactor trip due to the loss of 2 of 4 SSPS channels (channels 1 and 4). Loss of panels A and D will also cause loss of power to the ESFAS train A, NIS channels 1 and 4 instrumentation and control; and process rack protection sets 1 and 4.

IEFT-LO120VAD Fault Tree Use. This fault tree is the SSIE fault tree for the frequency of the loss of safety-related 120 V AC panels A and D.

5.2.2.4 Loss of Safety-Related 120 V AC Panels B and C (IEFT-LO120VBC)

Description. The loss of safety-related 120 V AC panels B and C will cause a reactor trip due to the loss of 2 of 4 SSPS channels (channels 2 and 3). Loss of panels B and C will also cause loss of power to the ESFAS train B slave relays; NIS channels 2 and 3 instrumentation and control; process rack protection sets 2 and 3; and the turbine-driven AFW pump speed controller.

IEFT-LO120VBC Fault Tree Use. This fault tree is the SSIE fault tree for the frequency of the loss of safety-related 120 V AC panels B and C.

5.2.2.5 Loss of Safety-Related 120 V AC Panels B and D (IEFT-LO120VBD)

Description. The loss of safety-related 120 V AC panels B and D will cause a reactor trip due to the loss of 2 of 4 SSPS channels (channels 2 and 4). Loss of panels B and D will also cause loss of power to the ESFAS train B slave relays; NIS channels 2 and 4 instrumentation and control; and process rack protection sets 2 and 4.

IEFT-LO120VBD Fault Tree Use. This fault tree is the SSIE fault tree for the frequency of the loss of safety-related 120 V AC panels B and D.

5.2.2.6 Loss of Safety-Related 120 V AC Panels C and D (IEFT-LO120VCD)

Description. The loss of safety-related 120 V AC panels C and D will cause a reactor trip due to the loss of 2 of 4 SSPS channels (channels 3 and 4). Loss of panels C and D will also cause loss of power to the NIS channels 3 and 4 instrumentation and control; process rack protection sets 3 and 4; and the turbine-driven AFW pump speed controller.

IEFT-LO120VCD Fault Tree Use. This fault tree is the SSIE fault tree for the frequency of the loss of safety-related 120 V AC panels C and D.

Key Support System Fault Trees. The following key support system fault trees associated with the 120 V AC system are used in the L3PRA project Level 1 model:

5.2.2.7 Loss of Safety-Related 120 V AC Panel A (AC-120VPNL-AY1AL)

Description. The loss of safety-related 120 V AC panel A will cause the loss of power to SSPS channel 1 trains A and B; ESFAS train A slave relays; NIS channel 1 instrumentation and control; and process rack protection set 1

AC-120VPNL-AY1AL Fault Tree Use. This support system fault tree models the loss of safety-related 120 V AC panel A.

5.2.2.8 Loss of Safety-Related 120 V AC Panel B (AC-120VPNL-BY1BL)

Description. The loss of safety-related 120 V AC panel B will cause the loss of power to SSPS channel 2 trains A and B; ESFAS train B slave relays; NIS channel 2 instrumentation and control; and process rack protection set 2.

AC-120VPNL-BY1BL Fault Tree Use. This support system fault tree models the loss of safety-related 120 V AC panel B.

5.2.3 480 V AC Power

Description. The 480 V AC power system functions to distribute electrical power to the safety-related and nonsafety-related 480 V loads. These loads consist of valve motor operators and other motors rated less than 200 hp. The 480 V AC power system also supplies power to the 125 V DC systems through battery chargers, and to the 120 V instrument AC power systems through regulated transformers. The 480 V AC power system is divided into safety-related and nonsafety-related systems. All safety-related 480 V AC buses and two of the nonsafety-related 480 V AC buses receive power from the safety-related 4.16 kV AC buses.

There are two divisions of safety-related 480 V AC buses, with three buses in each division. There are 12 Class 1E safety-related 480 V MCCs. The two non-Class 1E 480 V AC buses supplied from the safety-related 4.16 kV AC buses, will automatically disconnect from the safety-related system on under-voltage (i.e., LOOP) or safety injection. They will sequence back on during a LOOP event; during an SI event they can be manually reconnected to the safety-related 4.16 kV AC buses under administrative procedure. The important loads fed from these non-Class 1E 480 V AC buses include the EDG starting air compressors, the pressurizer heater panels, the containment building cavity cooling fans, and the main turbine turning gear (transfer switch).

SSIE Fault Trees. There are no SSIE fault trees associated with loss of 480 V AC buses because their loss will not result in a reactor trip.

Key Support System Fault Trees. The following key support system fault trees associated with the safety-related 480 V AC system are used in the L3PRA project Level 1 model:

5.2.3.1 Loss of Safety-Related 480 V AC Bus 1AB04 (AC-480VBUS-AB04)

Description. The loss of safety-related 480 V AC bus 1AB04 will also result in the loss of 480 V AC MCC 1ABE.

AC-480VBUS-AB04 Fault Tree Use. This support system fault tree models the loss of safety-related 480 V AC bus AB04.

5.2.3.2 Loss of Safety-Related 480 V AC Bus 1AB05 (AC-480VBUS-AB05)

Description. The loss of safety-related 480 V AC bus 1AB05 will also result in the loss of 480 V AC MCCs 1ABA, 1ABC, and 1ABF.

AC-480VBUS-AB05 Fault Tree Use. This support system fault tree models the loss of safety-related 480 V AC bus AB05.

5.2.3.3 Loss of Safety-Related 480 V AC Bus 1AB15 (AC-480VBUS-AB15)

Description. The loss of safety-related 480 V AC bus 1AB15 will also result in the loss of 480 V AC MCCs 1ABB and 1ABD.

AC-480VBUS-AB15 Fault Tree Use. This support system fault tree models the loss of safety-related 480 V AC bus AB15.

5.2.3.4 Loss of Safety-Related 480 V AC Bus 1BB06 (AC-480VBUS-BB06)

Description. The loss of safety-related 480 V AC bus 1BB06 will also result in the loss of 480 V AC MCC 1BBE.

AC-480VBUS-BB06 Fault Tree Use. This support system fault tree models the loss of safety-related 480 V AC bus BB06.

5.2.3.5 Loss of Safety-Related 480 V AC Bus 1BB07 (AC-480VBUS-BB07)

Description. The loss of safety-related 480 V AC bus 1BB07 will also result in the loss of 480 V AC MCCs 1BBA, 1BBC, and 1BBF.

AC-480VBUS-BB07 Fault Tree Use. This support system fault tree models the loss of safety-related 480 V AC bus BB07.

5.2.3.6 Loss of Safety-Related 480 V AC Bus 1BB16 (AC-480VBUS-BB16)

Description. The loss of safety-related 480 V AC bus 1BB16 will also result in the loss of 480 V AC MCCs 1BBB and 1BBD.

AC-480VBUS-BB16 Fault Tree Use. This support system fault tree models the loss of safety-related 480 V AC bus BB16.

5.2.4 4.16 kV AC Power

Description. There are thirteen 4.16 kV AC buses, between both units, included in the L3PRA project Level 1 model that receive power from both the UATs and RATs. The 4.16 kV buses are further divided into two safety-related buses per unit and nine nonsafety-related buses that distribute power to safety-related and nonsafety-related loads throughout the plant. During operation, the nonsafety-relate 4.16 kV AC system can be supplied from the RAT or the UAT.

Normally, the UATs supply the nonsafety-related system loads, and the RATs supply the safety-related buses. The safety-related electrical systems are laid out for maximum physical and electrical separation to increase system reliability and to ensure that no single credible accident will cause a loss of more than one safety-related power source. The safety-related 4.16 kV AC electrical system is totally redundant so that if a complete loss of one safety-related electrical division occurs, the remaining division will supply all redundant safety related equipment to ensure safe reactor shutdown and decay heat removal.

Each safety-related 4.16 kV AC bus is equipped with feeder breakers from the RAT and the EDGs; no connections exist between units for the safety-related buses. Upon a loss of voltage on the safety-related 4.16 kV buses, each bus will shed its loads, and the RAT feeder breakers to the safety-related buses will trip (open). Under-voltage on the safety-related 4.16 kV AC buses will automatically start the train-associated EDG and close its output breaker to re-energize the bus. After the bus has been re-energized, the safety-related loads will be sequenced onto the buses by the safeguards sequencer.

SSIE Fault Trees. The loss of 4.16 kV AC bus initiating event frequency is generated from data using the RADS calculator. Therefore, no SSIE fault tree was developed for this initiating event scenario (as discussed in Section 2.3).

Key Support System Fault Trees. The following key support system fault trees associated with the 4.16 kV AC system are used in the L3PRA project Level 1 model:

5.2.4.1 Loss of 4.16 kV AC Bus A (ACP-4KV-AA02)

Description. The loss of safety related 4.16 kV bus A will cause loss of power to its associated 480 V switchgears and MCCs that results in the unavailability of the train A ESF equipment. In

addition, loss of this bus will cause the unavailability of the train A and C battery chargers that will lead to the eventual loss of safety-related 125 V DC buses, once their batteries deplete (in approximately 4 hours). The loss of safety-related 125 V DC bus C results in the loss of the turbine-driven AFW pump. The potential for a consequential LOOP following a reactor trip (with or without) an SI actuation is explicitly modeled in this fault tree. See Section 8.2 for additional information.

ACP-4KV-AA02 Fault Tree Use. This support system fault tree models the loss of safety-related 4.16 kV AC bus A.

5.2.4.2 Loss of Safety-Related 4.16 kV AC Bus B (ACP-4KV-BA03)

Description. The loss of safety-related 4.16 kV bus B will cause loss of power to it associated 480 V switchgears and MCCs that results in the unavailability of the train B ESF equipment. In addition, the unavailability of train B and C battery chargers that will lead to the eventual loss of safety-related 125 V DC buses B and D, once their batteries deplete (in approximately 4 hours). The potential for a consequential LOOP following a reactor trip (with or without) an SI actuation is explicitly modeled in this fault tree. See Section 8.2 for additional information.

ACP-4KV-BA03 Fault Tree Use. This support system fault tree models the loss of safety-related 4.16 kV AC bus 1BA03.

5.2.5 Auxiliary Component Cooing Water

Description. Each unit's ACCW system consists of two 100 percent-capacity ACCW heat exchangers, two 100 percent-capacity ACCW pumps, one ACCW surge tank, and associated piping, valves, and instrumentation. The ACCW heat exchangers are horizontal, shell and tube, single pass, counter-flow type. The ACCW pumps are horizontal, centrifugal type. Motor cooling is provided by an air to water heat exchanger supplied by the discharge of the ACCW pumps. Each ACCW pump is powered from a separate safety-related 4.16 kV AC bus.

The ACCW surge tank is a horizontal, cylindrical tank with a capacity sufficient to ensure that the system is kept filled and pump net positive suction head (NPSH) requirements are maintained. The surge tank is connected to the main ACCW line on the suction side of the ACCW pumps. Makeup water is added to the surge tank as required from the demineralized makeup water system (normal source), the reactor makeup water system, or the component cooling water drain tank.

The ACCW system is designed so that the system can operate with either heat exchanger or pump in operation. The two ACCW heat exchangers are aligned in series and either will satisfy 100 percent of the ACCW cooling requirements. Each ACCW heat exchanger is in turn cooled by one NSCW train, one of which is always in service. Thus, ACCW cooling is available regardless of which NSCW train is in service. One ACCW pump is operated during normal operation. The second pump is in a standby mode of operation and is started upon low system pressure. These pumps are swapped in and out of service to equalize run times.

The ACCW system is essentially a closed loop system that circulates cooling water to the following components:

- NCP motor cooler

- Letdown heat exchanger, excess letdown heat exchanger, and seal water heat exchanger

- RCP motor area coolers, thermal barrier heat exchangers, and lube oil coolers

- Miscellaneous components such as sampling system coolers

A loss of a single train of ACCW will not cause a reactor trip and was not considered as a special initiating event. However, upon a total loss of ACCW to the RCPs (thermal barrier heat exchanger and motor area coolers), the RCPs must be shutdown (and the reactor manually tripped) within 10 minutes or sooner if the RCP temperature limits are exceeded for the RCP motor bearing, RCP stator winding, or RCP seal water inlet.

With the loss of all ACCW, the RCP seals will lose all cooling and injection. Operators have approximately 13 minutes to align a CCP for seal injection to prevent a challenge to the RCP seals (and potential LOCA).[198]

Required Support Systems. The following support systems are required for successful operation of the ACCW system:

- AC power is required for motive power to the pump motors and valve operators. DC power is required for control power.

- The NSCW system provides cooling water to the tube side of the ACCW heat exchangers. Train A supplies ACCW heat exchanger 1, while train B supplies ACCW heat exchanger 2. The ACCW system is designed with lower pressures than the NSCW system to prevent potential radioactive leakage into the NSCW system.

- The ESFAS system provides signals to start the ACCW pumps and close or open valves.

- The ACCW system has three sources of makeup supply water. These three sources are the demineralized makeup water system (normal source), the reactor makeup water system, or the component cooling water drain tank. All three sources are available for use in maintaining surge tank levels during normal system operation and during emergency operation involving a loss of water.

- The ACCW pump rooms are served by nonsafety-related systems that are parts of the auxiliary building normal ventilation system that provide the supply to and exhaust from the rooms. The ACCW heat exchanger rooms are also served by these systems. However, based on a room heat-up analysis, the ACCW pump rooms would remain below the temperature that would result in failure of the pumps for 24 hours without room cooling. Therefore, the loss of ACCW pump room HVAC is not modeled in the L3PRA Level 1 model.

[198] Credit for aligning a CCP as an alternate source of RCP seal injection is only modeled in the Loss of ACCW and the Loss of RCP Seal Injection Event Trees. See Section 5.1.25 for additional information.

SSIE Fault Tree. The following SSIE fault tree for the special initiating event for a loss of ACCW is used in the L3PRA project Level 1 model:

5.2.5.1 Loss of ACCW (IEFT-LOACCW)

Description. A loss of both ACCW trains will cause a loss of cooling to RCPs and operators will have to secure the RCPs and manually trip the reactor within 10 minutes or sooner if the RCP temperature limits are exceeded. A loss of all ACCW also results in loss of RCP seal cooling and injection.

IEFT-LOACCW Fault Tree Use. This fault tree is the SSIE fault tree for the frequency of the loss of ACCW.

Key Support System Fault Tree. The following key support system fault tree associated with the ACCW system is used in the L3PRA project Level 1 model:

5.2.5.2 Insufficient Flow or Cooling from ACCW System (ACCWT)

Description. Failure of both trains of ACCW results in loss of cooling to the RCP thermal barrier heat exchangers. In addition, cooling will be lost to the NCP that provides the normal supply of injection to the RCPs seals.

ACCWT Fault Tree Use. This support system fault tree models the loss of both trains of ACCW.

5.2.6 Instrument Air

Description. The instrument air system is part of the compressed air system and provides filtered, dry, oil-free air to be used as the motive force for operating pneumatic equipment throughout the plant. The reference plant is designed such that no plant equipment relies upon the compressed air system to perform its safety function and thus there is no safety design basis for the instrument air system. Although the instrument air system is not safety related, proper operation of the plant is dependent on its availability. The key SSCs that instrument air supplies include the MSIVs, MFIVs, TBVs, and the CST makeup valve from the demineralizer water system.

Each unit has two rotary compressors and one reciprocating compressor (Unit 1 has two reciprocating air compressors, one dedicated to Unit 1 and the other a swing unit), each with its own support equipment (aftercooler/moisture separator, and air receiver). They are each equipped with safety trip instrumentation (high lube temperature, low cooling water pressure, and high air/coolant receiver temperature). The rotary compressors can be started manually by a master control switch on the main control panel or can be set on AUTO for control by the local master controller. An emergency stop push button is located on each compressor. Compressor oil coolers are cooled by the TPCCW system. The reciprocating compressors are two-stage piston compressors. Each compressor motor is designed to trip on high intercooler condensate level, high lube oil temperature, low oil pressure, high discharge air pressure, or high discharge air temperature.

There are two types of mechanical aftercooler/separators that remove both moisture and oil. The aftercooler sections consist of a straight-through tube heat exchanger with air on the tube side and TPCCW system water on the shell side. The air receivers are pulsation-dampening chambers and provide no significant storage capacity. Contaminant filters are located on each

rotary compressor head between the moisture separator and the air receiver to ensure that any lubricant escaping the compressor does not enter the air header system. Each stage has a differential pressure switch to indicate a dirty filter by an indicating light on the filter. The instrument air dryers are the regenerative, desiccant type which provides outlet air dried to -100°F dew point at 120 psi. A single air dryer can handle the expected instrument air system capacity without overflow. Overflow is indicated by a high differential pressure using inlet and outlet pressure gages or by a high-humidity alarm. If this occurs, both dryers are required to be in operation.

Required Support Systems. The following support systems are required for successful operation of the instrument air system:

- AC power is required for the compressors.
- TPCCW provides cooling water to the compressors.

SSIE Fault Tree. The following SSIE fault tree for the special initiating event for a loss of instrument air is used in the L3PRA project Level 1 model:

5.2.6.1 Loss of Instrument Air System (IEFT-LOIAS)

Description. A loss of turbine building instrument air will cause all extraction steam stop valves to close, all feedwater heater high-level dump valves to fail fully open, and all MFRVs (and bypass valves) to close, resulting in a reactor trip on low SG water level.

IEFT-LOIAS Fault Tree Use. This fault tree is the SSIE fault tree for the frequency of the loss of instrument air.

Key Support System Fault Tree. The following key support system fault tree associated with the instrument air system is used in the L3PRA project Level 1 model:

5.2.6.2 Instrument Air System Fails (IAS)

Description. For instrument air system to fail, all four compressor trains must fail.

IAS Fault Tree Use. This support system fault tree models the loss of all four instrument air trains.

5.2.7 Nuclear Service Cooling Water

Description. The NSCW system is composed of two redundant, completely independent, full capacity flow trains comprised of cooling towers, pumps, piping, and valves. There are six train-oriented NSCW pumps per unit. Four of these pumps, two on each train, are running during normal operation. Two pumps, one on each train, are in standby during normal operation.[199]

[199] The L3PRA Project Level 1 model assumes that pumps 1–4 are running with pumps 5 and 6 in standby. Therefore, the test/maintenance for pumps 1–4 are not included in the applicable NSCW fault trees. In addition to the test/maintenance events for the standby pumps, the applicable NSCW fault trees also include the potential that all three NSCW pumps for a single train are unavailable due to test/maintenance.

The success of each NSCW train requires the operation of two of three pumps, though operator action (to strip loads) can be used to implement one pump operation (OA-OSW-------H).

The NSCW pumps take suction from the train-oriented cooling tower basins that have the combined capacity to provide cooling water under the worst-case heat load (design basis accident with LOOP and power supplied by the EDGs) for well beyond the PRA mission time; therefore, makeup to the cooling tower basins is not modeled in the L3PRA project Level 1 model.

The NSCW cooling towers are the ultimate heat sinks for the plant. After removing heat from the components that it serves, NSCW combines in a common train-oriented return header that has a return valve that operates in conjunction with a tower bypass valve for temperature control of the NSCW system. The cooling towers are not needed in cold weather conditions. The bypass valve will automatically open and the return valve will close as the return header temperature falls to below a design temperature. When the bypass valve is open, the tower is completely bypassed, and the return water goes directly into the cooling tower basin. Bypassing the cooling tower raises the temperature of the NSCW system. When the return header temperature increases past a design temperature, the return isolation valve opens, and the bypass valve closes and the normal flow path through the cooling tower is re-established.

Each train-oriented NSCW cooling tower has four fans, each of which automatically starts at a different NSCW return water temperature. One fan in each train-oriented tower is cycled on and off with return valve position.[200] When the tower is bypassed as described above the fans are not needed. The other three fans are cycled according to the NSCW return header temperature. As temperature decreases the fans that start at higher temperatures automatically stop.

The following components are served by the NSCW system:

- CCW motor coolers
- CCP oil coolers and motor coolers
- SI pump oil coolers and motor coolers
- Containment spray pump motor coolers
- RHR pump motor coolers
- ESF chiller condensers
- CCUs
- Reactor cavity cooling coils

[200] The L3PRA Level 1 model assumes that fan 1 is running in each NSCW cooling tower with the other fans in standby. Therefore, the test/maintenance for fan 1 is not included in the applicable NSCW fault trees. Note that the applicable NSCW fault trees also include the potential that all four NSCW fans are unavailable due to test/maintenance.

- Containment auxiliary air coolers
- EDG jacket water coolers
- Control building, auxiliary building, and diesel building seismic fire hose stations
- CCW heat exchangers
- ACCW heat exchangers
- Piping penetration area coolers

Required Support Systems. The following support systems are required for successful operation of the NSCW system:

- AC power is required for motive power to the pump motors, valve operators, and cooling tower fans. DC power is required for control power.
- The ESFAS system provides signals to start the NSCW pumps and close or open valves.[201] The blowdown path isolates along with the containment building auxiliary coolers and reactor cavity cooling coil. All containment cooler valves receive an open signal.
- Instrument air is used to control the water level in the cooling towers. Level in the tower is converted directly into a pneumatic signal by individual level transmitters, one for tower A and one for tower B. This air signal is amplified by a locally mounted air-operated controller, then sent to position the makeup valves from the well water storage tank.

SSIE Fault Tree. The following SSIE fault tree for the special initiating event for a loss of NSCW is used in the L3PRA project Level 1 model:

5.2.7.1 Loss of NSCW System (IEFT-NSCW)

Description. If a loss of NSCW occurs in both trains, the operator will trip the reactor, trip all RCPs, isolate chemical and volume control system (CVCS) letdown, and then attempt to place one train of NSCW in single-pump operation (as represented by the HFE OA-OSW-------H). The RCPs and CVCS letdown represent large heat loads cooled by ACCW, which is ultimately cooled by the NSCW system. The reactor is manually tripped because the RCPs are required to be tripped due to a loss of cooling. Stopping the RCPs will generate an automatic reactor trip signal if reactor power is above 10 percent. Note that the IEFT-NSCW fault tree only considers the loss of NSCW pump trains (including discharge MOVs and check valves) and does not consider fan or spray failures, because it is assumed that these failures will result in slower

[201] During an initiating or consequential event resulting in an SI actuation, the sequencer is assumed to send a confirmatory start signal to the running NSCW pumps (1–4); however, this start signal does not affect the running pumps. During an under-voltage condition on the buses caused by a LOOP initiating event, the running NSCW pumps are stripped off the buses and restarted. Given these assumptions, the applicable NSCW fault tree logic for the running pumps does not include start-related failures during an SI without a LOOP initiating event. However, the failure-to-start logic is included during a LOOP initiating event. As a modeling simplification, the NSCW fault tree logic does not consider consequential LOOP events.

system heat-up and lead to a technical specification directed, controlled shutdown, instead of a reactor trip.[202]

IEFT-LONSCW Fault Tree Use. This fault tree is the SSIE fault tree for the frequency of the loss of NSCW.

Key Support System Fault Trees. The following key support system fault trees associated with the NSCW system are used in the L3PRA project Level 1 model:

5.2.7.2 NSCW Train A Fails (NSCW-TRAIN A)

Description. The failure of NSCW train A will cause the loss of most of the train A ESF equipment required during an SI actuation. Note that for initiating and consequential events that require an SI actuation, the success criterion for the NSCW pumps requires 2 of 3 pumps per train and the success criterion for NSCW fans requires 3 of 4 fans per train. If NSCW is lost to the train A ESF components, the expectation is that most of this equipment will fail quickly.

NSCW-TRAIN A Fault Tree Use. This support system fault tree models the loss of NSCW train A for most ESF systems required given an SI actuation.

5.2.7.3 NSCW Train B Fails (NSCW-TRAIN-B)

Description. The failure of NSCW train B will cause the loss of most of the train B ESF equipment required during an SI actuation. Note that for initiating and consequential events that require an SI actuation, the success criterion for the NSCW pumps requires 2 of 3 pumps per train and the success criterion for NSCW fans requires 3 of 4 fans per train. If NSCW is lost to the train B ESF components, the expectation is that most of this equipment will fail quickly.

NSCW-TRAIN-B Fault Tree Use. This support system fault tree models the loss of NSCW train B for most ESF systems required given an SI actuation.

5.2.7.4 NSCW Train A Fails (NSCW-TRAIN-A-PRESI)

Description. In the absence of an event requiring an SI actuation, the failure of both NSCW trains will cause the subsequent loss of ACCW that results in the loss of RCP thermal barrier heat exchanger cooling and loss of normal RCP seal injection (via the NCP). In addition, the loss of NSCW train A will render CCP A unavailable to supply alternate charging and RCP seal injection. Note that the success criterion for the NSCW fans requires 1 of 4 fans per train if no SI actuation has occurred (the pump criterion remains 2 out of 3 pumps per train).

NSCW-TRAIN-A-PRESI Fault Tree Use. This support system fault tree models the loss of NSCW train A for the ACCW system and CCP A (for alternate charging and RCP seal injection).

5.2.7.5 NSCW Train B Fails (NSCW-TRAIN-B-PRESI)

Description. In the absence of an event requiring an SI actuation, the failure of both NSCW trains will cause the subsequent loss of ACCW that results in causes the loss of RCP thermal

[202] The NSCW SSIE fault tree only includes pump CCF events involving four or more pumps, which corresponds to the largest CCF event that is minimal with respect to the system success criteria. See Section 7.3.3 for additional information.

barrier heat exchanger cooling and loss of normal RCP seal injection (via the NCP). In addition, the loss of NSCW train A will render CCP B unavailable to supply alternate charging and RCP seal injection. Note that the success criterion for the NSCW fans requires 1 of 4 fans per train if no SI actuation has occurred (the pump criterion remains 2 out of 3 pumps per train).

NSCW-TRAIN-A-PRESI Fault Tree Use. This support system fault tree models the loss of NSCW train B for the ACCW system and CCP B (for alternate charging and RCP seal injection).

5.2.7.6 NSCW Train A Fails Following a LOOP (NSCW-TRA-LOSPL)

Description. During a LOOP initiating event with no SI actuation, the loss of NSCW train A will render EDG A unavailable causing a loss of all train A ESF equipment. Note that given a LOOP with no SI actuation, the NSCW success criteria are 2 of 3 pumps and 1 of 4 fans per train.

NSCW-TRA-LOSPL Fault Tree Use. This support system fault tree models the loss of NSCW train A for EDG A.

5.2.7.7 NSCW Train B Fails Following a LOOP (NSCW-TRA-LOSPL)

Description. During a LOOP initiating event with no SI actuation, the loss of NSCW train B will render EDG B unavailable causing a loss of all train B ESF equipment. Note that given a LOOP with no SI actuation, the NSCW success criteria are 2 of 3 pumps and 1 of 4 fans per train.

NSCW-TRB-LOSPL Fault Tree Use. This support system fault tree models the loss of NSCW train B for EDG B.

Table 5-1 System Dependency Matrix

		Safety-Related 4.16 kV AC Buses		125 V Safety-Related DC Buses				NSCW		CCW		ACCW		ESFAS	
Train		**1A**	**1B**	**1A**	**1B**	**1C**	**1D**	**A**	**B**	**A**	**B**	**A**	**B**	**A**	**B**
Auxiliary Feedwater	TDP					X								Note 1	
	MDP A	X		X										X	
	MDP B		X		X										X
Containment Cooling Units	001	X		X				X						X	
	002	X		X				X						X	
	003		X		X				X						X
	004		X		X				X						X
	005	X		X				X						X	
	006	X		X				X						X	
	007		X		X				X						X
	008		X		X				X						X
Emergency Diesel Generators	1A			X				X						X	
	1B				X				X						X
High-Pressure Injection	SI-A	X		X				X						X	
	SI-B		X		X				X						X
	CCP-A	X		X				X						X	
	CCP-B		X		X				X						X
High-Pressure Recirculation	SI-A	X		X				X						X	
	SI-B		X		X				X						X
	CCP-A	X		X				X						X	
	CCP-B		X		X				X						X
	LPR-A	X		X				X		X				X	
	LPR-B		X		X				X		X				X

Table 5-1 System Dependency Matrix (cont.)

		Safety-Related 4.16 kV AC Buses		125 V Safety-Related DC Buses				NSCW		CCW		ACCW		ESFAS	
Train		**1A**	**1B**	**1A**	**1B**	**1C**	**1D**	**A**	**B**	**A**	**B**	**A**	**B**	**A**	**B**
Low-Pressure Injection	A	X		X				X						X	
	B		X		X				X						X
Low-Pressure Recirculation	A	X		X				X		X				X	
	B		X		X				X		X				X
Normal Charging Pump	PDP	Note 2										Note 3			
Residual Heat Removal	A	X		X				X		X					
	B		X		X				X		X				
Auxiliary Component Cooling Water	001	X		X				X						X	
	002		X		X				X						X
Nuclear Service Cooling Water	001	X		X										X	
	002		X		X										X
	003	X		X										X	
	004		X		X										X
	005	X		X										X	
	006		X		X										X
Component Cooling Water	001	X		X				X						X	
	002		X		X				X						X
	003	X		X				X						X	
	004		X		X				X						X
	005	X		X				X						X	
	006		X		X				X						X

	Safety-Related 4.16 kV AC Buses		125 V Safety-Related DC Buses				NSCW		CCW		ACCW		ESFAS	
Train	**1A**	**1B**	**1A**	**1B**	**1C**	**1D**	**A**	**B**	**A**	**B**	**A**	**B**	**A**	**B**

Notes:

1. The turbine-driven AFW pump receives ESFAS signals from both trains.

2. The NCP is powered from 4.16 kV AC nonsafety-related bus 1NA05.

3. ACCW flows in series through the two ACCW heat exchangers, either of which will satisfy 100 percent of the system cooling requirements.

Table 5-2 System/Function Success Criteria for Top Event Fault Trees

System/Function (Fault Tree Name(s))	Applicable Event Tree(s)	General Success Criteria	Assumptions/Notes
Accumulators (ACC-M&LLOCA and ACC)	LLOCA, MLOCA, SLOCA, CSLOCA, SBO-1	For MLOCAs and LLOCAs, three accumulators (on intact RCS loops) must inject all their water. For SLOCAs, only two accumulators (on intact RCS loops) need to inject.	It is assumed that the accumulator on the failed RCS loop will dump its contents out the break; and therefore, is unavailable for success. However, for consequential SLOCAs (e.g., RCP seal failures or a stuck-open PORV/SRV), it is assumed that all four accumulators are available for injection.
Auxiliary Feedwater (AFW, AFW-LOCA, AFW-ATWS, AFW-B, AFW-ACR, and AFW-LOCA-ACR)	Transients with MFW Unavailable, SBO, ATWS	For events other than ATWS, 1 of 2 motor-driven AFW pumps or the turbine-driven AFW pump must deliver at least the minimum required flow to at least 2 of 4 SGs. Steam removal from the SGs fed with AFW is required by either: (1) three TBVs or (2) an ARV or 1 of 5 SRVs on 2 or 4 intact SGs. For an ATWS, all 3 AFW pumps must supply 4 of 4 SGs	For events in which AFW can bring the plant to a safe and stable end-state for 72 hours (i.e., non-LOCAs), CST inventory makeup must be successful. Operator action (OA-ORS-------H) is required to make the necessary AFW system restorations after AC power recovery given a SBO.

System/Function (Fault Tree Name(s))	Applicable Event Tree(s)	General Success Criteria	Assumptions/Notes
Binding/Popping Failures of RCP Seals (BP1, BP2, and RCPS-BP)	SBO	Success means that the integrity of the RCP seals remains intact. The stage 2 seals have a 0.2 probability of binding/popping failure and stage 1 seals have a 0.0125 probability of failure (according to the WOG 2000 RCP seal leakage model).	The RCPS-BP fault tree (used in the LOACCW event tree) also includes an operator action (RCS-XHE-XM-TRIP) to trip the RCPs.

Table 5-2 System/Function Success Criteria for Top Event Fault Trees (cont.)

System/Function (Fault Tree Name(s))	Applicable Event Tree(s)	General Success Criteria	Assumptions/Notes
Cooldown and Depressurization (CAD-MLOCA, CAD-ES12, CAD-FRC1, CAD-ES12-ACR, CAD-FRC1-ACR, CAD-SGTR-EARLY, and CAD-SGTR-LATE)	MLOCA, SLOCA, CSLOCA, SBO-1, SGTR	Operators must depressurize the SGs with the ARVs on 2 of 4 SGs. For SGTR scenarios, the ARVs on 2 of 3 intact SGs and the TBVs (3 of 3) are potentially available for cooldown and depressurization.	Different HFEs are used depending on the fault tree used. For CAD-SGTR-EARLY, operators must also use either the pressurizer sprays or PORVs to restore pressurizer level.
Charging (CHG, CHG-ACR)	Most Transient Initiating Events, SBO	Operators must start 1 of 2 CCPs via the normal charging path. Operators must also establish letdown.	
Condensate Storage Tank Refill (CSTR)	SGTR	Deliver an additional AFW source by switching to the second CST (manual) or to the demineralized water system (auto makeup).	CST makeup is included in the AFW fault tree for non-LOCA events.
Emergency Boration (EBR)	ATWS	Establish emergency boration flow using boric acid transfer pump to supply either the NCP or one of the CCPs from boric acid transfer tank. Injection to the RCS is via the normal charging line.	

Table 5-2 System/Function Success Criteria for Top Event Fault Trees (cont.)

System/Function (Fault Tree Name(s))	Applicable Event Tree(s)	General Success Criteria	Assumptions/Notes
Emergency Power (EPS)	All LOOP Initiating Event Categories	One of 2 dedicated EDGs to supply power to key safety-related equipment.	The EDGs require room cooling for success. The EDGs are dependent on the division batteries and division buses. The logic loop that occurs from EPS dependence on NSCW for cooling and NSCW dependence on EPS for emergency power, is broken at the NSCW dependency on emergency power.
Feed and Bleed (FAB, FAB-SLOCA, FAB-ACR, and FAB-SLOCA-ACR)	All Transient-Type Initiating Events, SLOCA, CSLOCA, SBO, SBO-1	For transient initiating events, operators must initiate feed and bleed using 1 of 2 CCPs and opening 1 of 2 PORVs. For events involving a SLOCA, operators can also initiate feed and bleed cooling using 1 of 2 SI pumps that requires both PORVs to open. Operators must trip all the RCPs before initiating feed and bleed.	Different HFEs are used depending on the fault tree used. Operator action (OA-ORS-------H) is required to make the necessary system restorations for feed and bleed cooling after AC power recovery given an SBO.

Table 5-2 System/Function Success Criteria for Top Event Fault Trees (cont.)

System/Function (Fault Tree Name(s))	Applicable Event Tree(s)	General Success Criteria	Assumptions/Notes
Feed and Bleed Recirculation (FABR, FABR-SLOCA, FABR-ACR, and FABR-SLOCA-ACR)	All Transient-Type Initiating Events, SLOCA, CSLOCA, SBO, SBO-1	One of 2 RHR pumps take suction from the containment sump and provide suction for SI pumps/CCPs. The heat sink for the recirculation water should be provided either by the CCW to an RHR heat exchanger or by 4 of 8 CCUs.	Different HFEs are used depending on the fault tree used. The HPI pump success criteria (CCPs and/or SI pumps) is conservatively assumed to be the same as that required for feed and bleed in the injection phase.
Feedwater (FW)	Transients with MFW Available	Operators must re-establish MFW flow to at least one SG from 1 of 2 MFW pumps (at least one condensate pump must be running to provide suction to MFW pumps). Steam removal from the SGs fed with MFW is required by either: (1) three TBVs or (2) an ARV or 1 of 5 SRVs for 2 of 4 SGs.	
Hot Leg Recirculation (HLR)	LLOCA	One of 2 RHR pumps inject into hot leg 1 or hot leg 4.	

Table 5-2 System/Function Success Criteria for Top Event Fault Trees (cont.)

System/Function (Fault Tree Name(s))	Applicable Event Tree(s)	General Success Criteria	Assumptions/Notes
High-Pressure Injection (HPI and HPI-ACR)	Event Trees Involving LOCAs (Except LLOCA), ATWS	For SLOCAs, 1 of 4 SIP/CCPs inject water from the RWST to 2 of 4 intact cold legs. For MLOCAs, 2 of 4 SI/CCPs inject RWST water to 2 of 3 intact cold legs).	
High-Pressure Recirculation (HPR, HPR-ACR, and HPR-ATWS)	MLOCA, SLOCA, CSLOCA, SBO-1, ATWS	One of 4 SI pumps/CCPs inject containment sump water to 2 of 4 cold legs (2 of 3 intact cold legs for MLOCAs). In addition, 1 of 2 RHR pumps take suction from the containment sump and provide suction for SI pumps/CCPs. The heat sink for the recirculation water should be provided either by CCW to a RHR heat exchanger or by 4 of 8 CCUs.	Different HFEs are used depending on the fault tree used.

Table 5-2 System/Function Success Criteria for Top Event Fault Trees (cont.)

System/Function (Fault Tree Name(s))	Applicable Event Tree(s)	General Success Criteria	Assumptions/Notes
RCP Stage 1 Seals Fail with Integrity of Stage 2 Seals Maintained (IEFT-ISL-RCP-S1LO)	ISL-RCP-S1LO	A complete loss of RCP seal injection/cooling with the subsequent failure of the stage 1 RCP seal, but with the integrity of the stage 2 seal maintained, can result in an ISLOCA via the seal leak-off line.	SSIE fault tree used to calculate the frequency of an ISLOCA in the RCP seal leak-off line. Loss of RCP seal initiating events are limited to: (1) LOOP with subsequent SBO, (2) total loss of NSCW, (3) the loss of ACCW with the failure to align the CCPs for seal injection, and (4) the loss of the normal seal injection with subsequent loss of ACCW flow to the RCP thermal barrier heat exchangers.
RHR Cold Leg Injection Train A/B Isolation Integrity (IEFT-ISL-RHR-CLI-A and IEFT-ISL-RHR-CLI-B)	ISL-RHR-CLI-A, ISL-RHR-CLI-B	Cold leg RHR system isolation check valves must isolate the low-pressure portion of the system from RCS pressure.	SSIE fault tree used to calculate the frequency of an ISLOCA in the RHR cold leg injection lines to the RCS.
RHR Hot Leg Suction Isolation Integrity (IEFT-ISL-RHR-HLS)	ISL-RHR-HLS	RHR system isolation MOVs for hot leg 1 or hot leg 4 must isolate the low-pressure portion of the system from RCS pressure.	SSIE fault tree used to calculate the frequency of an ISLOCA in the RHR hot leg suction lines to the RCS.

Table 5-2 System/Function Success Criteria for Top Event Fault Trees (cont.)

System/Function (Fault Tree Name(s))	Applicable Event Tree(s)	General Success Criteria	Assumptions/Notes
Loss of Two Safety-Related 120 V AC Panels Initiating Event (IEFT-LO120VAB, IEFT-LO120VAC, IEFT-LO120VAD, IEFT-LO120VBC, IEFT-LO120VBD, and IEFT-LO120VCD)	LO120VAB, LO120VAC, LO120VAD, LO120VBC, LO120VBD, LO120VCD	At least one of the indicated panels provides a continuous supply of safety-related 120 V AC power.	SSIE fault tree used to calculate the frequency of the loss of two safety-related 120 V AC panels.
Loss of Safety-Related 125 V DC Bus A or B Initiating Event (IEFT-LO125AD1 and IEFT-LO125BD1)	LO125AD1 LO125BD1	Bus A and B, respectively, provides a continuous supply of 125 V DC power.	SSIE fault tree used to calculate the frequency of the loss of a safety-related 125 V DC bus.
Loss of ACCW Initiating Event (IEFT-LOACCW)	Loss of ACCW	Success requires 1 of 2 pump trains and 1 of 2 heat exchangers.	SSIE fault tree used to calculate the frequency of the loss of ACCW. All dependencies are removed. The fault tree is developed to balance which pump is in standby mode.

Table 5-2 System/Function Success Criteria for Top Event Fault Trees (cont.)

System/Function (Fault Tree Name(s))	Applicable Event Tree(s)	General Success Criteria	Assumptions/Notes
Loss of Instrument Air (IEFT-LOIAS)	Loss of Instrument Air	Success requires a continuous supply of instrument air to plant loads from 1 of 4 air compressors.	SSIE fault tree used to calculate the frequency of the loss of instrument air.
Nuclear Service Cooling Water (IEFT-LONSCW)	Loss of NSCW	Success requires 2 of 3 NSCW pumps on 1 of 2 trains	SSIE fault tree used to calculate the frequency of the loss of NSCW. All dependencies are removed. Two NSCW pumps in each train are in operation while the third pump is in standby.
Loss of RCP Seal Injection (IEFT-LOSINJ)	Loss of RCP Seal Injection	A loss of normal RCP seal injection will occur if the NCP or its associated charging flow control valves, seal injection filters, or suction/discharge isolation valves fail. Operators (OA-SAGD-CHG--H) can reestablish RCP seal injection using 1 of 2 CCPs.	SSIE fault tree used to calculate the frequency of a loss of all RCP seal injection.

Table 5-2 System/Function Success Criteria for Top Event Fault Trees (cont.)

System/Function (Fault Tree Name(s))	Applicable Event Tree(s)	General Success Criteria	Assumptions/Notes
Automatic Closure of HV8100 or HV8112 Given a SI Actuation (ISL-RCP-S1LO-AUTO)	ISL-RCP-S1LO	During an ISLOCA from the RCP seal leak-off lines, the closure of HV8100 or HV8112 will limit the SLOCA to inside of containment.	These valves will close automatically due to a containment isolation signal given a SI actuation. During a SBO, automatic closure of HV8112 and HV8100 is not possible because 480 V AC power is lost; therefore, operator action (OA-IS-ISLSEALSBO) is required to manually close HV8100.
Operators Fail to Manually Close HV8141A/B/C/D (ISL-RCP-S1LO-HV8141)	ISL-RCP-S1LO	During an ISLOCA from the four RCP seal leak-off lines, operators can limit the SLOCA to inside of containment by manually closing the RCP seal leak-off return line isolation valves in each return line.	Operator action (OA-IS-ISLLKF-H) is required to manually close all four valves.
RCP Seal Leak-Off Line Relief Valve Protects Piping Integrity (ISL-RCP-S1LO-RPT)	ISL-RCP-S1LO	During an ISLOCA from the RCP seal leak-off lines, line pressure will increase above the set-point of the seal leak-off line relief valve. If this relief valve opens, RCP seal leak-off return piping will not fail; and therefore, the SLOCA will be limited to inside of containment.	

Table 5-2 System/Function Success Criteria for Top Event Fault Trees (cont.)

System/Function (Fault Tree Name(s))	Applicable Event Tree(s)	General Success Criteria	Assumptions/Notes
ISLOCA Downstream of RCP Thermal Barrier Heat Exchanger (ISL-RCP-TBHX-DNSTREAM)	ISL-RCP-TBHX	Two MOVs are available to prevent an ISLOCA downstream of a ruptured RCP thermal barrier heat exchanger. The first of these MOVs is associated with the individual RCP thermal barrier heat exchanger that could rupture. The second MOV is common to all four RCPs. If either of these MOVs close, the ISLOCA will be prevented.	Both MOVs will receive an automatic closure signal on high flow.
Operators Fail to Close HV1974 (ISL-RCP-TBHX-HV1974)	ISL-RCP-TBHX	During an ACCW system ISLOCA downstream of the ruptured RCP thermal barrier heat exchanger, HV1974 can be closed to limit the SLOCA to inside the containment.	Operator action (OA-IS-ISLACC-H) is required to manually close HV1974.
Operators Fail to Close HV1978 (ISL-RCP-TBHX-HV1978)	ISL-RCP-TBHX	During an ACCW system ISLOCA upstream of the ruptured RCP thermal barrier heat exchanger, HV1978 can be closed to limit the SLOCA to inside the containment.	Operator action (OA-IS-ISLACC-H) is required to manually close HV1978.
Relief Valves Protect Piping Integrity (ISL-RCP-TBHX-RPT)	ISL-RCP-TBHX	During a rupture of a RCP thermal barrier heat exchanger with the failure of the upstream check valves or the downstream MOVs, the ACCW supply and return lines will be pressurized. If all four relief valves open, an SLOCA will be limited to inside the containment.	

Table 5-2 System/Function Success Criteria for Top Event Fault Trees (cont.)

System/Function (Fault Tree Name(s))	Applicable Event Tree(s)	General Success Criteria	Assumptions/Notes
ISLOCA Upstream of RCP Thermal Barrier Heat Exchanger (ISL-RCP-TBHX-UPSTREAM)	ISL-RCP-TBHX	There is a check valve directly upstream of each RCP thermal barrier heat exchanger. If the check valve for the ruptured thermal barrier heat exchanger successfully closes, no ISLOCA will occur.	Since the ISL-RCP-TBHX event tree represents the failure of any of the four RCP thermal barrier heat exchangers, the RCP-specific valves are represented by a single basic event.
Low-Pressure Injection (LPI and LPI-ACR)	Event Trees Involving LOCAs (Including SGTR)	One of 2 RHR pumps to inject RWST water to any 2 of 4 cold legs (2 of 3 intact cold legs for MLOCA and LLOCA).	
Low-Pressure Recirculation (LPR and LPR-ACR)	Event Trees Involving LOCAs (Except SGTR)	One of 2 RHR pumps injecting containment sump water to 1 of 4 cold legs (1 of 3 intact cold legs for MLOCA and LLOCA). The heat sink for the recirculation water is provided by the CCW to RHR heat exchanger or by 4 of 8 CCUs.	
Main Feedwater during ATWS (MFW-ATWS)	ATWS	Continued MFW flow to at least one SG from 1 of 2 MFW pumps (1 of 3 condensate pumps is required to provide suction to MFW pumps).	
Offsite Power Recovery (OPR, OPR-1H, OPR-2H)	SBO	Success requires that offsite power be restored to the emergency buses. Fault trees are included for power recovery within 1 and 2 hours.	Offsite power cannot be recovered following depletion of the most limiting batteries required to restore offsite power (turbine building batteries – 2 hours).

Table 5-2 System/Function Success Criteria for Top Event Fault Trees (cont.)

System/Function (Fault Tree Name(s))	Applicable Event Tree(s)	General Success Criteria	Assumptions/Notes
Pressure-Induced SGTR (PI-SGTR)	SSB Event Trees	This fault tree captures the probability of having a sufficiently deep flaw along with the probability that the ensuing tube rupture will proceed to core damage.	A fault tree representing the relevant top event fault trees from the SGTR event tree is used to determine if the pressure-induced SGTR results in core damage.
Primary Pressure Relief (PPR)	ATWS	The reactor cycle is not in UET and all (unblocked) pressurizer PORV(s) and SRVs open to prevent RCS pressure from exceeding 3200 psi.	The L3PRA project Level 1 model includes two cases: (1) all PORVS/SRVs are available and (2) one PORV is blocked during the transient, with the other PORV and all SRVs available. The UETs (taken from WCAP-15831) for these cases are 0.11 and 0.32, respectively. UETs assume that initial power level is 100 percent and manual control rod insertion cannot be performed within 90 seconds given an ATWS with MFW unavailable.

Table 5-2 System/Function Success Criteria for Top Event Fault Trees (cont.)

System/Function (Fault Tree Name(s))	Applicable Event Tree(s)	General Success Criteria	Assumptions/Notes
Primary Relief Valves Close (PVC, PVC-B, PVC-ATWS)	Most Transients, SBO, ATWS	The pressurizer PORVs/SRVs should reclose (if challenged) after a turbine trip. During an ATWS with MFW unavailable, all (unblocked) PORVs/SRVs are assumed to open.	The PORV challenge probabilities were taken from Table 11 of NUREG/CR-7037. If a PORV fails to reclose, its associated block valve will receive an automatic isolation signal on low RPS pressure. The pressurizer SRVs will not be challenged unless the pressurizer PORVs fail to open. During an ATWS, the SRVs have an increased failure probability of 0.1 to reclose, since these valves are not designed to pass water.
Pressurizer Valves Reseat (PZRR)	Inadvertent SI Actuation	The pressurizer PORVs or SRVs need to reclose.	If a PORV fails to reclose, its associated block valve will receive an automatic isolation signal on low RPS pressure. The pressurizer SRVs will not be challenged unless the pressurizer PORVs fail to open. If challenged, the SRVs have an increased failure probability of 0.1 to reclose, since these valves are not designed to pass water.

Table 5-2 System/Function Success Criteria for Top Event Fault Trees (cont.)

System/Function (Fault Tree Name(s))	Applicable Event Tree(s)	General Success Criteria	Assumptions/Notes
RCP Seal Cooling (RCPSC)	Most Transients	Successful RCP seal cooling via the RCP thermal barrier heat exchangers requires 1 of 2 ACCW pumps and 1 of 2 ACCWS heat exchangers (cooled by NSCW).	
RCP Seal Injection (RCPSI, RCPSI-LOACCW, RCPSI-CCPs)	Most Transients, Loss of ACCW, SSB Event Trees	RCP seal injection is normally provided by the NCP. If RCP seal injection fails, seal leakage is assumed to increase to at least 21 gpm per RCP. For a loss of ACCW, sufficient time is available for operators (OA-CCP-ALIGN---H) to align 1 of 2 CCPs to provide RCP seal injection. During a SSB, RCP seal injection is provided by CCPs, which start during a SI actuation.	The NCP is tripped during a SI actuation and RCP seal injection is provided by HPI (i.e., the CCPs) through the normal charging line. Credit for operators to align the CCPs to provide RCP seal injection is only taken for loss of ACCW and loss of RCP seal injection initiating events, since for other initiators, there is insufficient time for operators to get to critical procedure steps. This credit for the loss of RCP seal injection initiating event is included in the IEFT-LOSINJ fault tree. Note that the assumption of elevated RCP seal leakage is conservative for scenarios with successful RCP seal cooling (via ACCW through the thermal barrier heat exchangers).

Table 5-2 System/Function Success Criteria for Top Event Fault Trees (cont.)

System/Function (Fault Tree Name(s))	Applicable Event Tree(s)	General Success Criteria	Assumptions/Notes
Reactor Protection System (RPS)	Most Event Trees	Success requires a sufficient number of control rods to be inserted into the reactor core to stop the nuclear chain reaction. The potential for operators (OA------MANRTH or RPS-XHE-XE-NSGNL) to manually scram the reactor is credited, depending on the availability of the RPS signal.	The RPS fault tree logic was aligns with NUREG/CR-5500. Operators cannot manually trip the reactor if the control rods are mechanically stuck or the reactor trip breakers are failed.
Reactor Vessel Rupture Mitigation (RPVRM)	XLOCA	Success requires mitigation of a reactor vessel rupture event.	There is no known mitigation measure for a reactor vessel rupture event. Therefore, this top event is set to TRUE.
Residual Heat Removal (RHR, RHR-ACR)	Event Trees involving a SLOCA	One of 2 RHR trains is required for successful shutdown cooling.	A failure of six or more CCUs will result in an actuation of containment spray (except for SGTR), which causes the entry conditions for recirculation (low RWST level) to be reached prior to conditions for shutdown cooling.
RWST Refill (RFL)	SGTR	During a SGTR and the failure to isolate the ruptured SG, operator action (RFL-XHE-REFILL-LT) is required to refill the RWST.	This fault tree only includes the HFE (i.e., no hardware failures are modeled).

Table 5-2 System/Function Success Criteria for Top Event Fault Trees (cont.)

System/Function (Fault Tree Name(s))	Applicable Event Tree(s)	General Success Criteria	Assumptions/Notes
Additional Requirements for 72-Hour Safe/Stable End-state (SAFE/STABLE, SAFE/STABLE-ACR)	Most Transients, SBO	Operators (CAD-XHE-SAFESTABLE) must depressurize the SGs with 3 of 3 TBVs (to the condenser) or an ARV for 1 of 4 SGs. If successful, this depressurization will allow the accumulators (2 of 4 accumulators required for success) to inject into the RCS.	

Table 5-2 System/Function Success Criteria for Top Event Fault Trees (cont.)

System/Function (Fault Tree Name(s))	Applicable Event Tree(s)	General Success Criteria	Assumptions/Notes
Steam Generator Isolation (SGI, SGI-SSBI, SGI-SSBO, SGI-CSSBI, SGI-CSSBO)	SGTR, SSB Event Trees	For a SGTR, successful SG isolation requires operators to close at least one MSIV on the affected SG and the associated MSIV bypass valve. If SG 1 or 2 is the affected SG, then operators must also close the steam supply valve to the turbine-driven AFW pump. Operators can also prevent SG overfill by closing the MSIVs and associated bypass valves on the other three (intact) SGs and stopping feed flow to the affected SG. For a SSB upstream of the MSIVs/downstream of the MFIVs, a MSIV (including bypass valve) and MFIVs (including bypass valve) or MFRVs must be closed on the faulted SG. In addition, operators (SSB-XHE-ISOLATION) must isolate AFW to the faulted SG. For a SSB downstream of the MSIVs/upstream of the MFIVs, the MSIVs and MFIVs/MFRVs (including bypass valves) must be closed on all four SGs. For a consequential SSB downstream of the MSIVs, only the MSIVs are required to close.	During a SSB, the MSIVs and bypass valves are assumed to receive an automatic closure signal (low steam line pressure). Feedwater isolation valves will receive an automatic isolation signal due to the SI actuation. Operator action is not included in the SGI-SSBO or SGI-CSSBO fault trees because of the automatic closure signals. The inclusion of the operator action, given the failure of the automatic closure signal, would have a negligible effect on the results.

Table 5-2 System/Function Success Criteria for Top Event Fault Trees (cont.)

System/Function (Fault Tree Name(s))	Applicable Event Tree(s)	General Success Criteria	Assumptions/Notes
Consequential SLOCA during SSB (SSB-CSLOCA,)	SSB Event Trees	Operator action (as represented by OAT----------H) is required to terminate SI, align a single CCP for normal charging, and establish letdown. In addition, the pressurizer PORVs/SRVs must reclose once SI has been terminated.	If a PORV fails to reclose, its associated block valve will receive an automatic isolation signal on low RPS pressure. The pressurizer SRVs will not be challenged unless the pressurizer PORVs fail to open. If challenged, the SRVs have an increased failure probability of 0.1 to reclose, since these valves are not designed to pass water.
Secondary Relief Valves Close (SVC)	Most Transients	If SG ARVs or SRVs are challenged, they need to reclose after SG pressure falls below their set-points.	The SG ARVs will only be challenged if the TBVs are unavailable or fail to open. The SG SRVs will only be challenged if the ARVs are unavailable or fail to open. The failure of one SG ARV or SRV is conservatively assumed to result in a consequential SSB (upstream of the MSIVs).

Table 5-2 System/Function Success Criteria for Top Event Fault Trees (cont.)

System/Function (Fault Tree Name(s))	Applicable Event Tree(s)	General Success Criteria	Assumptions/Notes
Terminate Safety Injection (TSI)	Inadvertent SI Actuation	Operator action (OAT----------H) is required to terminate SI (especially the tripping of the CCPs) to prevent loss of RCS inventory through the pressurizer valves.	
Turbine Trip (TT, TT-ATWS)	Most Transient Event Trees, ATWS	For successful turbine trip, all four steam supply lines to the high-pressure turbine need to be isolated after the reactor trip by closing either their respective control valve or main stop valve. If the turbine successfully trips, the TBVs will be demanded (if available). If challenged, the TBVs must reclose. During ATWS, the turbine must trip to prevent SG dry out given a loss of MFW.	AMSAC is credited in the TT-ATWS fault tree.

6 HUMAN RELIABILITY ANALYSIS

6.1 Introduction

The human reliability analysis (HRA) for the L3PRA project Level 1 model was developed based on reviews of the reference plant probabilistic risk assessment (PRA) model HRA. Other inputs include the American Society of Mechanical Engineers/American Nuclear Society (ASME/ANS) PRA standard (ASME/ANS, 2009), Electric Power Research Institute (EPRI) TR-100259, "An Approach to the Analysis of Operator Actions in PRA," (EPRI, 1992), additional information and interactions with the reference plant licensee and EPRI, and interactions with the L3PRA project Technical Advisory Group.

As part of the NRC's adoption of the reference plant HRA, the NRC recalculated human error probabilities (HEPs) that met either of the following two criteria: (1) the human failure event (HFE) was determined to be time critical (i.e., total system time window (T_{sw}) is less than 30 minutes) or (2) the cognition portion of the HEP (P_{cog}) for an HFE was judged to be low (i.e., less than 10^{-4}) according to NUREG-1792, "Good Practices for Implementing Human Reliability Analysis" (NRC, 2005b). Section 6.2 provides the revised timing analysis for HFEs that were determined to be time critical and the requantification of their associated HEPs using the Human Cognitive Reliability (HCR)/Operator Reliability Experiments (ORE) method (as described in EPRI TR-100259) using the EPRI HRA Calculator (EPRI, 2011). Section 6.3 provides the reevaluation of HFEs that had a P_{cog} less than 10^{-4}. In addition, several HFEs were reevaluated due to other factors (e.g., change in timing information, procedure modification, and expanded execution steps) regardless of their associated HEP. These reevaluations are described in Section 6.4.

A list of the reference plant model HFEs (and their associated HEPs) that were not reevaluated and were adopted into the L3PRA project PRA model are provided in Table 6-1. Due to different modeling assumptions and event/fault tree structures between the reference plant PRA and L3PRA project models it was necessary to incorporate some additional HFEs into the L3PRA project Level 1 model. These new HFEs are described in Section 6.5.

To ensure all key HFE combinations are evaluated for dependency and because of the modeling changes (including new HFEs), a new dependency analysis was performed for the L3PRA project Level 1 model. A summary of this evaluation is provided in Section 6.6. Lastly, Section 6.7 discusses pre-initiator HFEs

Table 6-1 Reference Plant PRA Model HFEs (and Associated HEPs) Adopted by the L3PRA Project Level 1 Model

Name	Description	HEP
OA-ALIGNPW-1HR	Operator fails to align alternate offsite power plant to 4.16 kilovolt (kV) bus within 1 hour after station blackout (SBO)	9.2E-02
OA-ALIGNPW-2HR	Operator fails to align alternate offsite power plant to 4.16 kV bus within 2 hours after SBO	1.2E-02
OA-ALTAFW----H	Operator fails to provide additional water source for long term auxiliary feedwater (AFW)	1.0E-04
OAB_SI-------H	Operator fails to bleed and feed - safety injection (SI)	2.4E-02
OAB_TR-------H	Operator fails to feed and bleed - transient	5.8E-02
OAB-SBOACR---H	Operator fails to initiate feed and bleed - SBO after alternating current (AC) recovery	8.7E-02
OAC_NC-------H	Failure to initiate normal cooldown after loss-of-coolant accident (LOCA) with high-pressure injection (HPI)	9.1E-04
OA-ESFAS-HEH	Operator fails to start equipment on failure of engineered safety features actuation system signal	1.8E-03
OA-HPR-ACRB—H	Operator failure to switch to high-pressure recirculation (HPR) - SBO, AC recovery, 21/480 gallons per minute (gpm) or stuck-open relief valve (SORV), without containment cooling units (CCUs)	4.8E-03
OAF_MFW------H	Operator fails to establish main feedwater (MFW) to steam generators (SGs)	2.7E-02
OA-HURGXFMR—H	Operator fails local change 120 volt (V) AC supply from inverter to RG transformer	3.4E-03
OAI_SG-------H	Operator fails to isolate ruptured SG	2.1E-02
OA-IS-ISLACC-H	Operator fails to isolate interfacing-system loss-of-coolant accident (ISLOCA) through auxiliary component cooling water (ACCW) reactor coolant pump (RCP) thermal barrier heat exchanger cooling line (Adopted HEPs directly from OA-OISLSI-H)	6.7E-04
OA-IS-ISLLKF-H	Operator fails to isolate RCP seal leak off isolation valves (Adopted HEPs directly from OA-OISLSI-H)	6.7E-04

Name	Description	HEP
OA-IS-ISLSEALSBO	Operator fails to isolate RCP seal lines at local - ISLOCA with SBO (HEP is based on engineering judgement)	1.0E-02
OA-LTFB-ACRB-H	Operator fails to initiate HPR for long term feed and bleed - SBO after AC recovery, feed and bleed initiated CCU fail	6.3E-03
OA------MANRTH	Operator fails to manually initiate a reactor trip	1.9E-03
OA-MANUAL-SI-H	Operator fails to manually initiate a safety injection	4.9E-04

Table 6-1 Reference Plant PRA Model HFEs (and Associated HEPs) Adopted by the L3PRA Project Level 1 Model (cont.)

Name	Description	HEP
OA-NSCWCT-MV-H	Operator fails to locally open nuclear service cooling water (NSCW) containment spray motor-operated valves (MOVs) - no SI, no loss offsite power (LOOP), no additional heat loads	1.1E-02
OA-OLP_ML----H	Operator fails to restart low-pressure injection (LPI) - medium LOCA, HPI fails)	1.2E-02
OA-OLP_SL----H	Operator fails to restart LPI - small LOCA, HPI fails	1.2E-02
OA-OLP_STOPB-H	Operator fails to stop residual heat removal (RHR) pump when reactor coolant system (RCS) pressure is above pump shutoff head – component cooling water (CCW) not available	8.7E-03
OA-ORS-------H	Operator fails to restore systems after AC recovered in SBO	5.7E-02
OA-OSW-------H	Operator fails to establish single NSCW pump operation	2.0E-02
OAR_HPATA----H	Operator fails to establish HPR during anticipated transient without scram (ATWS) - with CCU success (containment spray not actuated)	2.3E-03
OAR_HPATB----H	Operator fails to establish HPR during ATWS - with CCU failed (containment spray actuated)	2.3E-03
OAR_HPML-----H	Operator fails to establish HPR - medium LOCA	2.3E-03
OAR_HPSLB----H	Operator fails to establish HPR - small LOCA without CCUs	2.3E-03
OAR_LPLL-----H	Operator fails to establish low-pressure recirculation (LPR) - large LOCA	7.2E-03
OAR_LPML-----H	Operator fails to establish LPR - medium LOCA, HPI failed, depressurization and LPI success	5.0E-04
OAR_LPSL2----H	Operator fails to establish LPR after depressurization - small LOCA, CCUs failed	6.8E-04
OAR_LTFB_SLB-H	Operator fails to establish HPR for long term feed and bleed - small LOCA without CCUs	2.1E-03

Table 6-1 Reference Plant PRA Model HFEs (and Associated HEPs) Adopted by the L3PRA Project Level 1 Model (cont.)

Name	Description	HEP
OAR_LTFB-TRB-H	Operator fails to establish HPR for long term feed and bleed - transient without CCUs	2.3E-03
OA-START-AFW-H	Operator action to manually start AFW pumps in main control room (MCR) fails	3.3E-03
OA-SUMPMOV---H	Operator fails to open sump MOVs for recirculation - auto signal failed (Adopted HEP directly from OA ESFAS-HE1-H)	1.8E-03

6.2 Quantification of Time-Critical HFEs

This section provides information on the quantification of HFEs that were determined to be time critical (i.e., T_{sw} is less than 30 minutes). The timing information for most HFEs used in the L3PRA project Level 1 model were obtained from the reference plant PRA model; guidance was also used for timing estimation following EPRI TR-100259 and EPRI NP-6937, "Operator Reliability Experiments Using Power Plant Simulators," (EPRI, 1990). Time window definitions are provided in Figure 6-1 (adopted from EPRI TR-100259).

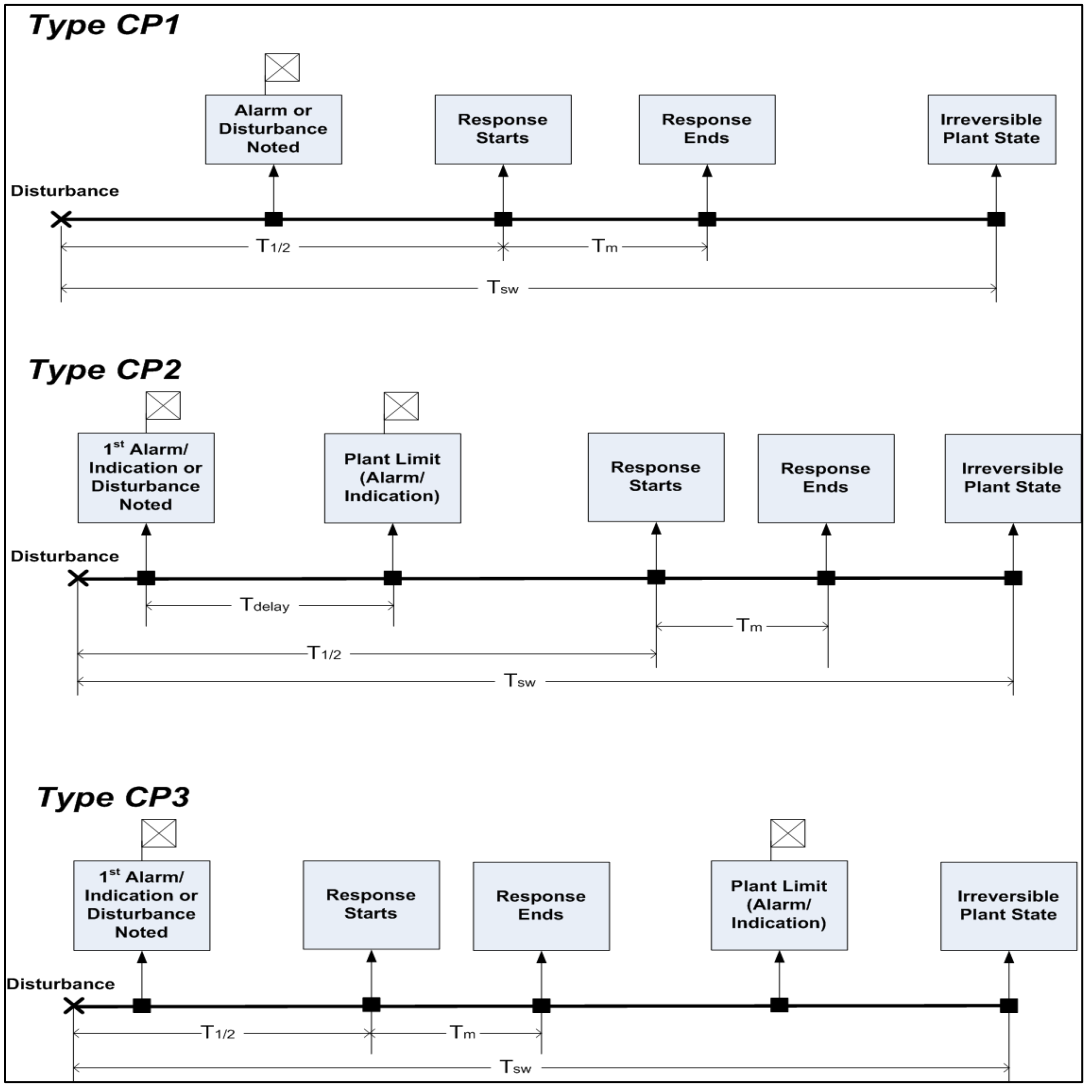


Figure 6-1 Time Window Definitions

The timing information used for (1) the total system window (T_{sw}), which was principally based on thermal-hydraulic calculations; (2) the manipulation time (T_M), which was based on timing information collected for job performance measures (JPMs); and (3) the time available to take action before plant conditions deteriorated to an unacceptable level (T_{Delay}) was taken from the

reference plant PRA model and supporting documentation. The reference plant PRA model did not include the crew median cognitive response time ($T_{1/2}$). The $T_{1/2}$ values for the time-critical HFEs were calculated to be consistent with definitions in EPRI TR-100259. [203]

The L3PRA project team used the timing information and other guidance discussed above to calculate the HEPs for the cognitive portion of the HFE for time critical actions using the HCR/ORE model (via the EPRI HRA Calculator). These values were then compared with HEPs calculated by the Cause-Based Decision Tree (CBDT) method (as described in EPRI TR-100259), and the higher cognitive HEP was selected for use in each case. The time critical HFEs and their HEPs, as used in the L3PRA, are provided in Table 6-2.

6.2.1 OA-CCP-ALIGN---H, Operator Fails to Align Centrifugal Charging Pump (CCP) within 13 Minutes of loss of ACCW

Timing Analysis. The Westinghouse Owner's Group (WOG) 2000 RCP seal leakage model (Westinghouse, 2002) assumes that RCP seal cooling must be restored within 13 minutes after the loss of all seal cooling in order to prevent catastrophic failure of the RCP seals. The time window of 13 minutes is based on the time it will take for the normal volume of cool water in the RCP seal area to leak past the seals. After this time, the seals are exposed to water at RCS temperature and will begin to degrade (the maximum possible leakage is assumed). As the normal charging pump (NCP) will continue to operate for at least 2 minutes without ACCW cooling, the time window can be extended by 2 minutes; therefore:

- T_{SW} = 15 minutes
- T_{Delay} = 5 minutes (1 minute to respond to alarm and enter the loss of ACCW procedure)
- T_M = 5 minutes (per operator interview)

HFE Calculation. According to above information this is a time-critical action. In this calculation $T_{1/2} = T_{Delay}$. Based on Figure 6-1, this is a type CP1 HFE and the revised time windows were estimated as follows:

- T_{SW} = 15 minutes
- $T_{1/2}$ = 5 minutes
- T_M = 5 minutes
- σ = 0.57 (PWR and CP1)

Therefore, the results from the HRA calculator are:

- HEP_{Cog} = 0.11

---

[203] The estimates for T_{Delay} appear to have included the time for crew cognitive response (i.e., includes $T_{1/2}$). Where possible, estimates for $T_{1/2}$ were developed considering T_{Delay} for the L3PRA Project Level 1 model. Of key importance is understanding the time window available to act before the plant conditions deteriorate to unacceptable limits. Therefore, the labeling of T_{Delay} and $T_{1/2}$ is not crucial if there is a full consideration of the timing limitations.

- HEP_{Total} = 0.12

The L3PRA project Level 1 model applied the modeling assumption that the HEP for OA-CCP-ALIGN---H can be used for OA-RWSTLOACC-H (operators fail to align the refueling water storage tank (RWST) to the CCPs when the volume control tank (VCT) level decreases during a loss of ACCW) and OA-SAGD-CHG—H (operators fail to establish safety grade charging after a loss of normal RCP seal injection initiating event) without additional analysis. Therefore, the HEPs for OA-RWSTLOACC-H and OA-SAGD-CHG—H are both set to 0.12 in the L3PRA project Level 1 model.

6.2.2 OAD_MLA------H, Operator Fails to Depressurize Secondary Side at the Maximum Rate

Timing Analysis. In investigating whether depressurization during a medium loss-of-coolant accident (MLOCA) is required given a failure of HP), MELCOR calculations were used to develop timing estimates. The results of the MELCOR calculations for 2.5- and 3-inch MLOCA scenarios and related information from the reference plant PRA model were used to develop the following timing estimates for OAD_MLA------H:

- T_{SW} = 25 minutes
- $T_{1/2}$ = 22 minutes
- T_M = 1 minute

HFE Calculation. According to the above information, this is a time-critical action. Based on Figure 6-1, this is a Type CP1 HFE [σ = 0.57 (PWR and CP1)]. Therefore, the new results from the HRA calculator are:

- HEP_{Cog} = 0.43
- HEP_{Total} = 0.44

6.2.3 OA-START-ACCWH, Operator Fails to Start ACCW Pump Given Failure of Running Pump

Timing Analysis. The WOG 2000 RCP seal leakage model assumes that RCP seal cooling must be restored within 13 minutes after the loss of all seal cooling to prevent catastrophic failure of the RCP seals. The time window of 13 minutes is based on the time it will take for the normal volume of cool water in the RCP seal area to leak past the seals. After this time, the seals are exposed to water at RCS temperature and will begin to degrade (the maximum possible leakage is assumed). The timing to allow the starting of the non-running ACCW pump reveals:

- T_{SW} = 13 minutes
- T_{Delay} = 1 minute (to respond to alarms and enter the alarm response procedure)
- T_M = 1 minute (for a well-practiced control room action)

HFE Calculation. According to the above information, this is a time-critical action. Based on Figure 6-1, this is a type CP2 HFE and the revised time windows were estimated as follows:

- T_{SW} = 13 minutes
- $T_{1/2}$ = 5 minutes (4 minutes for taking immediate actions and 1-minute T_{Delay})
- T_M = 1 minute
- σ = 0.38 (PWR and CP2)

Therefore, the new results from the HRA calculator are:

- $HEP_{Cog} = 6.2 \times 10^{-2}$
- $HEP_{Total} = 6.4E \times 10^{-2}$

6.2.4 OA-XFER-NON1EH, Operator Fails to Align Non-Class 1E Buses Given Fast and Residual Transfer Fails

Timing Analysis. In quantifying the HEP for this HFE, the most limiting case in terms of timing was assumed, that is, the AFW pumps fail and the condensate and MFW pumps are needed to feed the SGs. Analysis shows that if feed flow to the SGs is not restored, a feed and bleed condition would occur at t = 0.40 hour; therefore:

- T_{SW} = time to feed and bleed condition occurring = 0.40 hours = 24 minutes
- T_M = 1 minute for a simple control room action

The time for action to be taken to align non-Class 1E buses given fast and residual transfer fails (T_{Delay}) was calculated using the sum of the times to recognize the need to do the transfer and implement the procedural steps and was determined to be 22.6 minutes. This calculation relied on input from reference plant MAAP analyses and estimates of the time for operators to complete the procedural steps to initiate the align power to the condensate and MFW pumps to a non-Class 1E power supply.

- T_{Delay} = 22.6 minutes

HFE Calculation. According to the above information, this is a time-critical action. In this calculation $T_{1/2} = T_{Delay}$. Based on Figure 6-1, this is a type CP1 HFE and the revised time windows were estimated as follows:

- T_{SW} = 24 minutes
- $T_{1/2}$ = 22.6 minutes
- T_M = 1 minute
- σ = 0.57 (PWR and CP1)

Therefore, the new results from the HRA calculator are:

- HEP_{Cog} = 0.48
- HEP_{Total} = 0.48

Table 6-2 Time Critical HFEs Used in L3PRA Project Level 1 Model

Name	Description	HEP
OA-CCP-ALIGN---H	Operator fails to shift from NCP to CCP after loss of ACCW for RCP seal injection	1.2E-01
OA-RWSTLOACC-H	Operator fails to align the refueling water storage tank (RWST) to CCPs when VCT level decreased - loss of ACCW	1.2E-01
OA-SAGD-CHG—H	Operator failure to establish safety grade charging after loss of RCP seal injection initiating event	1.2E-01
OAD_MLA------H	Operator fails to depressurize secondary for LPI - MLOCA with HPI failed	4.4E-01
OA-START-ACCWH	Operator fails to start ACCW pump for special initiator	6.4E-02
OA-XFER-NON1EH	Operator fails to align non-Class 1E buses given fast transfer fails	4.8E-01

6.3 Quantification of HFEs with Low Cognitive Probabilities

This section provides the quantification of HFEs using the CBDT method to determine if recovery credit and other assumptions should be used in the L3PRA project Level 1 model. The NRC analyses closely followed the formal guidance provided in EPRI TR-100259, the EPRI HRA Calculator training, and implied and/or recommended conservatisms and/or HRA conventions that appear as defaults in the EPRI HRA Calculator.

In many cases, the quantified cognitive portion was driven by the dependency level assumed for the recovery option. Since self-recovery is based on the same crew and the same procedure, a non-zero level of dependence should be assumed.

Table 6-3 outlines the HFEs that were evaluated to assess cognitive probabilities. Notes are provided on the basis for the HEP values.

Table 6-3 Revised HFEs Due to NRC Assessment of Cognition Probabilities for the L3PRA Project Level 1 Model

Name	Description	HEP	Notes
OAD_SGR------H	Operator fails to depressurize secondary	1.5E-03	NRC analysts assumed that the system window time to use in the analysis should be based on the time until a SG atmospheric relief valve (ARV) or safety relief valve (SRV) lifts (i.e., a stuck-open ARV or SRV would fail SG isolation). This time (T_{sw}) is estimated to be 60 minutes. The execution portion of this HFE evaluated the actions that operators must take to terminate safety injection (SI) to prevent a stuck-open SG relief valve failing isolation of the faulted SG. All steps within the scope of this HFE were assessed to determine if failure of the step would lead to failure of the operator action (critical steps) that should be accounted for in the execution failure probability. The critical steps were used to calculate the execution failure probability used to determine the overall HEP for this HFE in the L3PRA project Level 1 model.
OA-HPR-ACRA--H	Operator failure to switch to HPR - SBO, AC recovery, 21/480 gpm or SORV, with CCUs	1.2E-03	The dependency level for evaluating recovery credit was determined to be low dependency.
OAL_LPLL-----H	Operator fails to establish low pressure hot leg recirculation - large LOCA	1.3E-04	
OA-LTFB-ACRA-H	Operator fails to HPR for long term feed and bleed - SBO after AC recovery, feed and bleed initiated, CCUs recovered	6.0E-04	

Name	Description	HEP	Notes
OAN_SL-------H	Operator fails to establish normal RHR - SLOCA	1.1E-03	
OAR_HPSLA----H	Operator fails to establish HPR - small LOCA with CCUs	6.0E-04	The dependency level for evaluating recovery credit was determined to be low dependency.

Table 6-3 Revised HFEs Due to NRC Assessment of Cognition Probabilities for the L3PRA Project Level 1 Model (cont.)

Name	Description	HEP	Notes
OAR_LPSL-----H	operator fails to establish LPR after depressurization - SLOCA, RHR failed, with CCUs available	1.1E-03	
OAR_LTFB_SLA-H	Operator fails to establish HPR for long term feed and bleed -SLOCA with CCUs	5.8E-04	
OAR_LTFB-TRA-H	Operator fails to establish HPR for long term feed and bleed - transient with CCUs	6.0E-04	

6.4 Additional HFE Evaluations

The HFEs below were evaluated due to changes in timing or scope/definition. Table 6.5 outlines the changes for the reevaluated HFEs.

6.4.1 OAC_AC-------H, Operator Fails to Depressurize for LPI - SLOCA, HPI Fails (FR-C.1/C.2)

Reason for Evaluation. To determine whether depressurization during a small loss-of-coolant accident (SLOCA) is required given a failure of HPI, MELCOR calculations and information from the reference plant PRA model were used to establish the timings. The results of the MELCOR calculations for 1.6-inch SLOCA scenarios were used to determine the timing estimates for OAC_AC-------H:

- T_{SW} = 74 minutes
- $T_{1/2}$ = 56 minutes
- T_M = 1 minute

HFE Calculation. Based on the timing analysis, the results from the HRA calculator are:

- $HEP_{Cog} = 1.0 \times 10^{-3}$
- $HEP_{Total} = 1.5 \times 10^{-3}$

6.4.2 OA-IS-ISLRHR-H, Operator Fails to Isolate ISLOCA through RHR Cold Leg Injection Lines

Reason for Evaluation. The recovery credit was not credited for this case.

HFE Calculation. Based on not crediting the recovery credit, the results from the HRA calculator are:

- $HEP_{Cog} = 1.1 \times 10^{-2}$
- $HEP_{Total} = 1.6 \times 10^{-2}$

6.4.3 OA-OBR-------H, Operator Fails to Establish Emergency Boration

Reason for Evaluation. The timing analysis for this HFE based on NRC ATWS model assumptions. In the L3PRA project Level 1 model, emergency boration is only needed to add negative reactivity (and thus bring the plant to a safe/stable end-state) given that the initial ATWS-generated pressure transient has been mitigated and the control rods are mechanically stuck (see Section 3.4.1 and Section 5.1.38).

HFE Calculation. Given the extensive time for recovery, this HEP was set to a minimum value of 10^{-4}.

6.4.4 OAT----------H, Operator Fails to Terminate SI

Reason for Evaluation. The execution portion of this HFE included steps to align normal charging and letdown after terminating SI.

HFE Calculation. Based on the evaluation of the included steps, the results from the HRA calculator are:

- $HEP_{Cog} = 2.0 \times 10^{-4}$
- $HEP_{Total} = 2.6 \times 10^{-4}$

Table 6-4 Additional HFEs that were Evaluated for the L3PRA Project Level 1 Model

Name	Description	HEP	Notes
OAC_AC-------H	Operator fails to depressurize for LPI - SLOCA, HPI failed	1.3E-03	This HFE was evaluated to use timings based on MELCOR calculations. This HFE is not considered a time critical action; therefore, CBDT was used to calculate the HEP.
OA-IS-ISLRHR-H	Operator fails to isolate ISLOCA through RHR cold leg injection lines	1.6E-02	This HFE was evaluated without credit for recovery.

Name	Description	HEP	Notes
OA-OBR-------H	Operator fails to establish emergency boration	1.0E-04	This HFE was evaluated based on NRC ATWS modeling assumptions. The HEP was set to a minimum HEP of 1E-04 due to extensive time for recovery.

Table 6-4 Additional HFEs that were Evaluated for the L3PRA Project Level 1 Model (cont.)

Name	Description	HEP	Notes
OAT----------H	Operator fails to terminate SI - secondary side break (SSB)	2.6E-04	Execution portion of the HFE included steps to align normal charging and letdown after terminating SI

6.5 L3PRA Project Level 1 model specific HFEs

Several HFEs were created specifically for the L3PRA project Level 1 model to apply NRC modeling assumptions (e.g., event tree changes or fault tree changes). Table 6.5 provides the timing estimates and calculated HEPs for each of the HFEs.

Table 6-5 L3PRA Project Level 1 Model Specific HFEs

Name	Description	T_{SW} (Min.)	$T_{1/2}$ (Min.)	T_M (Min.)	HEP	Notes
CAD-XHE-SAFESTABLE	Operator fails to depressurize secondary (72-hour safe/stable)	2640	2400	1	7.5E-04	This HFE was added to the L3PRA project Level 1 model to account for late depressurization due to gradual loss of RCS inventory due to elevated RCP seal leakage (i.e., 21 gpm per RCP) with no makeup. See Section 3.1 and Section 5.1.41 for additional information.
CAD-XHE-SGTR-LT	Failure to initiate normal cooldown with HPI - late steam generator tube rupture (SGTR)	1440	46	1	1.9E-03	This HFE was added to the L3PRA project Level 1 model to account for the secondary cooldown and depressurization (performed after the initial cooldown and depressurization to terminate primary-to-secondary leakage) to reduce RCS temperature and pressure to allow for the initiation of the shutdown cooling mode of RHR. See Section 3.3.5 and Section 5.1.4.7 for additional information.
CHG-XHE-NORMAL	Operator fails to establish charging given a loss of RCP seal injection	1440	20	2	3.2E-04	This HFE was added to the L3PRA project Level 1 model to account for RCS inventory makeup needed due to the gradual loss of RCS inventory due to elevated RCP seal leakage (i.e., 21 gpm per RCP). See Section 3.1 and Section 5.1.5 for additional information.

Name	Description	T_{SW} (Min.)	$T_{1/2}$ (Min.)	T_M (Min.)	HEP	Notes
OAB_TR-------H-LT	Operator fails to feed and bleed - transient (long-term)	1540	1440	8	2.9E-03	This HFE was added to the L3PRA project Level 1 model to account for timing for initiating feed and bleed cooling after late AFW failures due to condensate storage tank (CST) inventory depletion (as compared with scenarios in which AFW fails immediately). See Section 5.1.8 for additional information.

Table 6-5 L3PRA Project Level 1 Model Specific HFEs (cont.)

Name	Description	T_{SW} (Min.)	$T_{1/2}$ (Min.)	T_M (Min.)	HEP	Notes
OA-XFER-NON1EH-LT	Operator fails to align non-Class 1E buses given fast transfer fails (long-term)	1440	10	1	2.7E-03	This HFE was added to the L3PRA project Level 1 model to account for timing for aligning AC power to the nonsafety-related buses to allow for recovery of instrument air and restoration of CST auto-fill makeup for continued long-term AFW operation. Note that the timing for OA-XFER-NON1EH is based on the restoration of MFW (including condensate).
RCS-XHE-XM-TRIP	Operator fails to trip reactor coolant pumps	13	10	0.2	3.3E-01	This HFE was added to the L3PRA project Level 1 model to account for the operators needing to manually trip the RCPs given the subsequent loss of ACCW after a reactor trip has occurred. A failure to trip the RCPs given a complete loss of seal injection and cooling is assumed to result in a catastrophic failure of the seals (480 gpm per RCP) per the WOG 2000 RCP seal leakage model.
RCS-XHE-XM-TRIP-LONSCW	Operator fails to trip reactor coolant pumps (loss of NSCW or ACCW)	13	3	0.2	5.4E-03	This HFE was added to the L3PRA project Level 1 model to account for the operators needing to manually trip the RCPs given an initial loss of NSCW or ACCW (prior to a reactor trip). Note that the operators are procedurally directed to trip the RCPs after manually tripping the reactor that gives operators a larger time window as compared to if NSCW or ACCW fail after a reactor trip.

Name	Description	T_{SW} (Min.)	$T_{1/2}$ (Min.)	T_M (Min.)	HEP	Notes
RFL-XHE-REFILL-LT	Operator fails to refill RWST long-term				1.0E-04	This HFE was added to the L3PRA project Level 1 model to account for the operators needing to refill the RWST during a SGTR in which the operators failed to isolate the faulted SG or terminate primary-to-secondary leakage. The HEP was set to the minimum value of 1E-04 due to extensive time for recovery. See Section 3.3.5 and Section 5.1.40 for additional information.
RPS-XHE-XE-NSGNL	Operator fails to respond with no RPS signal present	1.5	0	0.5	2.3E-01	This HFE was added to the L3PRA project Level 1 model to account for the operators manually tripping the reactor given the RPS failures that render associated alarms/annunciators unavailable. See Section 5.1.37 for additional information.
RPS-XHE-TRIP-LT	Operators fails to trip the reactor (late)				1.0E-04	This HFE was added to the L3PRA project Level 1 model to account for the operators needing to add negative reactivity by manually tripping the reactor or inserting control rods after quasi-equilibrium conditions are reached after an ATWS. The HEP was set to the minimum value of 1E-04 due to extensive time for recovery. See Section 3.4.1 and Section 5.1.38 for additional information.

Name	Description	T_{SW} (Min.)	$T_{1/2}$ (Min.)	T_M (Min.)	HEP	Notes
SSB-XHE-ISOLATION	Operator fails to isolate faulted steam generator during steam line break	60	10	5	9.6E-03	This HFE was added to the L3PRA project Level 1 model to account for the operators needing to manually close AFW injection valves to the faulted SG and the steam admission valves for the turbine-driven AFW pump. Note that this HFE was added to account for high/dry/low conditions that could potentially lead to a thermally-induced SGTR following core damage (which is a Level 2 PRA concern) in one of the four loops. See Section 3.2 and Section 5.1.42.1 for additional information.

6.6 Evaluation of the Dependency between HFEs

To ensure that all key HFE dependency combinations were identified, the L3PRA project Level 1 model was solved by setting the HEPs for applicable HFEs to 0.9.[204, 205] It was determined that a cut set contribution cutoff of 10^{-6} was sufficient to prevent any potential HFE combinations that could significantly affect the internal event CDF from being eliminated from the evaluation prior to the review. This resulted in 1168 cut sets (with elevated HEPs) with CDFs greater than or equal 10^{-6}.[206] Using a lower cut set CDF screening frequency threshold could add a significant number of additional HFE combinations; however, it is not believed that the additional combinations will result in many new HFE pairs (i.e., most, if not all, will contain HFE pairs already included in this evaluation). From these cut sets 41 distinct HFE pairs were identified (that are often repeated in multiple cut sets).

After the dependent HFEs were identified, the level of dependency was determined. NUREG-1792 presents guidance on determining the level of dependency between HFEs. Elements to be considered include:

- The same crew member(s) are responsible for the actions.
- The actions can be considered to take place relatively close in time such that a common crew mindset may carry over from one action to the next.
- There are similar plant conditions between the actions and they are being directed by identical (or nearly so) procedure and cue.
- The actions have similar performance shaping factors.
- The actions are performed in the same location and performed in similar ways.
- There is reason to believe that the crew's interpretation of the need or decision for an action might influence the crew's decisions for actions later in the scenario.

The L3PRA project Level 1 model for internal events considers these elements in determining the level of dependency using a modified version of the approach outlined in the EPRI HRA Calculator. The following criteria are evaluated through this approach:

- Same Crew. If the actions can be assumed to be performed by a different crew, the HFEs are considered independent. If the difference in time between the cues for each of the HFEs is greater than the length of the shift, a new crew can be assumed to be responding to the cue of the second HFE.

---

[204] HEPs for operator actions that are based on data (e.g., offsite power recovery), pre-initiator HFEs (Type 1), and HEPs that were currently set to 1.0 (or TRUE) were left at their nominal probabilities; all other HEPs were set to 0.9.

[205] The L3PRA Project Level 1 dependency analysis only considers Level 1 HFEs. The dependency of between Level 1 and Level 2 HFEs was not considered. There is potential for operator actions considered in the Level 2 model to occur prior to some Level 1 operator actions.

[206] The corresponding CDFs for these cut sets will be at least an order of magnitude lower even if complete dependency existed, because the 1st HFE in the combination is independent (i.e., its HEP would not be elevated).

- Common Cognitive. If the crew can be assumed to be in a common cognitive mindset while responding to both HFEs, complete dependency is assigned. This element is assessed by evaluating if the cue and procedures being used are identical for the HFEs being evaluated.

- Time. This element assesses the amount of time that is estimated to have elapsed between the cues for each of the HFEs. The options are either that the cues occur simultaneously or are separated by one of the following time intervals:

  – 0 < Time ≤ 15 minutes

  – 15 < Time ≤ 30 minutes

  – 30 < Time ≤ 60 minutes

  – Time > 60 minutes

- Adequate Resources. This element assesses whether an adequate number of staff is available to support the required actions. This determination is made by comparing the required tasks with the number of staff available.

- Same Location. The location refers to the room or general area in which the actions will be executed. If the actions are executed in the same location, a higher level of dependency is typically assessed.

Using this approach, a level of dependency is assigned of either: complete, high, moderate, low, or zero. Following the assignment of the dependency level, the dependent HEPs were calculated by applying the following dependency formulas given in the Technique for Human Error Rate Prediction (THERP) method (NRC, 1983):

Dependence Level	Equation
Zero	HEP
Low	(1 + 19 × HEP) / 20
Moderate	(1 + 6 × HEP) / 7
High	(1 + HEP) / 2
Complete	1.0

Table 6-6 provides a summary of the L3PRA project Level 1 model dependency analysis results.

Note that the L3PRA project Level 1 model for internal events does not apply a minimum joint HEP (or threshold) for occurrences of multiple post-initiator HFEs in a single cut set; however, other portions of the L3PRA project do utilize one (e.g., low-power/shutdown) given larger uncertainties expected in these models (as compared to internal events). The current ASME/ANS PRA standard does not require a minimum joint HEP; however, one may be recommended as part of future revisions of the standard. The lack of use of a minimum joint HEP is potentially non-conservative and has been identified as a key modeling uncertainty in Table 10-1.

Table 6-6 L3PRA Project Level 1 Model Dependency Results

#	First HFE	Second HFE	Independent HEP (2^{nd} HFE)	Dependence Level	New HFE	Dependent HEP (2^{nd} HFE)	Notes
1	CAD-XHE-SGTR-LT	OA-ALTAFW----H	1.0E-04	Zero			Greater than 12 hours between these HFEs; operator actions are expected to be performed by different crews.
2	CHG-XHE-NORMAL	CAD-XHE-SAFESTABLE	7.5E-04	Zero			
3	OA-ALTAFW----H	OAB_TR-------H-LT	2.9E-03	Low	OAB_TR-------H-LT-LD	5.3E-02	
4	OA-ALTAFW----H	OAF_MFW------H	2.7E-02	Low	OAF_MFW------H-LD	7.5E-02	
5	OA-ALTAFW----H	OAR_LTFB-TRA-H	6.0E-04	Zero			Greater than 12 hours between these HFEs; operator actions are expected to be performed by different crews
6	OA-ALTAFW----H	OA-SUMPMOV---H	1.8E-03	Zero			
7	OAC_NC-------H	OAR_HPSLA----H	6.0E-04	Low	OAR_HPSLA----H-LD	5.1E-02	
8	OAC_NC-------H	OA-HPR-ACRA--H	1.2E-03	Low	OA-HPR-ACRA--H-LD	5.1E-02	

#	First HFE	Second HFE	Independent HEP (2^{nd} HFE)	Dependence Level	New HFE	Dependent HEP (2^{nd} HFE)	Notes
9	OA-CCP-ALIGN---H	OA-ALTAFW----H	1.0E-04	Zero			Greater than 12 hours between these HFEs; operator actions are expected to be performed by different crews
10	OA-CCP-ALIGN---H	OAC_NC-------H	9.1E-04	Moderate	OAC_NC-------H-MD	1.4E-01	

Table 6-6 L3PRA Project Level 1 Model Dependency Results (cont.)

#	First HFE	Second HFE	Independent HEP (2^{nd} HFE)	Dependence Level	New HFE	Dependent HEP (2^{nd} HFE)	Notes
11	OA-CCP-ALIGN---H	OAN_SL-------H	1.1E-03	Low	OAN_SL-------H-LD	5.1E-02	
12	OAD_SGR------H	OA-ALTAFW----H	1.0E-04	Zero			Greater than 12 hours between these HFEs; operator actions are expected to be performed by different crews
13	OAD_SGR------H	RFL-XHE-REFILL-LT	1.0E-04	Zero			
14	OAD_SGR------H	OA-XFER-NON1EH-LT	2.7E-03	High	OA-XFER-NON1EH-LT-HD	5.0E-01	
15	OAF_MFW------H	OAB_TR-------H	5.8E-02	High	OAB_TR-------H-HD	5.3E-01	
16	OAF_MFW------H	OAB_TR-------H-LT	2.9E-03	Low	OAB_TR-------H-LT-LD	5.3E-02	The new HFE (with same HEP) was previously identified; no new HFE is needed for this HFE pair.
17	OAF_MFW------H	OA-HURGXFMR--H	3.4E-03	Low	OA-HURGXFMR--H-LD	5.3E-02	

#	First HFE	Second HFE	Independent HEP (2^{nd} HFE)	Dependence Level	New HFE	Dependent HEP (2^{nd} HFE)	Notes
18	OAF_MFW------H	OAR_LTFB-TRA-H	6.0E-04	Low	OAR_LTFB-TRA-H-LD	5.1E-02	
19	OAF_MFW------H	OA-SUMPMOV---H	1.8E-03	Low	OA-SUMPMOV---H-LD	5.2E-02	
20	OAI_SG-------H	OA-ALTAFW----H	1.0E-04	Zero			Greater than 12 hours between these HFEs; operator actions are expected to be performed by different crews
21	OAI_SG-------H	RFL-XHE-REFILL-LT	1.0E-04	Zero			
22	OAI_SG-------H	OA-XFER-NON1EH-LT	2.7E-03	Moderate	OA-XFER-NON1EH-LT-MD	1.5E-01	
23	OAN_SL-------H	OA-ALTAFW----H	1.0E-04	Zero			Greater than 12 hours between these HFEs; operator actions are expected to be performed by different crews
24	OAN_SL-------H	OAR_LPSL-----H	1.1E-03	Low	OAR_LPSL-----H-LD	5.1E-02	

#	First HFE	Second HFE	Independent HEP (2^{nd} HFE)	Dependence Level	New HFE	Dependent HEP (2^{nd} HFE)	Notes
25	OA-RWSTLOACC-H	OA-ALTAFW----H	1.0E-04	Zero			Greater than 12 hours between these HFEs; operator actions are expected to be performed by different crews
26	OA-RWSTLOACC-H	OAN_SL-------H	1.1E-03	Low	OAN_SL-------H-LD	5.1E-02	The new HFE (with same HEP) was previously identified; no new HFE is needed for this HFE pair.
27	OA-RWSTLOACC-H	OAC_NC-------H	9.1E-04	Moderate	OAC_NC-------H-MD	1.4E-01	
28	OA-SAGD-CHG--H	OA-ALTAFW----H	1.0E-04	Zero			Greater than 12 hours between these HFEs; operator actions are expected to be performed by different crews
29	OA-SAGD-CHG--H	OA-XFER-NON1EH-LT	2.7E-03	Low	OA-XFER-NON1EH-LT-LD	5.3E-02	The 1st HFE is a Type-2 pre-initiator HFE; dependency is determined to be low.
30	OA-SAGD-CHG--H	OAT----------H	2.6E-04	Low	OAT----------H-LD	5.0E-02	

#	First HFE	Second HFE	Independent HEP (2^{nd} HFE)	Dependence Level	New HFE	Dependent HEP (2^{nd} HFE)	Notes
31	OA-SAGD-CHG--H	OAF_MFW------H	2.7E-02	Low	OAF_MFW------H-LD	7.5E-02	The new HFE (with same HEP) was previously identified; no new HFE is needed for this HFE pair.
32	OA-START-AFW-H	OAF_MFW------H	2.7E-02	Complete	OAF_MFW------H-CD	1.0E+00	
33	OAT----------H	OAC_NC-------H	9.1E-04	High	OAC_NC-------H-HD	5.0E-01	
34	OA-XFER-NON1EH-LT	CAD-XHE-SGTR-LT	1.9E-03	Low	CAD-XHE-SGTR-LT-LD	5.2E-02	
35	OA-XFER-NON1EH-LT	OA-ALTAFW----H	1.0E-04	Zero			Greater than 12 hours between these HFEs; operator actions are expected to be performed by different crews
36	OA-XFER-NON1EH-LT	OAN_SL-------H	1.1E-03	Low	OAN_SL-------H-LD	5.1E-02	

#	First HFE	Second HFE	Independent HEP (2^{nd} HFE)	Dependence Level	New HFE	Dependent HEP (2^{nd} HFE)	Notes
37	RCS-XHE-XM-TRIP	OAC_NC-------H	9.1E-04	High	OAC_NC-------H-HD	5.0E-01	These new HFEs (with same HEPs) were previously identified; no new HFEs are needed for these HFE pairs.
38	RCS-XHE-XM-TRIP-LONSCW	OA-CCP-ALIGN---H	1.2E-01	Complete	OA-CCP-ALIGN---H-CD	1.0E+00	
39	RCS-XHE-XM-TRIP-LONSCW	OAC_NC-------H	9.1E-04	Moderate	OAC_NC-------H-MD	1.4E-01	The new HFE (with same HEP) was previously identified; no new HFE is needed for this HFE pair.
40	RCS-XHE-XM-TRIP-LONSCW	OA-RWSTLOACC-H	1.2E-01	Complete	OA-RWSTLOACC-H-CD	1.0E+00	
41	RCS-XHE-XM-TRIP-LONSCW	OA-OSW-------H	2.0E-02	Complete	OA-OSW-------H-CD	1.0E+00	

6.7 Evaluation of Pre-Initiator HFEs

The L3PRA project team reviewed the reference plant screening process used to eliminate valve misalignments. Based on this review, the following three valves were not screened out:

- SI RWST outlet isolation valve (manual, locked-open)
- Motor-driven AFW pump B suction valve from CST 1 (manual, locked-open)
- Motor-driven AFW pump A suction valve from CST 1 (manual, locked-open)

For the L3PRA project Level 1 model, pre-initiator HFEs for each of these valves were evaluated using the HRA approach from the Accident Sequence Evaluation Program (ASEP) as described in NUREG/CR-4772, "Accident Sequence Evaluation Program Human Reliability Analysis Procedure" (NRC, 1987). According to ASEP, the basic HEP of every pre-initiator is 10^{-2} and each factor of recovery credit may be 0.1. According to the ASME/ANS PRA standard (supporting requirement HR-D4), the following four factors may be considered for crediting recovery of the error:

- Post-maintenance or post-calibration tests required and performed by procedure
- Independent verification, using a written check-off list, which verifies component status following maintenance/testing
- A separate check of component status made later, using a written check-off list, by the original performer
- Work shift or daily checks of component status, using a written check-off list

For the motor-driven AFW pump CST suction valves, the only recovery factor that can be credited is an independent review (by another person or operator later). Therefore, a screening value 10^{-3} was applied to the HEPs of these two pre-initiator HFEs included in the L3PRA project Level 1 model.

For the SI RWST outlet isolation valve, the independent review is also the only factor that can be credited. However, the potential for misalignment of this valve would normally have been screened out, except that misalignment of this valve would affect multiple emergency core cooling systems. It was determined that an additional credit of 0.1 could be applied to the associated pre-initiator HFE for the SI RWST outlet isolation valve since it met other screening criteria. Therefore, a screening value of 10^{-4} was applied to this HFE in the L3PRA Level 1 model.

7 DATA ANALYSIS

The basic event data in the L3PRA project Level 1 model consists of initiating event frequencies, human failure event (HFE) probabilities, component unreliabilities and unavailabilities, and data-supported recovery failure probabilities. The initiating event frequency analysis is described in Section 2.2. The human reliability analysis (HRA) of operator actions and other human failure events is described in Section 6. The remaining basic event unreliability and unavailability analysis and data-supported recovery failure analysis are described in this section. The L3PRA project Level 1 model uses some reference plant PRA model basic event probabilities that are not included in the data analysis that follows.

The data analysis that follows addresses component unavailability, both independent and common-cause component unreliability, and non-recovery probabilities for offsite power. Component unavailability and unreliability are encoded in SAPHIRE template events. The template events enforce consistency and the state-of-knowledge correlation throughout the model. Each basic event that represents a given component type and failure mode subscribes to a specific template event so only the templates need to be described in the data analysis. In addition to template events, SAPHIRE relies heavily on plug-in software modules (accessed through SAPHIRE compound event types) to calculate common-cause failure (CCF) probabilities and offsite power non-recovery probabilities. Template data are described in Section 7.2, CCF probability calculations are described in Section 7.3, offsite power non-recovery probabilities are described in Section 7.4, and parameter uncertainty is described in Section 7.5. Also, a discussion of the component boundaries used for the data analysis is provided in Section 7.1.

7.1 Component Boundaries

Component boundaries in the L3PRA project Level 1 model are, by default, defined in Appendix A of NUREG/CR-6928 (NRC, 2007), and are generally consistent with those used in Mitigating Systems Performance Index (MSPI) Program (NEI, 2013), and the U.S. Nuclear Regulatory Commission (NRC) CCF data collection efforts. The component failure mode templates, described in the next section, conform to the NUREG/CR-6928 component boundary definitions.

There are instances in the L3PRA project Level 1 model where the fault trees are developed in greater detail than required to conform to the component boundaries provided in NUREG/CR-6928, creating the potential for some overlap in the accounting of component failure probability. This occurs in legacy logic from the original reference plant model fault tree development. Some of this legacy logic is still required to support the external events analysis. In other cases, the overlap was evaluated and found to have no impact on overall component or system unreliability. In these cases, a decision was made to either retain or rewrite the logic based on the amount of effort required. Notable exceptions to the NUREG/CR-6928 component boundaries include:

- The emergency diesel generator (EDG) fuel oil supply system is modeled in detail. This logic represents a source of dependency between the EDGs that would not be convincingly represented by CCF modeling alone. The impact of this “double-counting” on EDG train unreliability and emergency power system CCF probability is negligible.

- The auxiliary feedwater (AFW) turbine-driven pump trip throttle valve and some local instrumentation and control components have been incorporated into the L3PRA project

Level 1 model. The impact of this double-counting is negligible, representing less than 1 percent of overall component unreliability.

- Device actuation, in general. Many components in the L3PRA project Level 1 model, including the EDGs, include detailed actuation circuitry modeling that has been developed to aid in modeling fire scenarios. This double-counting has negligible impact on component unreliability, as the circuitry components are orders of magnitude more reliable than the component being actuated.

7.2 Template Events

Template events are SAPHIRE basic events that most often represent a probability for a specific failure mode for specific component (e.g., check valve fails to open, or motor-operated valve fails to close). By creating template events and using them in the database, the component failure probability equation, component failure rate parameter, uncertainty distribution type, and uncertainty distribution parameter for a given component type and failure mode need only be entered once, instead of separately for each specific component in the model. Once the probability calculation type, rate parameter, and uncertainty parameter have been entered, those basic events representing components of the same type, with the same failure mode, will reference the template. The advantage of using templates is if a failure rate parameter changes, the parameter only must be changed once, at the template event, and all components that are of that type will be updated automatically, and the state of knowledge correlation is always enforced.

The Institute of Nuclear Power Operations (INPO) Consolidated Events System (ICES) database was chosen as the preferred data source for the quantification of component unreliability. ICES data were supplemented with quality-assured information for components or systems that have been the subject of NRC-sponsored reliability studies.

The unreliability calculations were performed with the NRC web-based implementation of the Reliability and Availability Data System (RADS) calculator. The industry-average unreliability values were used by default, and for priors when using a Bayesian process to compute plant-specific values. In cases where system studies identified significant plant-specific differences, the plant-specific values generated from the system studies were considered. However, a review of more recent data indicated that plants exhibiting the worst performance in those studies (reflecting the following performance periods: 1987–1993, 1987–1995, or 1987–1997) generally were no longer outliers in terms of performance. That observation led to a more detailed review of selected component and initiating event performance for 1997–1999 and 2001–2003, which again indicated that plants with the worst performance during the earlier period were, in general, nominal performers during the latter period. In contrast, at the industry level, performance during 1997–2003 was relatively stable. Therefore, industry-average performance inputs were preferred for most parameter values. The preferred data source for industry-average failure rate information was the 2010 update to NUREG/CR-6928, provided on the NRC Operational Experience Website.

A plant-specific performance estimate for unreliability values for significant basic events was performed when possible. The parameter estimate methodology seeks to determine if plant-to-plant variability is observed in the data supporting the estimate. If so, then the empirical Bayes approach is used to obtain a parameter estimate that best represents the population variability (and provides for plant-specific estimates, if needed). If the empirical Bayes procedure fails, it is generally because plant-to-plant variability is not observed, or at least not detected by the

empirical Bayes procedure. In this case, the data set is considered homogeneous and parameter estimates are sought using a non-informative prior distribution, which is generally a Jeffreys prior. The industry-average distributions from the 2010 update to NUREG/CR-6928 were used as prior distributions for a Bayesian update using plant-specific data as evidence. The industry-average data for the priors was generated using a variety of approaches as described in NUREG/CR-6928. Many parameters were derived using Jeffreys priors. In these cases, plant-specific evidence had little influence on the prior distribution, which was strongly determined by the comparatively large amount of pooled industry information. However, in other cases, the industry-average priors were generated using an Empirical Bayes approach for representing plant-to-plant variability. The plant-specific evidence does influence these priors in a more noticeable way.

Table 7-1 provides a summary of the template events supporting the quantification of significant basic events, based on Fussell-Vesely (FV) importance measure greater than 0.005 or risk achievement worth (RAW) greater than 2. The table indicates if each template is based on a plant-specific unreliability estimate or on the industry-average 2010 update. The table shows that, when possible, plant-specific unreliability estimates were used in the quantification of risk-significant basic events. Note that CCF failure probabilities are addressed in the following section.

Table 7-1 Template Events Supporting Significant Basic Events

Template	Description	Plant Specific	Remarks
BAC-LP	Alternating current (AC) bus fails to operate	Yes	
BAC-TM	AC bus in test or maintenance	No	Plant-specific data not available in RADS.
BAT-LP	Battery fails to operate	Yes	
BAT-TM	Battery in test or maintenance	No	Plant-specific data not available in RADS.
BDC-LP	Direct current (DC) bus fails to operate	No	Failure data is too sparse for plant-specific estimate.
BCH-FC	Battery charger fails to operate	Yes	
CNT-OO	Contacts fail to close on demand	Yes	Legacy value from reference plant PRA model.
CRB-CC	Circuit breaker fails to open on demand	Yes	
CRB-CO	Circuit breaker transfers open	Yes	
CTF-MA	Cooling tower fan in test or maintenance	No	Plant-specific data not available in RADS.
DGN-FR	EDG fails to run (FTR) and fails to load and run (FTLR)	Yes	
DGN-FS	Diesel generator fails to start (FTS) on demand	Yes	
DGN-TM	Diesel generator in test or maintenance	Yes	
DPL-FC	AC distribution panel fails during operation	Yes	Legacy value from reference plant PRA model.
DPL-MA	AC distribution panel is in maintenance	No	Plant-specific data not available in RADS.

Template	Description	Plant Specific	Remarks
FUS-OP	Fuse opens prematurely	Yes	Legacy value from reference plant PRA Model.
INV-FO	Inverter fails to operate	Yes	
INV-MA	Inverter in maintenance	Yes	Reference plant-provided PRA value.
MDP-FR-E	Motor-driven pump fails to run for first hour (normally in standby)	Yes	
MDP-FR-L	Motor-driven pump fails to run after first hour (normally in standby)	Yes	
MDP-FR-NR	Motor-driven pump fails to run (normally running)	Yes	

Table 7-1 Template Events Supporting Significant Basic Events (cont.)

Template	Description	Plant Specific	Remarks
MDP-SWS-FR	Service water system motor-driven pump fails to run	Yes	
MDP-LK	Reactor coolant pump (RCP) seals leak	No	Westinghouse Owner's Group (WOG) 2000 RCP seal leakage model (Westinghouse, 2002) values applied industry wide.
MDP-TM(ALL)	Motor-driven pump in test or maintenance (all)	Yes	
MDP-TM(CCW)	Motor-driven pump in test or maintenance [component cooling water (CCW) system]	Yes	
FAN-FS	Heating, ventilating and air conditioning (HVAC) fan fails to start	No	Fan failure data is pooled; plant-specific values not supported by the data.
FAN-TM	HVAC fan is in test or maintenance	No	Plant-specific data not available in RADS.
MOV-CC	Motor-operated valve fails to open	Yes	
MOV-CO	Motor-operated valve fails open	Yes	
MOV-MA	Motor-operated valve in test or maintenance	No	Plant-specific data not available in RADS.
MOV-PG	Motor-operated valve plugs	No	Plant-specific data not available in RADS.
RLY-FC	Relay fails during operation	Yes	Legacy value from reference plant PRA model.
SEQ-FO	Emergency power system load sequencer fails to operate	No	Failure data is too sparse for plant-specific estimate.
SSD-MA	Sequencer in test or maintenance	No	Plant-specific data not available in RADS.
TDP-FR-E	Turbine-driven pump fails to run for first hour (normally in standby)	Yes	

Table 7-1 Template Events Supporting Significant Basic Events (cont.)

Template	Description	Plant Specific	Remarks
TDP-FR-L	Turbine-driven pump fails to run after first hour (normally in standby)	Yes	
TFW-FC	Transformer fails to operate	Yes	
TNK-RP	Tank rupture	Yes	
XVM-PG	Manual valve plugs	No	Plant-specific data not available in RADS.

The template events in Table 7-1 group components by type without explicit consideration of service conditions or test interval. This is a consequence of using publicly available failure information that does not make these distinctions. There is, however, an implicit accounting for these issues in the 2010 update data and in the plant-specific information used in the L3PRA project Level 1 model. The accounting occurs because nuclear industry data is used as a data source. AC buses, batteries, circuit breakers, EDGs, load sequencers, HVAC components, and other components included in the ICES data base and appearing in the significant event list are subject to similar operating environments and testing requirements because of nuclear plant design and regulatory maintenance requirements. For other components that may not be similar across the industry but may be similar within an easily identified sub-set of industry devices, an appropriate sub-set was selected. For example, the turbine-driven pump templates, which in this study are used for the AFW pumps (in standby) and MFW pumps (normally operating), are based on PWR system data only; and, therefore, exclude data for boiling-water reactor high-pressure coolant injection and reactor core isolation cooling pumps.

Motor-driven pumps and valves of various types are subject to a wider variety of operating environments than the previously mentioned components. The conditions range from open service water systems with both standby and normally operating components operating at relatively low pressures and temperatures and subject to a range of environmental effects, to reactor coolant system components in continuous operation, operating at much higher temperatures and pressures and with stringent water quality controls. Since service water pumps represent an extreme case their quantification was based on ICES motor-driven pump devices belonging specifically to service water systems. The remaining population of motor-driven pumps was separated into normally running and normally in standby categories with separate template sets for each. Valve data were pooled across system, service condition, and test interval, as were other components not specifically addressed above. This is a consequence of the analyses documented in NUREG/CR-6928 that includes a search for subgroups or levels within each component group population and only pooled data when no subgroupings could be justified as statistically separate within the population.

Test and maintenance unavailability events are also a combination of reference plant PRA model values and values generated using the web-based RADS system. The RADS-generated unavailability values for component outage events are identified by type of component, but they generally apply at the train level. For example, the MDP-TM (RHR) event covers all components within a pump train that are single failures for the train and can be unavailable while the plant is critical. Therefore, several components could contribute to the train test and maintenance outage. However, experience has shown that in general almost all train test and maintenance outages result from the main component. The MSPI basis documents were used as the preferred source for updating test and maintenance events. The MSPI basis documents present baseline test and maintenance data covering 2002–2004. MSPI test and maintenance data were preferred over Reactor Oversight Process (ROP) safety system unavailability (SSU) data because the MSPI collection guidelines more closely match those required for SPAR models (e.g., in terms of equipment boundaries and other related assumptions), and the SPAR model component failure data was used as the generic prior data in the L3PRA project Level 1 model. For example, the MSPI includes component overhaul outages while the plant is in critical operation, while the SSU data exclude such outages. Other differences in guidelines also exist, and in all cases the MSPI guidelines more closely fit the L3PRA project Level 1 model requirements.

Table 7-2 provides a summary of the posterior distributions that were calculated using the industry-average distributions from the 2010 update to NUREG/CR-6928 as prior distributions, updated with plant-specific evidence from 1998–2011.

Table 7-2 Plant Specific Failure Template Events

Template Rule	Description	Prior Distribution				Plant Experience		Posterior Distribution		
		Type	Mean	a	b	Events	Demands/ Hours	a	b	Mean
ACC-ELS	Accumulator external leakage (small)	Gamma	1.11E-07	8.50	7.65E+07	0	1.96E+06	8.50	7.85E+07	1.08E-07
ACC-FTOP	Accumulator fails to operate	Gamma	1.66E-07	0.59	3.57E+06	0	1.96E+06	0.59	5.54E+06	1.07E-07
AOV-ELS	Air-operated valve external leakage (small)	Gamma	5.51E-08	64.50	1.17E+09	0	1.08E+07	64.50	1.18E+09	5.46E-08
AOV-FC	Air-operated valve fails to control	Gamma	2.49E-07	1.42	5.72E+06	1	1.08E+07	2.42	1.65E+07	1.47E-07
AOV-FTO	Air-operated valve fails to open	Beta	9.51E-04	1.11	1.17E+03	1	2.18E+03	2.11	3.35E+03	6.31E-04
AOV-FTOC	Air-operated valve fails to open/close	Beta	9.51E-04	1.11	1.17E+03	1	2.18E+03	2.11	3.35E+03	6.31E-04
AOV-ILS	Air-operated valve internal leakage (small)	Gamma	9.69E-08	113.50	1.17E+09	0	1.08E+07	114.00	1.18E+09	9.60E-08
AOV-SOP	Air-operated valve transfers position	Gamma	1.31E-07	0.68	5.21E+06	0	1.08E+07	0.68	1.60E+07	4.25E-08

Template Rule	Description	Prior Distribution				Plant Experience		Posterior Distribution		
		Type	Mean	a	b	Events	Demands/ Hours	a	b	Mean
BAT-FTOP	Battery fails to operate	Gamma	5.86E-07	1.88	3.21E+06	1	1.72E+06	2.88	4.93E+06	5.85E-07
BCH-FTOP	Battery charger fails to operate	Gamma	2.71E-06	1.28	4.73E+05	27	3.44E+06	28.30	3.91E+06	7.24E-06
BUS-FTOP-AC	Ac bus fails to operate	Gamma	1.39E-06	0.70	5.07E+05	3	1.35E+06	3.70	1.86E+06	1.99E-06
CBK-FTOC	Circuit breaker fails to open/close	Beta	2.39E-03	0.95	3.98E+02	4	5.27E+02	4.95	9.22E+02	5.35E-03
CBKMV-FTOC	Circuit breaker transfers open	Beta	2.70E-03	0.56	2.05E+02	3	6.72E+01	3.50	6.47E+01	5.13E-02
CBKMV-SOP	Medium voltage circuit breaker fails to open/close	Gamma	1.04E-07	14.50	1.40E+08	0	2.81E+06	14.50	1.43E+08	1.02E-07
CBK-SOP	Medium voltage circuit breaker spurious operation	Gamma	2.11E-07	1.16	5.47E+06	1	4.32E+06	2.16	9.79E+06	2.20E-07
CKV-ELS	Check valve external leakage (small)	Gamma	1.05E-08	10.50	1.00E+09	0	3.44E+07	10.50	1.04E+09	1.01E-08
CKV-ILS	Check valve internal leakage (small)	Gamma	3.08E-07	0.57	1.86E+06	0	3.44E+07	0.57	3.62E+07	1.58E-08

Template Rule	Description	Prior Distribution				Plant Experience		Posterior Distribution		
		Type	Mean	a	b	Events	Demands/ Hours	a	b	Mean
CKV-SC	Check valve fails to remain open (spurious close)	Gamma	5.47E-09	5.50	1.00E+09	0	3.44E+07	5.50	1.04E+09	5.29E-09
CKV-SO	Check valve spurious opening	Gamma	3.48E-09	3.50	1.00E+09	0	3.44E+07	3.50	1.04E+09	3.37E-09
EDG-FTLR	Diesel generator fails to load and run, early	Beta	3.78E-03	2.77	7.31E+02	1	7.11E+02	3.77	1.44E+03	2.62E-03
EDG-FTR	Diesel generator fails to run, long-term	Gamma	1.09E-03	3.55	3.27E+03	3	1.64E+03	6.55	4.90E+03	1.34E-03

Table 7 2 Plant Specific Failure Template Events (cont.)

Template Rule	Description	Prior Distribution				Plant Experience		Posterior Distribution		
		Type	Mean	a	b	Events	Demands/ Hours	a	b	Mean
EDG-FTS	Diesel generator fails to start	Beta	2.89E-03	8.11	2.80E+03	3	9.79E+02	11.10	3.77E+03	2.94E-03
HOV-ELS	Hydraulic-operated valve external leakage (small)	Gamma	2.23E-07	19.50	8.75E+07	0	2.45E+06	19.50	9.00E+07	2.17E-07
HOV-FC	Hydraulic-operated valve fails to operate/control	Gamma	4.86E-07	42.50	8.75E+07	0	2.45E+06	42.50	9.00E+07	4.72E-07
HOV-FTOC	Hydraulic-operated valve fails to open/close	Beta	1.20E-03	24.50	2.05E+04	0	6.20E+02	24.50	2.11E+04	1.16E-03
HOV-ILS	Hydraulic-operated valve internal leakage (small)	Gamma	2.86E-08	2.50	8.75E+07	0	2.45E+06	2.50	9.00E+07	2.78E-08
HOV-SOP	Hydraulic-operated valve spurious operation	Gamma	2.00E-07	17.50	8.75E+07	0	2.45E+06	17.50	9.00E+07	1.94E-07
HTX-CCW-LOHT	CCW heat exchanger plugging all causes (hr-1)	Gamma	5.23E-07	16.50	3.16E+07	0	9.82E+05	16.50	3.25E+07	5.07E-07
HTX-ELS	Heat exchanger external leakage (small)	Gamma	3.34E-07	0.62	1.84E+06	0	3.68E+06	0.62	5.52E+06	1.12E-07
HTX-ILS	Heat exchanger internal leakage (small)	Gamma	3.79E-07	0.43	1.13E+06	0	3.68E+06	0.43	4.81E+06	8.92E-08

Table 7 2 Plant Specific Failure Template Events (cont.)

Template Rule	Description	Prior Distribution				Plant Experience		Posterior Distribution		
		Type	Mean	a	b	Events	Demands/ Hours	a	b	Mean
HTX-LOHT	Heat exchanger plugging (pooled)	Gamma	4.57E-07	0.53	1.17E+06	0	3.68E+06	0.53	4.85E+06	1.10E-07
INV-FTOP	Inverter fails to operate	Gamma	5.60E-06	1.18	2.11E+05	4	3.68E+05	5.18	5.80E+05	8.95E-06
MDP-CCW-FTR	CCW motor-driven pump fails to run, normally running	Gamma	3.02E-06	1.27	4.22E+05	2	6.14E+05	3.27	1.04E+06	3.16E-06
MDP-CCW-FTS	CCW motor-driven pump fails to start, normally running	Beta	1.08E-03	1.29	1.19E+03	1	3.54E+03	2.29	4.73E+03	4.84E-04
MDP-ELS	Motor-driven pump external leakage (small)	Gamma	3.42E-07	0.73	2.14E+06	2	6.99E+06	2.73	9.13E+06	2.99E-07
MDP-NR-FTR	Motor-driven pump fails to run, normally running	Gamma	3.53E-06	2.29	6.50E+05	3	1.40E+06	5.29	2.05E+06	2.58E-06
MDP-NR-FTS	Motor-driven pump fails to start, normally running	Beta	1.36E-03	3.28	2.41E+03	11	1.08E+04	14.30	1.32E+04	1.08E-03
MDP-SBY-FTR<1H	Motor-driven pump fails to run, early	Beta	1.23E-04	1.82	1.48E+04	1	5.30E+03	2.82	2.01E+04	1.40E-04
MDP-SBY-FTR>1H	Motor-driven pump fails to run, long-term	Gamma	1.04E-05	0.78	7.50E+04	1	1.40E+06	1.78	1.48E+06	1.21E-06

Table 7 2 Plant Specific Failure Template Events (cont.)

Template Rule	Description	Prior Distribution				Plant Experience		Posterior Distribution		
		Type	Mean	a	b	Events	Demands/ Hours	a	b	Mean
MDP-SBY-FTS	Motor-driven pump fails to start, normally standby	Beta	9.47E-04	1.95	2.05E+03	11	1.08E+04	12.90	1.29E+04	1.00E-03
MDP-SWS-FTR	Service water motor-driven pump fails to run	Gamma	6.60E-06	1.27	1.93E+05	0	6.05E+05	1.27	7.98E+05	1.59E-06
MDP-SWS-FTS	Service water motor-driven pump fails to start	Beta	9.08E-04	1.06	1.16E+03	6	3.40E+03	7.06	4.56E+03	1.55E-03
MOV-ELS	Motor-operated valve external leakage (small)	Gamma	3.28E-08	0.48	1.45E+07	0	3.70E+07	0.48	5.15E+07	9.23E-09
MOV-FC	Motor-operated feed control valve fails to operate	Gamma	6.62E-08	1.46	2.21E+07	5	3.70E+07	6.46	5.90E+07	1.09E-07
MOV-FTC	Butterfly valve fails to close	Beta	9.63E-04	2.05	2.12E+03	6	5.19E+04	6.50	5.18E+04	1.25E-04
MOV-FTO	Butterfly valve fails to open	Beta	9.63E-04	2.05	2.12E+03	9	5.19E+04	11.00	5.40E+04	2.05E-04
MOV-FTOC	Butterfly valve fails to open/close	Beta	9.63E-04	2.05	2.12E+03	17	5.19E+04	19.00	5.40E+04	3.53E-04
MOV-ILS	Motor-operated valve internal leakage (small)	Gamma	1.01E-07	0.65	6.48E+06	0	3.70E+07	0.66	4.35E+07	1.51E-08

Table 7 2 Plant Specific Failure Template Events (cont.)

Template Rule	Description	Prior Distribution				Plant Experience		Posterior Distribution		
		Type	Mean	a	b	Events	Demands/ Hours	a	b	Mean
MOV-SOP	Motor-operated valve fails to remain open	Gamma	3.39E-08	0.57	1.68E+07	1	3.70E+07	1.57	5.38E+07	2.92E-08
MSV-ELS	Main steam isolation valve external leakage (small)	Gamma	1.34E-07	7.50	5.60E+07	0	1.96E+06	7.50	5.79E+07	1.30E-07
MSV-FTOC	Main steam isolation valve fails to open/close	Beta	7.79E-04	23.50	3.02E+04	0	7.53E+02	23.50	3.09E+04	7.60E-04
MSV-ILS	Main steam isolation valve internal leakage (small)	Gamma	1.51E-06	84.50	5.60E+07	0	1.96E+06	84.50	5.79E+07	1.46E-06
MSV-SOP	Main steam isolation valve spurious operation	Gamma	3.84E-07	21.50	5.60E+07	1	1.96E+06	22.50	5.79E+07	3.89E-07
PDP-ELS	Positive displacement pump external leakage (small)	Gamma	7.40E-07	14.50	1.96E+07	0	2.45E+05	14.50	1.98E+07	7.31E-07
PDP-NR-FTR	Positive displacement pump fails to run, normally running	Gamma	2.30E-05	1.15	5.01E+04	0	2.82E+02	1.15	5.03E+04	2.29E-05
PDP-NR-FTS	Positive displacement pump fails to start, normally running	Beta	3.15E-03	1.02	3.23E+02	1	5.18E+02	2.02	8.40E+02	2.40E-03
PORV-ELS	Power-operated relief external leakage (small)	Gamma	1.19E-07	5.50	4.63E+07	0	1.47E+06	5.50	4.77E+07	1.15E-07

Table 7 2 Plant Specific Failure Template Events (cont.)

Template Rule	Description	Prior Distribution				Plant Experience		Posterior Distribution		
		Type	Mean	a	b	Events	Demands/ Hours	a	b	Mean
PORV-FC-MSS	Main steam power-operated relief fails to control (cooldown)	Gamma	2.69E-07	8.50	3.16E+07	0	9.82E+05	8.50	3.25E+07	2.61E-07
PORV-FTC-PPR	One pressurizer PORV/SRV fails to reclose	Beta	9.66E-04	4.50	4.65E+03	0	4.03E+01	4.50	4.69E+03	9.58E-04
PORV-FTO-PPR	Pressurizer power-operated relief/dump valve fails to open	Beta	3.54E-03	16.50	4.64E+03	0	4.03E+01	16.50	4.68E+03	3.51E-03
PORV-ILS	Power-operated relief valve internal leakage (small)	Gamma	5.08E-07	23.50	4.63E+07	0	1.47E+06	23.50	4.77E+07	4.92E-07
PORV-SOP	Power-operated relief valve spurious opening	Gamma	4.65E-07	21.50	4.63E+07	2	1.47E+06	23.50	4.77E+07	4.92E-07
ROD-FTOP	Control rod fails to operate/insert rod	Gamma	2.98E-07	28.50	9.56E+07	0	1.31E+07	28.50	1.09E+08	2.62E-07
ROD-SOP	Control rod spurious operation	Gamma	1.94E-07	18.50	9.56E+07	0	1.31E+07	18.50	1.09E+08	1.70E-07
SOV-ELS	Solenoid-operated valve external leakage (small)	Gamma	3.43E-08	4.50	1.31E+08	0	3.31E+06	4.50	1.35E+08	3.34E-08
SOV-FC	Solenoid-operated valve fails to control	Gamma	4.68E-07	61.50	1.31E+08	0	3.31E+06	61.50	1.35E+08	4.57E-07

Table 7 2 Plant Specific Failure Template Events (cont.)

Template Rule	Description	Prior Distribution				Plant Experience		Posterior Distribution		
		Type	Mean	a	b	Events	Demands/ Hours	a	b	Mean
SOV-ILS	Solenoid-operated valve internal leakage (small)	Gamma	1.79E-07	23.50	1.31E+08	1	3.31E+06	24.50	1.35E+08	1.82E-07
SOV-SOP	Solenoid-operated valve spurious opening or closing	Gamma	3.43E-08	4.50	1.31E+08	0	3.31E+06	4.50	1.35E+08	3.34E-08
SVV-ELS	Code safety valve external leakage (small)	Gamma	2.79E-08	4.50	1.61E+08	0	5.52E+06	4.50	1.67E+08	2.70E-08
SVV-FTC-PWR-MSS	Main steam code safety relief valve (SVV) fails to close	Beta	1.69E-04	2.50	1.48E+04	0	1.34E+02	2.50	1.49E+04	1.67E-04
SVV-FTO-PWR-MSS	Main steam code safety relief valve (SVV) fails to open	Beta	4.51E-04	0.50	1.12E+03	0	1.34E+02	0.50	1.25E+03	4.02E-04
SVV-ILS	Code safety valve internal leakage (small)	Gamma	8.99E-08	14.50	1.61E+08	0	5.52E+06	14.50	1.67E+08	8.69E-08
SVV-SOP-PWR-MSS	Main steam code safety relief valve (SVV) spurious operation	Gamma	6.96E-08	9.50	1.37E+08	0	4.91E+06	9.50	1.41E+08	6.72E-08
SVV-SOP-PWR-RCS	Pressurizer code safety relief valve (SVV) spurious operation	Gamma	2.21E-07	5.50	2.48E+07	0	6.14E+05	5.50	2.55E+07	2.16E-07
TBV-FC	Turbine bypass valve fails to control	Gamma	1.05E-06	18.50	1.75E+07	0	2.95E+06	18.50	2.05E+07	9.03E-07

Table 7 2 Plant Specific Failure Template Events (cont.)

Template Rule	Description	Prior Distribution				Plant Experience		Posterior Distribution		
		Type	Mean	a	b	Events	Demands/ Hours	a	b	Mean
TDP-ELS	Turbine bypass valve external leakage (small)	Gamma	7.20E-07	14.50	2.02E+07	0	2.45E+05	14.50	2.04E+07	7.11E-07
TDP-SBY-FTR<1H	Turbine-driven pump fails to run, early	Beta	4.43E-03	0.96	2.16E+02	1	2.15E+02	1.96	4.31E+02	4.55E-03
TDP-SBY-FTR>1H	Turbine-driven pump fails to run, long-term	Gamma	1.56E-03	12.50	8.03E+03	0	4.12E+02	12.50	8.44E+03	1.48E-03
TDP-SBY-FTS	Turbine-driven pump fails to start, normally standby	Beta	6.49E-03	0.94	1.44E+02	3	5.19E+02	3.94	6.60E+02	5.93E-03
TFM-FTOP	Transformer fails to operate	Gamma	9.44E-07	0.96	1.01E+06	0	4.91E+05	0.96	1.50E+06	6.36E-07
TNK-PRESS-LIQ-ELS	Pressurized liquid tank external leakage (small)	Gamma	3.26E-07	6.50	1.99E+07	0	2.45E+05	6.50	2.02E+07	3.22E-07
TNK-UNPRESS-LIQ-ELS	Unpressurized liquid tank external leakage (small)	Gamma	2.60E-07	6.50	2.50E+07	0	2.45E+05	6.50	2.52E+07	2.58E-07

7.3 Common-Cause Failure Events

Basic events representing CCFs in the L3PRA project Level 1 model are a mix of reference plant PRA model events and events merged in from the existing reference plant SPAR model. The result is a collection of CCF events that includes all existing reference plant SPAR model CCF events and the reference plant PRA model CCF events not superseded by the SPAR model events. The alpha factor method was used to estimate probabilities for all CCF events in the model. Table 7-3 provides a summary of the CCF event templates supporting the L3PRA project Level 1 model significant basic events. Reference plant-specific alpha factors were not generated for any of the templates, as CCF failure populations are generally too small for credible plant-specific results.

Table 7-3 Summary of the L3PRA Project Level 1 Model CCF Template Events

Template	Description	Plant-Specific Q_t Values	Plant-Specific Alpha Factors
BAT-LP	Batteries fail to operate	Yes	No
BCH-FC	Battery chargers fail to operate	Yes	Yes
CCW-HTX-PG	Component cooling water system heat exchanger plugging	Yes	No
CKV-CC	Check valves fail to open	No	No
CRB-CC	Circuit breakers fail to open on demand	Yes	No
CTF-FS	Cooling tower fans fail to start	No	No
DGN-FR	EDGs fail-to-run and fail to load/run	Yes	No
DGN-FS	EDGs fail to start	Yes	No
EPS-MDP-FR	EDG fuel oil transfer pumps fail to run	Yes	Yes
EPS-MDP-FS	EDG fuel oil transfer pumps fail to start	Yes	Yes
ESF-ACT	ESFAS trains fail to operate	Yes	Yes
INV-FC	Inverters fail to operate	Yes	Yes
MDP-FR	Motor-driven pumps fail to run	Yes	No

MDP-FS	Motor-driven pumps fail to start	Yes	No
MOT-FS	HVAC fans fail to start	No	No
MOV-CC	Motor-operated valves fail to open	Yes	No
MOV-OO	Motor-operated valves fail to close	Yes	No
PND-CC	EDG ventilation dampers fail to open	No	No
RLY-FC	Relays fail during operation	Yes	Yes
ROD-FC	Mechanical failure of control rods to drop	No	No
SCV-CC	Stop check valves fail	Yes	Yes
SEQ-FO	Emergency power system load sequencers fail to operate	No	No
SMP-PG	Emergency core cooling system (ECCS) containment sump plugs	No	No
SWS-MDP-FR	Service water system pumps fail to run	Yes	No
SWT-FC	Service water temperature switches fail	Yes	Yes
TFF-CCF	AFW system min-flow line flow transmitters fail	Yes	No

7.3.1 Alpha Factors

Estimates of the probability of a CCF event involving *k* specific components in a CCCG of size *m* were obtained using the alpha factor method as described in NUREG/CR-5485, "Guidelines on Modeling Common-Cause Failures in Probabilistic Risk Assessment" (NRC, 1998). Reasons for this choice include:

- It is a multi-parameter model that can handle any redundancy level.
- It is based on ratios of failure rates that makes the assessment of its parameters easier when no statistical data are available.
- It has a simpler statistical model, and produces more accurate point estimates and uncertainty distributions, compared to other parametric models that have the above two properties.

NUREG/CR-5485 recommends developing common-cause alpha factors by system, component, and failure mode. INL implements these recommendations in its NRC-sponsored data collection program using the guidance summarized in NUREG/CR-6928 and in "System

and Component Descriptions, Boundaries, and Failure Modes," (INL, 2016). The alpha factors developed by INL used in the L3PRA project Level 1 model were generated using the CCF Calculator on the NRC Reactor Operating Experience Data Website. The shared rules used to generate the alpha factor set are titled "SPAR Rules 2010." The resulting alpha factors are the same as those used in the 2010 data update for the SPAR models published on the NRC Reactor Operational Experience Results and Databases Website (annotated as "No" in Table 7-3, "Plant Specific Alpha Factors" column). Plant specific alpha factors taken from the Reference Plant PRA were used in certain cases (annotated as "Yes" in Table 7-3, "Plant Specific Alpha Factors" column).

7.3.2 SAPHIRE CCF Calculation Types

SAPHIRE has built-in calculation types for CCF modeling. They are "R" and "Q" calculation types. Both calculation types implement Equation 5.6 or 5.7 from NUREG/CR-5485, the former being for staggered testing, and the latter for non-staggered testing. The "R" type is used for CCF basic events for which a probability is required, and the "Q" type is used for CCF basic events for which a frequency is required (i.e., initiator components in support system initiating event fault tree models). The SAPHIRE-calculated CCF probabilities in the L3PRA project Level 1 model all use the non-staggered testing option, which is correct for all applications in which the alpha factor estimators already account for the testing scheme in use when the data was collected.

The SAPHIRE built-in calculation types require as inputs the total failure probability basic events for each component in the CCCG, and alpha factor basic events corresponding to the individual alpha factors for the component group. In the L3PRA project Level 1 model the SAPHIRE option to use expanded virtual CCF events is used. The virtual events are system-generated events that correspond to the $\boldsymbol{Q_k^{(m)}}$ events in Equations 5.6 and 5.7 of NUREG/CR-5485. These events are placed in the fault tree logic as demonstrated in NUREG/CR-5485.

7.3.3 CCF Event Simplifications

As mentioned previously, SAPHIRE has "R" and "Q" calculation types to calculate CCF probabilities for each combination of component failure that can occur in a CCCG. In many cases the L3PRA project Level 1 model uses just one event for the entire CCCG. This is the preferred or default case where CCF events for each failure combination in the CCCG are rolled-up into one event for the group. In other cases, it may be desirable to use some or all events representing specific CCCG component combinations in the fault tree logic. This represents the "expanded" case for CCF event usage. The expanded case is used when cross-products between detailed CCF events in the CCCG and events outside the CCCG are thought to be important, or in which the use of rolled-up events may lead to excessive conservatism in the result.

An important example for the use of the "expanded" events is in the nuclear service cooling water (NSCW) fault tree logic. The CCCG for the NSCW pumps comprises 6 trains and 202 permutations of pump failure events (excluding combinations of only independent events). While it was reasonable to include all permutations of pump failure in the support system fault tree logic, including all the combinations in the support system initiating event (SSIE) tree version of the same fault tree would have required a huge amount of modeling effort for a minimal refinement in the final core damage frequency cut set equation. Therefore, in this case, only the specific permutations involving four or more pumps in the group were used in the fault

tree model (which corresponds to the CCF events capable of defeating the system success criteria in a single element cut set).

7.4 Offsite Power Recovery Failure Events

The offsite power recovery failure probabilities used in the L3PRA project Level 1 model are based on NUREG/CR-6890 (NRC, 2005a) and its online updates. This NUREG/CR provides loss of offsite power (LOOP) frequency and duration data that are the basis for the non-recovery probabilities used in the L3PRA project Level 1 model. Four LOOP subcategories are defined as follows:

- *Plant Centered.* A LOOP event in which the design and operational characteristics of the nuclear power plant itself play the major role in the cause and duration of the loss of offsite power. The line of demarcation between plant-centered and switchyard-centered LOOP events is the nuclear power plant main and station transformer high-voltage terminals. Both transformers are part of the switchyard.

- *Switchyard Centered.* A LOOP event in which the equipment, whether human-induced or actual equipment failure, in the switchyard play the major role in the loss of offsite power.

- *Grid Related.* A LOOP event in which the initial failure occurs in the interconnected transmission grid that is outside the direct control of plant personnel.

- *Weather Related.* A LOOP event caused by severe or extreme weather, in which the weather is widespread, not just centered at the site, and capable of major disruption. Severe weather is defined to be weather with forceful and non-localized effects.

7.4.1 Non-Recovery Probabilities

The probability that offsite power will not be recovered by time t is the fraction of all LOOP events (for the LOOP category under consideration) with duration L greater than t, or

$$P(L > t) = \int_t^\infty f_L(l)dl = 1 - F_L(t) \tag{1}$$

Where f_L is the density function for the distribution of observed LOOP durations, and F_L is the cumulative distribution form of f_L.

NRC (2005a) provides lognormal density and cumulative distribution functions for L in the form

$$f_L(t) = \frac{1}{t\sqrt{2\pi}\sigma} e^{-\frac{1}{2}\left|\frac{\ln(t)-u}{\sigma}\right|} \tag{2}$$

$$F_L(t) = \Phi\left[\frac{\ln(t) - u}{\sigma}\right] \tag{3}$$

where

t = offsite power recovery time

u = mean of natural logarithms of data

σ = standard deviation of natural logarithms of data

Φ = cumulative distribution function

Table 7-4 provides the parameters used to evaluate Equation 1. The calculation is handled automatically by a SAPHIRE plug-in. Figure 7-1 provides the resulting offsite power non-recovery curves used in the model. Events using the offsite power recovery failure calculation are named OEP-XHE-XL-NR*****; where ***** represents the sequence-specific time available for recovery of offsite power for specific class of LOOP (e.g., OEP-XHE-XL-NR02HPC is failure to recover from a plant-centered loss of offsite power [PC] in 2 hours [02H]).

Table 7-4 LOOP Recovery Curve Parameters

LOOP Category	Recovery Curve Parameter	Uncertainty Distribution Type	Uncertainty Parameter	Basic Event
Plant Centered	5.40E-01	Lognormal	1.50E+00	ZV-SBO-REC-PC-Median
	10.1E+00	Lognormal	1.60E+00	ZV-SBO-REC-PC-EF
Switchyard Centered	7.12E-01	Lognormal	1.31E+00	ZV-SBO-REC-SC-Median
	9.38E+00	Lognormal	1.36E+00	ZV-SBO-REC-SC-EF
Grid Related	1.51E+00	Lognormal	1.54E+00	ZV-SBO-REC-GR-Median
	5.29E+00	Lognormal	1.65E+00	ZV-SBO-REC-GR-EF
Weather Related	2.71E+00	Lognormal	2.16E+00	ZV-SBO-REC-WR-Median
	2.89E+01	Lognormal	2.45E+00	ZV-SBO-REC-WR-EF

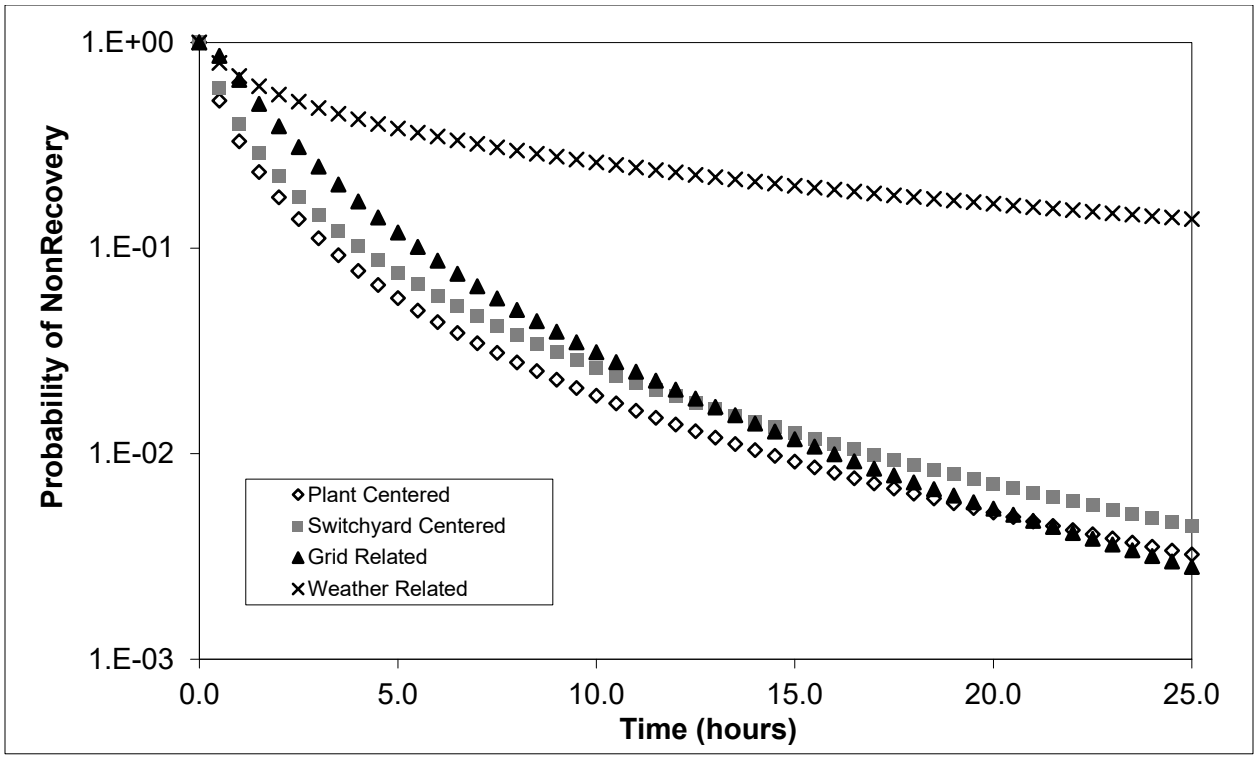


Figure 7-1 Offsite Power Non-Recovery Probabilities

Convolution Corrections

The L3PRA project Level 1 model and some industry risk models take a similar approach to analyzing the risk associated with LOOP and subsequent station blackout (SBO) events. The key elements in determining the core damage risk are the reliability of the emergency power system, the reliability of the equipment used to cope in the absence of emergency power, and the likelihood that offsite power can be recovered or restored before the core is damaged from inadequate core cooling. The following discussion will address some of the conservatisms implicit in these models and demonstrate how the conservatism is reduced in the L3PRA project Level 1 model.

The LOOP/SBO dominant cut sets for a power plant with two divisions of emergency power typically contain the following:

- [Offsite power is lost] AND [EDG 1 fails to start] AND [EDG 2 fails to start] AND [Operator fails to recover offsite power]

- [Offsite power is lost] AND [EDG 1 fails to run] AND [EDG 2 fails to run] AND [Operator fails to recover offsite power]

The first of the above two cut sets can be accurately quantified by multiplying event probabilities because there are no complex timing issues that need to be accounted for. The second cut set implies timing issues that are typically addressed through a series of conservative simplifying assumptions:

- If two EDGs fail to run, they fail at the same time, and that time is when the LOOP first occurs.

- The time available to recover offsite power is counted from when the LOOP first occurs.

- The time to core damage, given inadequate core cooling, is constant. It does not increase as decay heat levels decrease following successful initial core cooling.

There is generally a limiting time in which the recovery of AC power must occur. The limiting time is often based on the time required to uncover the core given a total loss of core cooling but may instead be based on battery depletion time or other sequence-based timing considerations. The key conservatism here is that the time at which core cooling is lost is assumed to be the time at which the LOOP occurs. In the first cut set, all core cooling depends on the two EDGs; therefore, core cooling is lost when the LOOP occurs and the EDGs fail to start. In this case the time available to recover AC power (and therefore core cooling) is the core uncovery time. In the second cut set, the calculations can be simplified to assume both EDG fail-to-run events occur when the LOOP does; however, this is also unrealistic. A more probable scenario is that both EDGs are initially running and EDG 1 fails at t_1 hours. At this point, EDG 2 is still running and powering decay heat removal systems. If EDG 2 then fails at t_2 hours, then core cooling is lost at t_2 hours instead of at t_0. If the timing constraint on the cut set is based on the core uncovery time (t_{cu}) then the time available for offsite power recovery is not just t_{cu} hours; it is $t_2 + t_{cu}$ hours. A realistic model must account for all possible failure and recovery scenarios and it would take direct simulation or Markov modeling to determine the probabilities. However, most of the conservatism can be addressed by analytical evaluation of the EDG fail-to-run cut sets and recovery of offsite power.

The following method is developed from basic reliability equations and designed to address the largest conservatism in the above cut sets. The goal is to develop expressions for the unreliability probability density function and cumulative distribution function for the fail-to-run and fail-to-recover offsite power cut sets above. The method that follows is designed for solution using an Excel spreadsheet.

"Reliability and Risk Analysis Methods and Nuclear Power Applications" (McCormick, 1981) states that the probability that some device will not fail between *0* and *t* is the reliability of the device, *R(t)*, where

$$R(t) = \exp\left[-\int_0^t \lambda(t')dt'\right] \tag{4}$$

The quantity $\lambda(t)$ is called the hazard rate. The quantity $\lambda(t)dt$ represents the probability the device fails in *dt* about *t*, given successful operation to *t*. The starting point for the spreadsheet model is the basic reliability equation for devices (in this case, EDGs) in active parallel operation; either device 1 or device 2 must operate for system success:

$$R_{sys}(t) = R_1(t) + R_2(t) - R_1(t) \cdot R_2(t) \tag{5}$$

Where

$R_1(t)$ = The probability EDG 1 operates to time *t*

$R_2(t)$ = The probability EDG 2 operates to time *t*

$R_{sys}(t)$ = The probability the emergency power system operates to time *t*

For exponentially distributed failure times, $\lambda(t) = \lambda$:

$$R_{sys}(t) = \exp(-\lambda_1 t) + \exp(-\lambda_2 t) - \exp[-(\lambda_1 + \lambda_2)\, t] \tag{6}$$

For a device in continuous operation, that does not undergo repair, the probability the device operates to time *t* and fails in time *dt* about time *t* as:

$$f(t)\,dt = R(t)\,\lambda(t)\,dt = \left[1 - F(t)\right]\lambda(t)\,dt \tag{7}$$

The quantity $F(t)$ is the probability the device will fail between *0* and *t* and is called the device unreliability, which is just $1 - R(t)$. To construct the expression for failure of the emergency power system with failure to recover offsite power, start with Equation 7 and multiply by the offsite power recovery failure probability:

$$f(t)\,dt = R_{sys}(t)\,\lambda_{sys}(t)\,dt\,[1 - F_L(t + t_{cu})] = [1 - F_{sys}(t)]\,\lambda_{sys}(t)\,dt\,[1 - F_L(t + t_{cu})] \tag{8}$$

In this expression the quantity $R_{sys}(t)$ represents the probability that one of the diesels operates to time *t*. The quantity $\lambda_{sys}(t)\,dt$ represents the probability of emergency power failure in *dt* about *t*, given successful operation to *t*, and the quantity $1 - F_L(t + t_{cu})$ represents failure to recover offsite power before the core is uncovered. The t_{cu} term is generally assumed to be constant, but increases with the passage of time. Therefore, additional conservatism can be removed by expressing t_{cu} as a function of time, $t_{cu}(t)$. The $\lambda_{sys}(t)$ term above is the system hazard rate which can be determined from either the system reliability or unreliability as follows:

$$\lambda_{sys}(t) = \frac{dF_{sys}(t)/dt}{1 - F_{sys}(t)} \approx \frac{\Delta F_{sys}/\Delta t}{1 - F_{sys}(t)} \approx -\frac{\Delta R_{sys}/\Delta t}{R_{sys}(t)} \tag{9}$$

The $F_L(t + t_{cu})$ term in Equation 8 represents the cumulative distribution function for the loss-of-offsite power duration data, that is, the fraction of all loss of offsite power events with duration less than or equal to $t + t_{cu}$.

The system failure probability density, with credit for offsite power recovery, and in a form suitable for spreadsheet solution, is then:

$$f(t)dt = \left[1 - F_{sys}(t)\right]\frac{\Delta F_{sys}/\Delta t}{1 - F_{sys}(t)}\,dt\,\left[1 - F_L(t + t_{cu})\right] \tag{10}$$

The above expression can be written using either R_{sys} or F_{sys}. The expression is cast in terms of F_{sys} to take advantage of the higher numerical precision that is possible this way. The last step required is to integrate the probability density function to get the cumulative failure probability $F(t)$. This can be done with sufficient accuracy using the Trapezoidal Rule:

$$F(t) = \int_0^t f(t')dt' \approx \sum_{i=0}^{n} h\left[\tfrac{1}{2} f(t_i) + \tfrac{1}{2} f(t_{i+1})\right] \tag{11}$$

Where *h* is a constant time step $t_{i+1} - t_i$, and *n* is the number of time steps between *0* and *t*. All terms in Equations 10 and 11 can be calculated using functions available within Excel. A 1-hour time step provides an adequate level of accuracy for the two-EDG system described above. A

0.10-hour time step for a 24-hour mission produces a result that agrees with MathCAD solution using an alternate formulation to three significant figures.

Once the correct cut set probability is obtained, a correction factor event is obtained by dividing the convolved results by the nominal result. The correction factor event is then added to appropriate combinations of EDG fail-to-run cut sets by SAPHIRE recovery rules.

7.5 Parameter Uncertainty

Most basic events used in the L3PRA project Level 1 model (for internal events) include parameter uncertainty distributions. Demand-based component failure probabilities are based on binomial failure models and have beta-distributed parameters. Time-based component failure probabilities are based on Poisson failure models and have gamma-distributed parameters. CCF events are either demand-based or time-based and have uncertainty distributions developed by propagating the related total failure probability event uncertainty and alpha factor parameter uncertainty (beta-distributed) through the SAPHIRE CCF event computation. HFE probabilities are based on a lognormal model and are characterized by a mean and error factor. The L3PRA project Level 1 model also includes a few events for which there is no current basis for assigning uncertainty distributions, for example, the probability a loss-of-coolant accident (LOCA) occurs on a specific cooling loop. In this case each of the four loops is assumed to be an equally probable location for the LOCA and no uncertainty distribution is provided for the probability.

The 2010 update to NUREG/CR-6928 provides the prior distributions for Bayesian estimation of plant-specific failure probabilities, and for direct use in cases where plant-specific values did not appear to be supported by the data. Additional information on parameter uncertainty derivation and estimation are provided in Section 4 of NUREG/CR-6928, and its appendices.

The plant-specific estimates described in preceding sections result from a Bayesian process that naturally provides uncertainty distributions for the posterior values. The beta and gamma distribution provided in the 2010 update provide conjugate priors for the update process, which produces posterior beta and gamma distributions defining each failure estimate. Table 7-2 summarizes the prior distribution inputs and posterior distribution outputs for all plant-specific estimates. In addition, Appendix A contains similar information for each basic event in the L3PRA project Level 1 model.

The following two sections provide additional information on the parameter uncertainty associated with initiating event frequencies and human error probabilities, respectively.

7.5.1 Initiating Events

Initiating event frequencies estimated from event occurrence data use Poisson failure models and are characterized by gamma-distributed rate parameters that are summarized in Table 2-1. Initiating event frequencies that are estimated from SSIE fault trees do not have simple distribution forms. In these cases, the initiating event uncertainty distributions are obtained from a fault tree result in which basic event uncertainties are propagated to the top event through a Monte Carlo analysis. No attempt was made to fit uncertainty distributions to the SSIE fault tree output, although the output distributions tend to be approximately lognormal and distribution parameters could be computed from the percentiles in Table 2-1. Results from SSIE fault trees are part of the core damage frequency equation; therefore, a Monte Carlo analysis of the core damage cut set equation includes the SSIE fault tree uncertainty contribution.

7.5.2 Human Failure Events

The execution human error probability (HEP) is calculated through the application of the Technique for Human Error Rate Prediction (THERP) method (NRC, 1983). The THERP HEP value is considered a median value, but the HRA Calculator (EPRI, 2011) converts it to a mean value. This mean execution HEP value is added to the cognitive HEP value (calculated either through the application of Human Cognitive Reliability/Operator Reliability Experiments [HCR/ORE] or Cause Based Decision Tree [CBDT], EPRI, 1992) to obtain the final mean HEP value. To estimate the uncertainty of the HEPs, the following approach was developed:

- The HFEs are assumed to have lognormally distributed failure probabilities.
- If the mean value of any HEP is greater than 0.95, then the mean HEP will be set to 1.0 and it will be used as a place holder for future applications when the shaping factors (e.g., procedures, training, etc.) used to evaluate the HEP are changed.
- Error factors (EFs) for HEPs with a mean less than 10^{-3} will be set to 10. For HEPs with a mean between 10^{-3} and 0.95, an EF of 5 will be applied.[207]

However, using the above approach for HEPs with relatively high means and error factors, can lead to some Monte Carlo samples being discarded by SAPHIRE during the uncertainty analysis, because the sampled probabilities exceed 1.0. To minimize the number of discarded samples, the error factors for these events were adjusted to preserve the mean value and anchor the 95th percentile of the distribution to a value of approximately 0.95. This replacement does not affect the point estimate calculations, which use the mean values.

[207] As described by items 4 and 5 of Table 20-20 of NUREG/CR-1278, "Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications," (NRC, 1983). Items 4 and 5 are applied for tasks consisting of the performance of step-by-step procedures but carried out in non-routine circumstances. Originally, NUREG/CR-1278 applied median HEPs to determine the EFs. However, HCR and CBDT only estimate mean HEP values; therefore, median HEPs cannot be estimated from the mean value without their associated EFs. This approach uses the mean HEP values to estimate the EFs first, then the median HEPs can be calculated.

8 ADDITIONAL DISCUSSION OF SEVERAL KEY MODELING ASSUMPTIONS AND ISSUES

The main purpose of this section is to provide additional information on key L3PRA project Level 1 modeling assumptions and issues that either warrant further discussion given their impact on the results or that do not fit naturally into the other sections of this report. Key modeling assumptions and issues covered in this section include:

- Modeling assumptions associated with alternating current (AC) power recovery during a loss of offsite power (LOOP) and subsequent station blackout (SBO) (Section 8.1)
- Issues related to the modeling of consequential LOOPs (Section 8.2)
- The approach used in the modeling of safe/stable end states (Section 8.3)
- Plant-specific revisions to the Westinghouse Owner's Group (WOG) 2000 reactor coolant pump (RCP) seal leakage model (Westinghouse, 2002) (Section 8.4)
- Modeling of consequential steam generator tube rupture (SGTR) (Section 8.5)

8.1 AC Power Recovery

The recovery of AC power is the only SSC recovery credited in the L3PRA project Level 1 model. The recovery of AC power was limited to SBO scenarios resulting from LOOP initiating events and consequential LOOPs. The general assumptions for AC power recovery in the L3PRA project Level 1 model are similar for these two classes of LOOPs; however, some differences exist due to the fault tree modeling approach used for consequential LOOPs (see Section 8.2 for additional information on the modeling of consequential LOOPs). The key modeling assumptions for AC power recovery during an SBO resulting from a LOOP initiating event are:

- No credit was allowed for recovery of offsite power following depletion of the (most limiting) plant batteries required to realign offsite power to a safety-related bus (i.e., turbine building batteries—2 hours). See Section 8.1.1 for additional information.
- No credit is provided in the L3PRA project Level 1 model for the continued operation of the turbine-driven AFW pump after direct current (DC) power is lost; however, credit for continued operation of the turbine-driven auxiliary feedwater (AFW) is provided in the Level 2 portion of the L3PRA project model. See Section 8.1.2 for additional information.
- Credit for aligning offsite power from the alternate switchyard via the station auxiliary transformer (SAT) was included in SBO sequences for plant-centered and switchyard-related LOOPs. See Section 8.1.3 for additional information.
- Convolution corrections were included for EDG fail to run events and recovery of offsite power. See Section 7.4.2 for additional information.

8.1.1 AC Power Recovery during SBO

In the L3PRA project Level 1 model, AC power recovery is credited for LOOP events that result in a subsequent SBO. For LOOP initiating events, AC power (offsite power or the alternate switchyard) recovery is credited via the applicable OPR fault trees (see Section 5.1.30 for additional information).[208] However, AC power recovery is not applied to SBO scenarios that are a result of SSC failures that would render AC power either unrecoverable or ineffective. Therefore, the OPR fault tree logic was structured such that AC power credit is not applied to SBO cut sets (that result from LOOP initiating events) in which each safety-related train is failed due to either: (1) reserve auxiliary transformer (RAT) output breaker failure to open, (2) sequencer failure, (3) NSCW failure with subsequent RCP seal LOCA, or (4) unavailabilities of the safety-related batteries.[209]

The L3PRA project Level 1 model includes three different sets of batteries: (1) the safety-related batteries (4-hour battery life) that supply DC power to the breakers/switchers downstream of the RATs; (2) the turbine building batteries (2-hour battery life) that supply DC power to circuit switchers directly upstream of the RATs; and (3) the switchyard batteries (4-hour battery life) that supply DC control power to the circuit breakers that are located in the high-voltage switchyard (immediately downstream of 230kV bus 1 and bus 2). The SBO procedure (ECA-0.0) provides direction for shedding unnecessary DC loads on the safety-related batteries, but does not address prolonging the life of the turbine building batteries. Therefore, the turbine building batteries have the limiting depletion time for realigning offsite power to safety-related 4.16 kV AC buses A and B.

Realignment of offsite power requires that DC power be available to operate some of the breaker and switchers. It is not clear how operators would respond if the prerequisite for DC power is not met. Some of the breakers and switchers that are needed to restore offsite power to safety-related 4.16 kV AC buses A and B can be operated manually with a local hand crank, while some cannot be operated manually without DC power. Given this, the L3PRA project Level 1 model uses the potentially conservative assumption that AC power must be recovered prior to depletion of the most limiting plant batteries required to realign offsite power to a safety-related bus.

8.1.2 Turbine-Driven AFW Pump Operation without DC Power

Continued operation of the turbine-driven AFW pump after DC power is lost is possible. This action could delay the time to when core damage occurs (or prevent it). However, the L3PRA project Level 1 model assumes that AC power recovery must occur prior to depletion of the most limiting plant batteries (i.e., the turbine building batteries); therefore, credit for “blind” operation of the turbine-driven AFW pump is not provided, since the plant would not be in a stable condition (due to continual RCP seal leakage). Without reliable indication of SG water level (after the safety-related batteries are depleted at four hours), there is significant potential for unsustainable operation (e.g., overfilling the steam generators (SGs) and flooding the steam lines, including the AFW pump turbine); and therefore, any potential credit would be minimal.

---

[208] Credit for the alternate switchyard is described further in Section 8.1.3.

[209] The top 200 L3PRA Project Level 1 model cut sets were reviewed to identify additional SBO cut sets containing other SSC failures that may render AC power either unrecoverable or ineffective. This review revealed no additional failures/unavailabilities that could also render AC power non-recoverable. Therefore, the potential application of AC power recovery to any additional cut sets in which the failure may preclude (or render moot) AC power recovery is expected to have a negligible impact on the overall CDF.

However, the L3PRA project Level 2 model does apply some credit for "blind" feeding of the turbine-driven AFW pumps as a means of extending the time to core damage to approximately 140 hours.[210] At approximately 140 hours, decay heat removal is no longer the limiting factor (inventory loss through the RCP seals becomes limiting), and core damage ensues regardless of the success of "blind" feeding using the turbine-driven AFW pump. The L3PRA project Level 2 model uses this credit to parse sequences as either (1) sequences resulting in no containment failure within 7 days or (2) sequences that should be processed by the containment event tree.

8.1.3 Recovery of AC Power via the Alternate Switchyard

Credit for aligning offsite power from the alternate switchyard via the SAT is included in SBO sequences for plant-centered and switchyard-related LOOPs. The alternate switchyard is not expected to be available during grid- and weather-related LOOPs; therefore, no credit for the alternate switchyard is provided for these LOOP types.

The procedural direction to align the alternate switchyard via the SAT is provided in ECA-0.0. Entry conditions for ECA-0.0 are that both 4.16 kV safety-related buses are deenergized; therefore, alignment of the alternate switchyard is credited for scenarios in which both these safety-related buses are deenergized. The alignment of the alternate switchyard is credited for the same SBO scenarios described in Section 8.1.1.

8.2 Consequential LOOP Events

In the L3PRA project, consequential LOOPs are modeled explicitly in the Level 1 model AC power fault tree logic, consistent with the current state-of-practice. Section 8.2.1 discusses the implementation of this consequential fault tree modeling. Additional information on other key consequential LOOP-related modeling assumptions, such as the probabilities of consequential LOOPs (Section 8.2.2) and the application of AC power recovery (Section 8.2.3), are also described below.

8.2.1 Modeling Consequential LOOP in Applicable AC Power Fault Trees

A consequential fault tree node (OEP) was created (shown in Figure 8-1) and added to applicable AC power support system fault trees (e.g., AA02-OFFSITE, BA03-OFFSITE). The fault tree logic is broken into two classes of events, transient-type initiating events and initiators that result in SI actuation (e.g., LOCAs, SSBs), because the consequential LOOP probability is different for these two types of events (see Section 8.2.2 for additional information). In addition, the OEP fault tree logic includes the potential for a random, post-trip LOOP during the PRA mission time (24 hours) via basic event OEP-VCF-LP-RLOOP.

The modeling of the potential for consequential LOOPs using the fault tree approach has the major benefit of not impacting the events trees and other fault trees; however, the following limitations are noted:

- A greater reliance on post-processing rules to apply AC power recoveries. This results in an ad-hoc application of recovery (i.e., application is based on a top-down review of dominant cut sets), rather than the complete application that would come from including

[210] This time corresponds to the "> 72 hours" time in Table 8-1, wherein ECA-0.0 depressurization has successfully occurred. If early depressurization does not occur, the 48-hour time in Table 8-1 applies.

it explicitly in both the event trees and fault trees. In addition, given the absence of event-tree-based sequence information, the different times available for AC power recovery need to be considered within the post-processing rules. See Section 8.2.3 for additional information.

- The lack of sequence information also requires simplifying assumptions for other modeling aspects (e.g., in assigning sequences to plant damage states as part of the Level 2 PRA modeling).

Due to these limitations, the consequential LOOP modeling philosophy used in the L3PRA project Level 1 model is a candidate for future study.

8.2.2 Consequential LOOP Probabilities

The current consequential LOOP probability for transient-type initiating events (basic event OEP-VCF-LP-CLOPT) used in the L3PRA project Level 1 model is taken from NUREG/CR-6890 (NRC, 2005a).[211] The probability of 5.3×10^{-3} was calculated using the number of consequential LOOPs (3) and the number of non-LOOP reactor trips (661) during the 1997–2004 period.

A recent review of the LOOP database revealed that 2 of the 3 consequential LOOPs following a reactor trip during the 1997–2004 period are no longer classified as consequential LOOPs. Also, additional operating experience has accumulated over the past decade. The revision of the consequential LOOP probabilities based on updated operating experience is a candidate for future study.

Following a reactor trip, the offsite electrical grid is taxed not only by the loss of voltage support from the reactor, but also due to the transfer of plant non-safety loads from the unit auxiliary transformer to the RATs, which are supplied from the offsite grid. Following an SI actuation, the grid is further stressed by the in-rush current that accompanies the starting of the ECCS loads, making it more likely that the safety bus degraded voltage protection relays will actuate, resulting in a consequential LOOP. The current consequential LOOP probability given an SI actuation (basic event OEP-VCF-LP-CLOPL) is 3.0×10^{-2}. This probability was obtained by applying a Jeffreys non-informative prior to the point estimate (2.0×10^{-2}) provided in "Generic Probability of a LOOP after a Large LOCA: An Evaluation," (BNL, 2006). The point estimate in (BNL, 2006) is based on the number of consequential LOOPs following a major SI actuation (1) and the total number of major SI actuations (49), from January 1, 1986 through July 31, 2006.

8.2.3 Crediting AC Power Recovery for Consequential LOOPs

The crediting of AC power recovery (offsite and the alternate switchyard) during a consequential LOOP aligns with most of the assumptions for crediting AC power recovery for LOOP initiating events (as described in Section 8.1). The main deviation for how AC power recovery is applied for consequential LOOPs (as compared to LOOP initiating events) is that recovery credit is applied solely via post-processing rules because the OEP fault tree logic (shown in Figure 8-1) does not apply the AC power recoveries. As is done for LOOP initiating events, AC power recovery was only applied for consequential LOOP cut sets that resulted in a subsequent SBO.

---

[211] The main purpose of the LOOP/SBO study (documented in NUREG/CR-6890) was to determine the potential effects of deregulation on the occurrence of LOOP events and grid reliability (including seasonal effects).

As is described in Section 8.1.1, it was determined that AC power credit should not be applied to cut sets in which each safety-related train is failed due to one of the following reasons: (1) RAT output breaker failure to open, (2) sequencer failure, (3) NSCW failure with subsequent RCP LOCA, or (4) unavailabilities of the safety-related batteries. Therefore, the EPS fault tree was solved to determine the key SSC unavailability patterns for which AC power recovery should be applied. From these results, the post-processing rules used to apply the AC power recovery given a consequential LOOP and subsequent recoverable SBO were developed.[212]

Another deviation in how AC power recovery is applied for consequential LOOPs as compared to LOOP initiating events is that the alternate switchyard is credited for all consequential LOOPs because they are all assumed to be temporary local-grid disturbances in which the alternate switchyard would be available within minutes of the event. The alternate switchyard is not credited for grid-related and weather-related LOOP initiating events.

For consequential LOOP events, the L3PRA project Level 1 models uses a 2-hour non-recovery probability for a plant-centered LOOP (OEP-XHE-XL-NR02HPC) and human failure event (HFE) for operator failure to align the alternate switchyard within 2 hours (OA-ALIGNPW-2HR).[213] The plant-centered LOOP non-recovery probabilities were chosen because their LOOP durations most closely resemble those of consequential LOOPs that have been identified (to date).[214] The actual or potential recovery time was approximately two hours or less for 8 of the 9 consequential LOOPs that were identified in NUREG/CR-6890 and NUREG-1784, “Operating Experience Assessment—Effects of Grid Events on Nuclear Power Plant Performance” (NRC, 2003b). Reevaluation of the non-recovery probabilities for consequential LOOPs is a candidate for future study.

[212] The basic event combinations contained in the applicable post-processing rules were identified from the top 100 cut sets from the EPS fault tree. Some of the resulting basic event combinations| are not recoverable in that core damage would not be avoided by recovery of offsite power or the alignment of the alternate switchyard. These combinations have been commented out of the rules instead of deleted to allow for review of the judgments that were made.

[213] For consequential LOOP scenarios with a subsequent SBO and the failure/unavailability of the turbine-driven AFW pump, operators would only have approximately 1 hour to recovery AC power. To adjust for these two scenarios, the 2-hour recoveries (offsite and the alternate switchyard) were used as the default values in the post-processing rules. However, the dominant cut sets were reviewed for consequential LOOP and subsequent SBO scenarios that included the failure/unavailability of the turbine-driven AFW pump. The post-processing rules were adjusted accordingly to include the 1-hour recoveries (i.e., OEP-XHE-XL-NR01HPS and OA-ALIGNPW-1HR) for these cut sets.

[214] Some consequential LOOPs also resemble switchyard-centered LOOPs; however, updated combined plant-centered/switchyard-centered recovery probabilities were not readily available when work was completed in this area for the L3PRA Project Level 1 model.

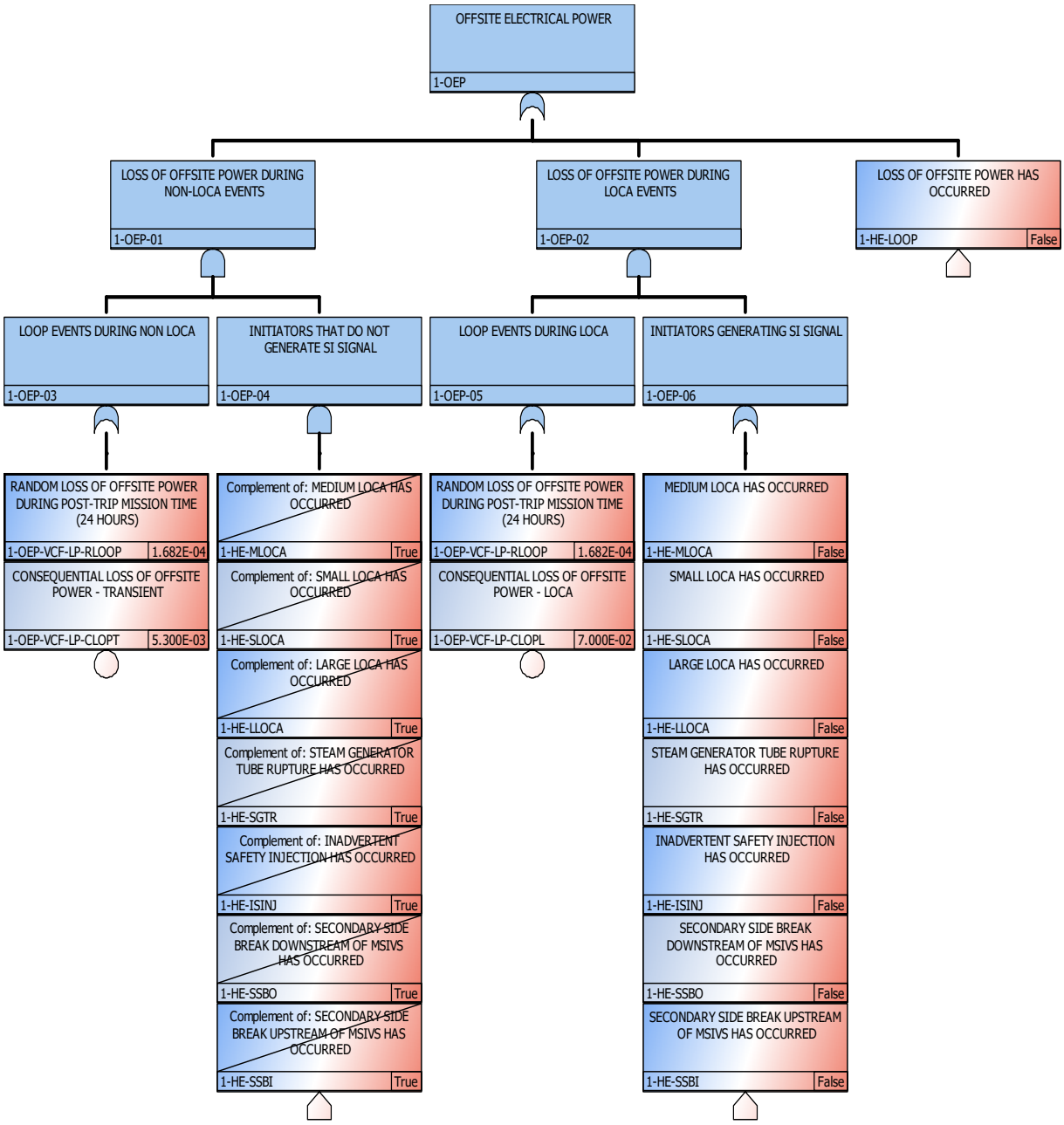


Figure 8-1 Consequential LOOP (OEP) Fault Tree Logic

Modeling of Safe/Stable End States

The American Society of Mechanical Engineers/American Nuclear Society (ASME/ANS) PRA standard (ASME/ANS, 2009) defines a safe/stable state as “a plant condition, following an initiating event, in which RCS conditions are controllable at or near desired values.” Supporting requirement AS-A2 states, “for each modeled initiating event, identify the key safety functions that are necessary to reach a safe, stable state and prevent core damage.” Supporting requirement SC-A5 elaborates by stating that (for capability category II/III) additional evaluations

must be performed for sequences where stable plant conditions are not achieved at 24 hours. Examples of appropriate evaluation techniques include assigning an appropriate plant damage state for the sequence, extending the mission time until an acceptable end-state is reached, or modeling additional system recovery or operator actions. Only in the definition of "success path" does the standard provide a later back-stop time (that being 72 hours), and the success path concept is only invoked in the seismic margins assessment. Meanwhile, NUREG-2122, "Glossary of Risk-Related Terms in Support of Risk-Informed Decisionmaking" (NRC, 2013), defines safe stable state as a "condition of the reactor in which the necessary safety functions are achieved," and goes on to state, "In a PRA, safe stable states are represented by success paths in modeling of accident sequences. A safe stable state implies that the plant conditions are controllable within the success criteria for maintenance of safety functions."

MELCOR calculations performed for the L3PRA project identified some SGTR sequences where core damage is expected to occur shortly after 30 hours. In addition, sequences involving an RCP seal leakage rate of less than or equal to 21 gallons per minute (gpm) per RCP with AFW available can eventually result in core damage if primary system make-up is not available.

To address the issue of a safe/stable end-state, several options were considered, including: (1) assigning any ambiguous sequences to core damage, (2) adjusting sequence end-times and component mission times, and (3) assigning ambiguous sequences to a new end state (e.g., core vulnerable). Ultimately, it was decided to apply the following guiding principles to the L3PRA project Level 1 model:

- For those event tree sequences that are safe (i.e., no core damage), but not stable, at 24 hours (i.e., they would result in core damage at some point after 24 hours), the model generally extends the accident sequence to 72 hours. If core damage would occur before 72 hours, additional mitigation actions (e.g., condensate storage tank (CST) refill, alternate charging alignment, or FR-C.1 inadequate core cooling emergency depressurization) are queried or the sequences are modeled as core damage sequences. If core damage does not occur before 72 hours, these sequences are modeled as "OK," even though they are not "stable." It is reasoned that a 72-hour window, since the onset of the plant upset condition, allows sufficient time that some unmodeled action using onsite or offsite resources can be taken to prevent core damage.

- The mission time for calculating equipment reliability remains 24 hours. The 72-hour window is only being applied to sequences that are safe, but not stable, at 24 hours, to determine if the "unstable condition" degrades to core damage in that time-frame, assuming plant equipment that was operable at 24 hours continues to operate for the subsequent 48 hours.

Applying these guidelines leads to multiple modeling decisions, particularly with respect to sequences that involve a loss of all RCP seal cooling and injection. Table 8-1 captures the general timeframes assumed in the L3PRA project Level 1 model for these types of sequences. The safe/stable guidelines were also used in the development of the SGTR event tree. Meanwhile, for SBO, the impact of the safe/stable issue is somewhat suppressed by the unrelated modeling assumption that AC power recovery must occur prior to battery depletion for core damage avoidance to be creditable (in conjunction with the relatively short time to battery

depletion). If AC power is recovered prior to battery depletion during an SBO, then sequences are handled analogously to how they are handled in non-SBO cases [e.g., for sequences with seal leakage of 21 gpm per RCP, re-closed PORVs, and turbine-driven AFW (with successful CST refill), either charging must be recovered to establish a safe/stable condition or SG cooldown (to allow accumulator injection) must occur to prevent core damage for at least 72 hours].[215] Additional information on specific sequence and success criteria assumptions throughout the L3PRA project Level 1 model are provided in Section 3, Section 4, and Section 5.

Table 8-1 General Timeframes for Avoiding Core Damage for Loss of RCP Seal Cooling Events (i.e., Leakage of 21 gpm per RCP)

	SBO	Loss of NSCW	Other Loss of RCP Seal Cooling
No Operator-Induced Depressurization	~ 48 hours (but n/a)[a,b]	~ 48 hours[c]	> 72 hours[d]
ECA-0.0 Depressurization	> 72 hours (but n/a)[b,e]	N/A	N/A
"Normal" Cooldown	N/A	N/A	N/A
FR-C.1/C.2 Depressurization (Including CST Refill/Makeup)	N/A (CSFSTs don't apply)	> 72 hours[c]	> 72 hours[d]
Notes a. Based on reference plant MELCOR SBO calculations. b. The L3PRA project Level 1 model does not credit blind feeding using the turbine-driven AFW during a SBO after battery depletion; however, credit is provided in the Level 2 portion of the model. c. Based on equivalency to the SBO analog. d. Based on availability of ECCS in these cases. e. Based on reference plant MELCOR SBO calculations.			

8.3 RCP Seal LOCA Modeling

The L3PRA project Level 1 model accounts for the possibility of RCP seal LOCAs by implementing the WOG 2000 RCP seal leakage model as evaluated and accepted by the NRC in "Safety Evaluation of Topical Report WCAP-15603, Revision 1, WOG 2000 Reactor Coolant Pump Seal Leakage Model for Westinghouse PWRs" (NRC, 2003c). The current SPAR models for Westinghouse pressurized-water reactors (PWRs), including the reference plant, use the expanded WOG 2000 RCP seal leakage model. However, several aspects of the RCP seal leakage modeling were reviewed for their applicability to the L3PRA project Level 1 model; specifically, the applicability of the O-ring extrusion failure mode (Section 8.4.1) and collapsing multiple leakage rates into limiting scenarios (Section 8.4.2).

[215] As a modeling simplification, the additional systems/functions were limited to the alignment of charging and secondary cooldown (with accumulator injection and the required CST makeup). However, additional mitigation actions are potentially available, such as the manual isolation of the RCP seal leakage.

8.3.1 Applicability of O-ring Extrusion Failure Mode

The reference plant PRA model adapted the RCP modeling described in WCAP-16141, "RCP Seal Leakage PRA Model Implementation Guidelines for Westinghouse PWRs," that eliminated the need for modeling RCS depressurization to 1710 pounds per square inch (psi) within 2 hours to prevent O-ring extrusion of the RCP seals.[216] WCAP-16141 has not been reviewed by the NRC staff. However, the safety evaluation report for WCAP-15603 states the following, "NRC staff accepts the use of a zero failure probability for O-ring extrusion failure of high-temperature O-rings as long as the licensee documents the justification and supporting analyses and bases in the licensee-controlled PRA documentation. Such documentation should show that the plant's cooldown will result in a RCS pressure of less than 1710 psi within 2 hours."

Reference plant-specific MELCOR calculations performed for 21 gpm per RCP seal leakage rate with continuous AFW, and no depressurization, indicate that RCS pressure would be well below 1710 psi at approximately 2 hours. The reference plant also has a unique RCP seal design that does not include O-rings. Therefore, the O-ring extrusion failure mode is not included in the L3PRA project Level 1 model.

8.3.2 Collapsing Multiple Leakage Rates into Limiting Scenarios

The current SPAR models for Westinghouse PWRs (including the reference plant) assume that the catastrophic failure of RCP seals (i.e., the binding/popping failure of the stage 1 and 2 seals) results in a medium loss-of-coolant accident (MLOCA); see Table 8-2 for the various seal leakage rates and seal failure probabilities.[217, 218] The reference plant MELCOR at-power model assumes that the 480 gpm per RCP seal leak corresponds to 1.3-inch break (i.e., a SLOCA).[219] No other information could be identified that supports the MLOCA assumption, and therefore, all RCP seal failures are assumed to result in an SLOCA in the L3PRA project Level 1 model.

Table 8-2 WOG 2000 RCP Seal Model Leakage Rate and Failure Probabilities

[216] WCAP-16141 is not publicly available.

[217] There is also a stage 3 seal, but according to the WOG 2000 RCP seal model, it is assumed to match the integrity of the stage 2 seals (i.e., if stage 2 seals fail, then the stage 3 seals will fail also).

[218] The failure of operators to trip the RCPs given a complete loss of RCP seal injection/cooling will also result in the catastrophic failure of RCP seals (i.e., 480 gpm per RCP seal leakage).

[219] This assumption does not account for the tortuous path of the actual seal leakage; it simply reproduces the associated leakage rate.

Leakage Categories	Estimated Leakage (gpm per RCP)	Seal Failure Probability
Nominal Leakage (Assumes RCP Seal Injection is Provided)	3–5	—
Increased Leakage; with Seal Integrity Maintained (RCP Seal Injection is Unavailable)	21	—
Binding and Popping Failure (1st Stage Seal)	76	0.0125
Binding and Popping Failure (2nd Stage Seal)	182	0.20
Binding and Popping Failure (1st or 2nd Stage Seals)	480	0.21

8.4 Consequential SGTR Modeling

In addition to SGTR initiating events, SGTRs can also potentially develop during an accident owing to thermal-hydraulic conditions triggered by an unrelated initiator. Such consequential SGTRs are typically grouped in to two types: pressure-induced SGTRs and temperature-induced SGTRs. The former is typically considered in Level 1 PRAs (because accidents like ATWS and SSBs can produce the most challenging pressure conditions), while the latter are typically considered in Level 2 PRAs (because core oxidation and relocation can produce the most challenging temperature conditions). Of course, for Level 2 PRAs to consider temperature-induced SGTRs, it is necessary for the Level 1 PRA to provide the necessary plant damage state information.

A systematic approach was implemented to consider which parts of the Level 1 PRA might include consequential SGTR modeling and to provide justification for when such modeling was needed. This approach resulted in the determination that (1) explicit modeling of pressure-induced SGTR is appropriate for ATWS and SSBs, (2) attention must be paid to handling of potential high/dry/low sequences for future use in the Level 2 PRA, and (3) explicit modeling of other types of consequential SGTR sequences is not generally justified.[220]

The actual modeling of pressure-induced SGTR in the L3PRA project Level 1 model (and implicitly in the associated Level 2 plant damage state binning) is discussed, where relevant, in Section 3 and Section 5, and summarized by:

- SGTRs as an initiating event are modeled in the SGTR event tree;
- Transients and SLOCAs leading to ATWS with success of MFW or primary-pressure relief do not consider pressure-induced SGTR due to low frequency contribution;
- Transients and SLOCAs leading to ATWS with failure of MFW and primary-pressure relief assume pressure-induced SGTR (as a simplifying assumption);
- SSB initiating events leading to ATWS, which are assumed to always result in core damage, are also assumed to involve pressure-induced SGTR (as a simplifying assumption);
- SSB initiating events with success of reactor protection system (RPS) query the likelihood of consequential SGTR based on the probability of having a deep tube flaw

[220] High/dry/low sequences correspond to high reactor vessel pressure, a dry steam generator, and a low secondary pressure.

and the conditional core damage probability (CCDP) of a SGTR proceeding to core damage;

- All transients with success of RPS that lead to a consequential secondary-side break query the likelihood of consequential SGTR based on the probability of having a deep tube flaw and the CCDP of a SGTR proceeding to core damage.

To further justify the treatment of consequential SGTR, evaluations were done using the L3PRA project Level 1 model to demonstrate that:

- Consequential SGTR (and SGTR initiating event) were a small fraction of core damage frequency (CDF) (less than 2 percent);

- Consequential SGTR potential was dominated by post-core damage, temperature-induced SGTR (approximately 89 percent);

- Pressure-induced SGTR was a small contributor to the overall consequential SGTR (approximately 7 percent) and a very small contributor to CDF (less than 1 percent); and

- Unmodeled consequential SGTR sequences would be a small fraction of modeled consequential SGTR sequences (approximately 3 percent).[221]

The important qualifiers on these results are:

- Consistent with the state-of-practice in consequential SGTR modeling, leaks below the critical break area (one double-ended tube break) are not considered because they are assumed to be mitigatable with high reliability.

- These estimates (necessarily) project what the Level 2 temperature-induced SGTR frequency will be, based on (1) the high/dry/low frequency and (2) the conditional temperature-induced SGTR probability. This does not include any 'benefit' that the Level 2 PRA model will ultimately estimate with respect to operator actions prior to hot leg creep rupture.

Based on the above, the L3PRA project Level 1 model is believed to appropriately consider the important contributors to consequential SGTR.

[221] The unmodeled sequences refer to three types of consequential SGTR that are possible, but were not ultimately included in the L3PRA Level 1 model: (i) ATWS events with success of primary pressure relief but failure of feedwater; (ii) non-high/dry/low sequences with a SG becoming faulted, followed by operator action to isolate that SG, leading to the potential for high/dry/low-like conditions in that loop; and (iii) sequences with high RCS pressure where feedwater status is indeterminate in the L3PRA Level 1 model, which depending on how they are ultimately treated in the plant damage state binning, could produce additional consequential SGTR frequency if independent failure of feedwater occurs.

9 QUANTIFICATION

The L3PRA project Level 1 model for internal events for a single unit (SVN version 266) was quantified using SAPHIRE, version 8.1.4. The SVN software is an application used internally to retain and track the different versions of the overall (integrated) L3PRA project model. SAPHIRE is a personal computer-based software for creating and quantifying fault trees and event trees. The event tree linking and quantification performed by SAPHIRE generates a core damage frequency estimate and a listing of dominant cut sets and dominant accident sequences.

Section 9.1 describes the core damage quantification process using SAPHIRE. The key results from quantification of the L3PRA project Level 1 internal event model are provided in Section 9.2.

9.1 Core Damage Quantification

The SAPHIRE quantification paradigm is sequence centric. That is, SAPHIRE generates and stores event tree sequence logic, and has solution control options that allow for exact sequence quantification in some circumstances, and for obtaining the best approximation when exact quantification is not possible. The SAPHIRE design therefore makes it possible to quantify either large event tree models where exact solutions may be possible, or fault tree linked models where exact solutions are seldom possible (the L3PRA project Level 1 model is a fault tree linked model). Key quantification assumptions in the SAPHIRE design are that event tree sequences are mutually exclusive, while cut sets generated on a sequence basis are independent. When SAPHIRE displays or reports event tree results, it gives results that are true to these assumptions. A consequence of this is that when SAPHIRE displays or reports event tree sequence results, there may be cut sets that appear to be identical, but are not because of the neglected elements of success nodes that are not visible in the result. When event tree sequence results are gathered into a single end-state, SAPHIRE can be asked to relax these assumptions and treat all cut sets as independent. The result is that duplicate cut sets are subsumed, and the end-state result will be of slightly lower frequency than the event tree sequence result. The end-state result that is free of duplicated cut sets is the result preferred by many analysts and the result that is reported in this section. However, there are times when specific sequence results are desired. The reader is cautioned that sequence results will often not be completely consistent with the end-state result because of the above considerations.

Accident sequences created in the event tree linking process use linkage rules (if appropriate) to develop logic based on predefined rules. The event tree linkage rules allow the user to:

- Replace one or more top events with substituted fault trees based on the logical conditions defined by the rule. These top event fault tree substitutions are presented in Section 5 (see “Additional Fault Trees”).

- Assign sequence flag sets to the sequences based on the logical conditions defined by the rule. The flag sets identify any conditional processing of the top event. The process flags identified in the flag sets define conditional dependencies based on the sequence branch path (i.e., success or failure). For example, the low-pressure injection (LPI) success criteria vary with size of the loss-of-coolant accident (LOCA). Sequence flag sets are used to identify the initiating event and act on house events in the fault tree

logic to select the required modeling variations. An example using top-level fault tree logic is provided in Figure 9-1.

The event tree linkage rules are found by selecting the following in SAPHIRE: (select all event trees or those of interest) Publish, Event Tree Report, and Linkage Rules. The event tree process flags are found in SAPHIRE through the following: (select all event trees or those of interest) Publish, Project Reports, and Flag Sets with Description.

In addition to the above processing, fault tree flag sets are used to "activate" or "deactivate" portions of a fault tree on a sequence-by-sequence basis. "House events" are used to trigger these modifications to fault trees. The fault tree flag sets are used to eliminate multiple fault tree models. For example, flag sets are used on systems in the loss of offsite power (LOOP) and station blackout (SBO) event trees where alternating current (AC) power dependency changes from offsite to onsite power then back to offsite power. By using the fault tree flag sets, only one logic model is required to handle the change in AC power dependency. The fault tree process flags are found by selecting the following in SAPHIRE: (select all event trees) Publish, Project Reports, and Flag Sets with Description.

Recovery rules (post-processing rules) are used by the SAPHIRE code to perform the following functions:

- The recovery rules remove combinations of test and maintenance events that are disallowed by the plant technical specifications.

- The L3PRA project Level 1 model is like most probabilistic risk assessments (PRAs) in that nominal recovery of hardware failures is not generally credited; however, AC power recovery is a typical exception. The L3PRA project Level 1 model considers recovery of AC power (e.g., offsite power and the alternate switchyard) for SBO scenarios. The recovery credit is applied via post-processing rules for consequential LOOPs that result in a SBO.[222] Specifically, the recovery rules are used to apply credit for AC power recovery for consequential LOOPs that result in a SBO for scenarios that are considered recoverable [e.g., emergency diesel generator (EDG)-related failures]. See Section 8.2.3 for additional information.

    - In addition, post-processing rules were used to change the amount of credit for key failures/unavailabilities of the turbine-driven auxiliary feedwater pump train that would result in less time available for operators to recover AC power from either offsite power or the alternate switchyard during a consequential LOOP and subsequent SBO (1 hour versus 2 hours).

[222] For LOOP initiating events, AC power recovery is applied solely via the OPR fault trees (e.g., OPR-1H or OPR-2H) in the SBO event tree; therefore, post-processing rules are not needed.

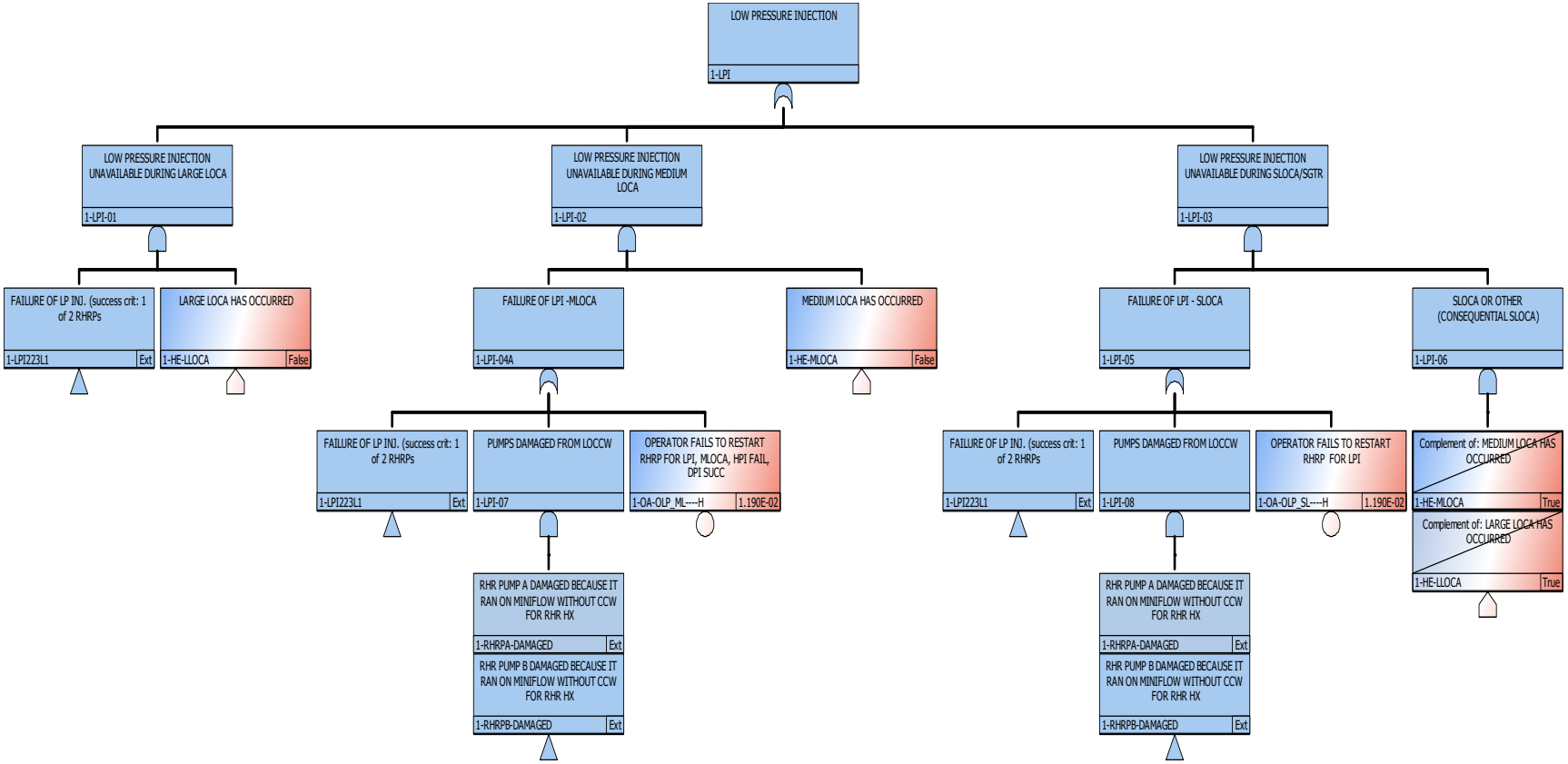


Figure 9-1 Example of House Events that Utilize Flag Sets for Top Event Fault Trees

- The core damage scenarios include dependencies among operator actions. The recovery rules apply the results of the formal dependency calculations by removing the independent basic events and replacing them with their dependent versions. A list of the human failure events (HFEs) that were considered as having some formal dependency in the L3PRA project Level 1 model is provided in Table 6-6.

- Post-processing rules are used to substitute some HFEs on a cut set-specific basis:

  - A long-term HFE (OAB_TR-------H-LT) for initiating feed and bleed cooling given key auxiliary feedwater (AFW) unavailabilities related to the unavailability of condensate storage tank (CST) inventory makeup replaces the normal (short-term) HFE (OAB-TR-------H).

  - When both the initial failure to trip the reactor during an anticipated transient without scram (ATWS) HFE (A------MANRTH or RPS-XHE-XE-NSGNL) and long-term failure to trip the reactor (RPS-XHE-TRIP-LT) are present in the same cut set; the shorter term HFE is deleted.

- Convolution correction rules are used to remove conservatisms in LOOP sequence EDG fail-to-run cut sets as described in Section 7.4.2.

The recovery rule file for this model is found by selecting the following in SAPHIRE: Publish, Project Reports, and Event Tree Recovery Rules.

9.2 Key Results

The core damage results for the L3PRA project Level 1 internal event model contain approximately 175,000 core damage cut sets (at a truncation of 10^{-12}). These cut sets are comprised of over 5,000 basic events that mostly represent initiating events, independent equipment unavailabilities, common-cause failures (CCFs), and human errors. The core damage frequency (CDF) and percentage contribution to the overall CDF are provided for all initiating events in Section 9.2.1. A table of the all the significant accident sequences and a brief discussion of the dominant sequence contributors to CDF are provided in Section 9.2.2. A brief description of the dominant cut sets to CDF is provided in Section 9.2.3; while a complete list of all L3PRA project Level 1 model significant cut sets is provided in Appendix B. The results of the parameter uncertainty calculations are provided in Section 9.2.4. The L3PRA project Level 1 model truncation and convergence evaluation is discussed in Section 9.2.5. Finally, the importance results for significant basic events [e.g., structure, system, and component unavailabilities; CCFs; and HFEs) are provided in Section 9.2.6.

9.2.1 Initiating Events

The CDF for the L3PRA project Level 1 internal event model for a single unit is 6.4×10^{-5} per reactor-critical year (RCY). The contribution of specific initiating events to the CDF is summarized in Table 9-1 and Figure 9-2.

As can be seen from Table 9-1 and Figure 9-2, LOOP initiating events account for 62 percent of internal event CDF, nearly half of which comes from grid-related LOOP. In the L3PRA project, the grid-related LOOP frequency (1.23×10^{-2} per RCY) was obtained from the published 2010 update to NUREG/CR-6928 (as discussed in Section 2.2). It should be noted that in NUREG/CR-6928, grid-related LOOP events that affect multiple units are counted as separate

events for each unit. WCAP-16565, "Considerations for Risk-Informed Modeling Grid Centered Loss of Offsite Power Events," which is referenced in some licensee probabilistic risk assessments (PRAs), considers grid-related LOOPs that affect multiple units to be counted only as a single event, leading to a significantly lower grid-related LOOP frequency.[223] Other reasons why the L3PRA project internal event CDF is dominated by LOOP initiating events are discussed in Section 8.1.

The next largest initiating event contributor is loss of nuclear service cooling water (NSCW) that accounts for nearly 14 percent of internal event CDF. As discussed further in Section 9.2.2, the loss of NSCW causes a loss of the ultimate heat sink and total loss of reactor coolant pump (RCP) seal cooling and injection, and its frequency is dominated by NSCW pump CCF events.

Table 9-1 Initiating Event Contribution to Internal Event CDF

Initiating event	CDF (per RCY)	Percent Contribution to CDF	Cumulative Contribution to CDF
Grid-Related LOOP	1.83E-05	28.7%	28.7%
Switchyard-Centered LOOP	1.04E-05	16.2%	44.9%
Weather-Related LOOP	9.02E-06	14.1%	59.0%
Loss of NSCW	8.76E-06	13.7%	72.7%
Other Transients	2.53E-06	4.0%	76.7%
Medium LOCA	2.34E-06	3.7%	80.3%
Plant-Centered LOOP	1.91E-06	3.0%	83.3%
Secondary-Side Break (SSB) Downstream of the Main Steam Isolation Valves (MSIVs) or Upstream of the Main Feedwater Isolation Valves (MFIVs)	1.59E-06	2.5%	85.8%
Loss of 4.16 kilovolt (kV) AC Bus A	1.43E-06	2.2%	88.1%
Turbine Trip	1.07E-06	1.7%	89.7%
Loss of RCP Seal Injection	1.04E-06	1.6%	91.3%

[223] WCAP-16565 is not publicly available.

Table 9-1 Initiating Event Contribution to Internal Event CDF (cont.)

Initiating event	CDF (per RCY)	Percent Contribution to CDF	Cumulative Contribution to CDF
Reactor Trip	9.77E-07	1.5%	92.9%
Loss of 4.16 kV AC Bus B	8.77E-07	1.4%	94.2%
Loss of 125 volt (V) Direct Current (DC) Bus BD1	8.61E-07	1.3%	95.6%
Loss of MFW	5.21E-07	0.8%	96.4%
Loss of Condenser Heat Sink	4.75E-07	0.7%	97.2%
Loss of 125 V DC Bus AD1	3.59E-07	0.6%	97.7%
Loss of Auxiliary Component Cooling Water (ACCW)	2.47E-07	0.4%	98.1%
Small LOCA	2.39E-07	0.4%	98.5%
Interfacing-Systems Loss-of-Coolant Accident (ISLOCA) from RHR Hot Leg Suction Lines	2.25E-07	0.4%	98.8%
Inadvertent Safety Injection (SI) Actuation	1.46E-07	0.2%	99.1%
Steam Generator Tube Rupture (SGTR)	1.24E-07	0.2%	99.2%
SSB Upstream of the MSIVs or Downstream of the MFIVs	1.06E-07	0.2%	99.4%
Excessive LOCA (Reactor Vessel Rupture)	1.00E-07	0.2%	99.6%
Loss of 120 V AC Panels A and B	9.61E-08	0.2%	99.7%
ISLOCA from Residual Heat Removal (RHR) Cold Leg Injection Line A	4.19E-08	0.1%	99.8%
ISLOCA from RHR Cold Leg Injection Line B	4.19E-08	0.1%	99.9%
Large LOCA	3.56E-08	0.1%	99.9%
ISLOCA from RCP Stage 1 Seal Leak Off	3.38E-08	0.1%	100.0%
Loss of Instrument Air	2.47E-08	0.0%	100.0%
Loss of 120 V AC Panels A and C	7.51E-11	0.0%	100.0%

Initiating event	CDF (per RCY)	Percent Contribution to CDF	Cumulative Contribution to CDF
Loss of 120 V AC Panels A and D	4.30E-11	0.0%	100.0%
Loss of 120 V AC Panels B and C	4.30E-11	0.0%	100.0%
Loss of 120 V AC Panels B and D	4.30E-11	0.0%	100.0%
Loss of 120 V AC Panels C and D	4.30E-11	0.0%	100.0%
ISLOCA from a RCP Thermal Barrier Heat Exchanger	3.53E-11	0.0%	100.0%
	6.39E-05	100.0%	

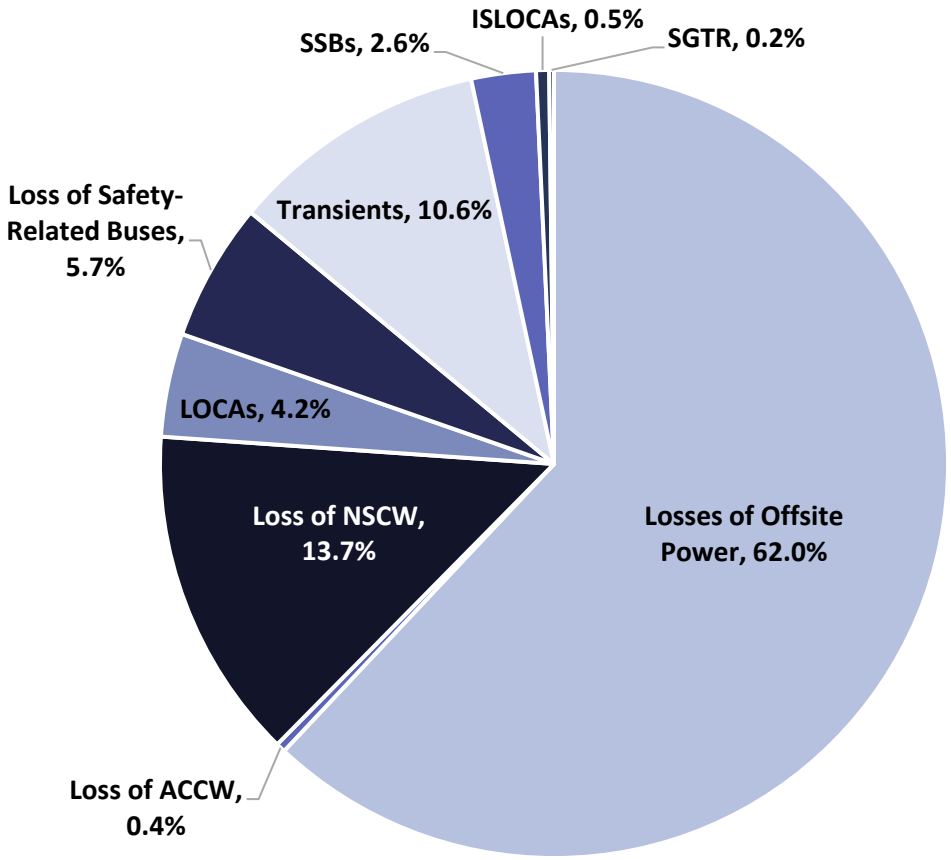


Figure 9-2 Initiating Event Group Contributions to Overall CDF

Figure 9-2. Significant Accident Sequences

Accident sequences that are part of the summed 95 percent or contribute to at least 1 percent of the total CDF (per hazard group) are considered significant per the American Society of Mechanical Engineers/American Nuclear Society (ASME/ANS) PRA standard (ASME/ANS, 2009). Table 9-2 contains the 41 significant accident sequences for the L3PRA project Level 1 internal event model. The accident sequence naming convention used comprises the event tree name from the SAPHIRE model followed by a series of hyphen-separated numbers indicating the sequence number on the named event tree, followed by the sequence numbers from all transfer event trees. For example the first sequence in the table is designated LOOPGR 10-07-1 indicating the event sequence begins with a grid-related LOOP initiating event, develops along the path of the 10th sequence on the grid-related LOOP event tree, transfers to a second event

Table 9-2 L3PRA Project Level 1 Model Significant Accident Sequences

Accident Sequence	Description	CDF (per RCY)	Percent Contribution to CDF	Cumulative Contribution to CDF
LOOPGR:10-07-1	/1-RPS, 1-EPS, /1-AFW-B, /1-PVC-B, /1-BP1, /1-BP2, 1-OPR-02H	1.42E-05	22.2%	22.2%
LONSCW:5-1	1-IEFT-LONSCW, /1-RPS, /1-TT, /1-SVC, /1-PVC, 1-RCPS-BP	8.66E-06	13.6%	35.8%
LOOPWR:10-07-1	/1-RPS, 1-EPS, /1-AFW-B, /1-PVC-B, /1-BP1, /1-BP2, 1-OPR-02H	7.58E-06	11.9%	47.7%
LOOPSC:10-07-1	/1-RPS, 1-EPS, /1-AFW-B, /1-PVC-B, /1-BP1, /1-BP2, 1-OPR-02H	7.22E-06	11.3%	59.0%
LOOPGR:10-06-1	/1-RPS, 1-EPS, /1-AFW-B, /1-PVC-B, /1-BP1, /1-BP2, /1-OPR-02H, 1-AFW-ACR, 1-FAB-ACR	2.93E-06	4.6%	63.6%
LOOPSC:10-06-1	/1-RPS, 1-EPS, /1-AFW-B, /1-PVC-B, /1-BP1, /1-BP2, /1-OPR-02H, 1-AFW-ACR, 1-FAB-ACR	2.48E-06	3.9%	67.4%
OTRANS:10-1	/1-RPS, /1-TT, /1-SVC, /1-PVC, 1-RCPSI, /1-RCPSC, 1-FW, 1-FAB	1.99E-06	3.1%	70.5%
LOOPPC:10-07-1	/1-RPS, 1-EPS, /1-AFW-B, /1-PVC-B, /1-BP1, /1-BP2, 1-OPR-02H	1.34E-06	2.1%	72.6%
MLOCA:2-1	/1-RPS, /1-HPI, 1-HPR	1.30E-06	2.0%	74.7%
SSBO:11-08-1	/1-RPS, /1-PI-SGTR, /1-SGI-SSBO, 1-RCPSI-CCPS, 1-RCPSC, /1-AFW-LOCA, 1-HPI, /1-CAD-FRC1, /1-ACC, 1-LPI	1.18E-06	1.8%	76.5%

Accident Sequence	Description	CDF (per RCY)	Percent Contribution to CDF	Cumulative Contribution to CDF
LOOPWR:10-06-1	/1-RPS, 1-EPS, /1-AFW-B, /1-PVC-B, /1-BP1, /1-BP2, /1-OPR-02H, 1-AFW-ACR, 1-FAB-ACR	9.31E-07	1.5%	78.0%
LOSINJ:06-1	1-IEFT-LOSINJ, /1-TT, /1-SVC, /1-PVC, /1-RCPSC, 1-FW, 1-FAB	9.10E-07	1.4%	79.4%
TTRIP:10-1	/1-RPS, /1-TT, /1-SVC, /1-PVC, 1-RCPSI, /1-RCPSC, 1-FW, 1-FAB	8.47E-07	1.3%	80.7%
RTRIP:10-1	/1-TT, /1-SVC, /1-PVC, 1-RCPSI, /1-RCPSC, 1-FW, 1-FAB	7.77E-07	1.2%	82.0%
LO125BD1:11-1	1-IEFT-LO125BD1, /1-RPS, /1-SVC, /1-PVC, 1-RCPSI, /1-RCPSC, 1-AFW, 1-FAB	7.67E-07	1.2%	83.2%
MLOCA:5-1	/1-RPS, 1-HPI, /1-AFW-LOCA, /1-CAD-MLOCA, /1-ACC-M&LLOCA, 1-LPI	7.44E-07	1.2%	84.3%
LO4160VA:04-1	/1-RPS, /1-SVC, /1-PVC, /1-RCPSI, 1-AFW, 1-FAB	5.51E-07	0.9%	85.2%
LOOPPC:10-06-1	/1-RPS, 1-EPS, /1-AFW-B, /1-PVC-B, /1-BP1, /1-BP2, /1-OPR-02H, 1-AFW-ACR, 1-FAB-ACR	4.59E-07	0.7%	85.9%
LOOPGR:10-22-1	/1-RPS, 1-EPS, 1-AFW-B, /1-PVC-B, /1-BP1, /1-BP2, 1-OPR-01H	4.54E-07	0.7%	86.6%
LO4160VA:10-1	/1-RPS, /1-SVC, /1-PVC, 1-RCPSI, /1-RCPSC, 1-AFW, 1-FAB	4.11E-07	0.6%	87.3%
LO4160VB:10-1	/1-RPS, /1-SVC, /1-PVC, 1-RCPSI, /1-RCPSC, 1-AFW, 1-FAB	4.05E-07	0.6%	87.9%
LOOPGR:06-1	/1-RPS, /1-EPS, /1-SVC, /1-PVC, /1-RCPSC, 1-AFW, 1-FAB	3.35E-07	0.5%	88.4%

Accident Sequence	Description	CDF (per RCY)	Percent Contribution to CDF	Cumulative Contribution to CDF
LOMFW:10-1	/1-RPS, /1-TT, /1-SVC, /1-PVC, 1-RCPSI, /1-RCPSC, 1-AFW, 1-FAB	3.28E-07	0.5%	88.9%

Table 9-2L3PRA Project Level 1 Model Significant Accident Sequences (cont.)

Accident Sequence	Description	CDF (per RCY)	Percent Contribution to CDF	Cumulative Contribution to CDF
LO4160VB:07-1	/1-RPS, /1-SVC, /1-PVC, 1-RCPSI, /1-RCPSC, /1-AFW, 1-CHG, 1-SAFESTABLE	3.24E-07	0.5%	89.4%
LO4160VA:07-1	/1-RPS, /1-SVC, /1-PVC, 1-RCPSI, /1-RCPSC, /1-AFW, 1-CHG, 1-SAFESTABLE	3.22E-07	0.5%	89.9%
LOCHS:10-1	/1-RPS, /1-SVC, /1-PVC, 1-RCPSI, /1-RCPSC, 1-AFW, 1-FAB	2.98E-07	0.5%	90.4%
LOOPSC:06-1	/1-RPS, /1-EPS, /1-SVC, /1-PVC, /1-RCPSC, 1-AFW, 1-FAB	2.83E-07	0.4%	90.8%
LOOPWR:10-22-1	/1-RPS, 1-EPS, 1-AFW-B, /1-PVC-B, /1-BP1, /1-BP2, 1-OPR-01H	2.73E-07	0.4%	91.3%
OTRANS:11-08-1	/1-RPS, /1-TT, /1-SVC, /1-PVC, 1-RCPSI, 1-RCPSC, /1-AFW-LOCA, 1-HPI, /1-CAD-FRC1, /1-ACC, 1-LPI	2.44E-07	0.4%	91.7%
LOOPGR:10-09-1	/1-RPS, 1-EPS, /1-AFW-B, /1-PVC-B, /1-BP1, 1-BP2, 1-OPR-02H,	2.28E-07	0.4%	92.0%
ISL-RHR-HLS:2-1	1-IEFT-ISL-RHR-HLS	2.25E-07	0.4%	92.4%
LO125AD1:11-1	1-IEFT-LO125AD1, /1-RPS, /1-SVC, /1-PVC, 1-RCPSI, /1-RCPSC, 1-AFW, 1-FAB	2.20E-07	0.3%	92.7%
MLOCA:7-1	/1-RPS, 1-HPI, /1-AFW-LOCA, 1-CAD-MLOCA	2.16E-07	0.3%	93.0%
OTRANS:04-1	/1-RPS, /1-TT, /1-SVC, /1-PVC, /1-RCPSI, 1-FW, 1-FAB	2.12E-07	0.3%	93.4%

Accident Sequence	Description	CDF (per RCY)	Percent Contribution to CDF	Cumulative Contribution to CDF
SSBO:10-1	/1-RPS, /1-PI-SGTR, /1-SGI-SSBO, 1-RCPSI-CCPS, /1-RCPSC, 1-AFW, 1-FAB	2.08E-07	0.3%	93.7%
LOOPSC:10-09-1	/1-RPS, 1-EPS, /1-AFW-B, /1-PVC-B, /1-BP1, 1-BP2, 1-OPR-02H,	1.93E-07	0.3%	94.0%
LOACCW:11-05-1	1-IEFT-LOACCW, /1-RPS, /1-TT, /1-SVC, /1-PVC, 1-RCPSI-LOACCW, 1-RCPS-BP, /1-AFW-LOCA, /1-HPI, 1-CAD-ES12, 1-HPR	1.68E-07	0.3%	94.3%
SLOCA:08-1	/1-RPS, /1-AFW-LOCA, 1-HPI, /1-CAD-FRC1, /1-ACC, 1-LPI	1.41E-07	0.2%	94.5%
SSBO:05-05-1	/1-RPS, /1-PI-SGTR, /1-SGI-SSBO, /1-RCPSI-CCPS, 1-SSB-CSLOCA, /1-AFW-LOCA, /1-HPI, 1-CAD-ES12, 1-HPR	1.17E-07	0.2%	94.7%
LOSINJ:07-08-1	1-IEFT-LOSINJ, /1-TT, /1-SVC, /1-PVC, 1-RCPSC, /1-AFW-LOCA, 1-HPI, /1-CAD-FRC1, /1-ACC, 1-LPI	1.11E-07	0.2%	94.8%
LOOPWR:06-1	/1-RPS, /1-EPS, /1-SVC, /1-PVC, /1-RCPSC, 1-AFW, 1-FAB	1.06E-07	0.2%	95.0%

tree (the SBO event tree in this case), and develops along the path of the 7th sequence on the SBO event tree.[224] From these significant accident sequences, the dominant contributors to L3PRA project Level 1 model CDF for internal events are:

- A LOOP initiating event and subsequent failures leading to a SBO, with operators failing to restore AC power [offsite power or the alternate switchyard (if available)] prior to turbine building battery depletion time of 2 hours. The four accident sequences (10-07-1) that comprise this scenario account for approximately 48 percent of the CDF.[225] This sequence CDF is heavily influenced by the L3PRA project Level 1 model assumptions of not crediting (1) AC power recovery after depletion of the turbine building batteries and (2) turbine-driven AFW pump operation after depletion of the safety-related batteries (see Section 8.1 for additional information).

- A loss of NSCW initiating event causing a loss of the ultimate heat sink and total loss of RCP seal cooling and injection, with subsequent failure of RCP seals causing a SLOCA with no emergency core cooling system (ECCS) injection systems available (NSCW provides cooling water to all ECCS pumps). This sequence (5-1) accounts for approximately 14 percent of the internal event CDF. These results are dominated by NSCW pump CCF events. The CCF modeling is simplified to include only selected high-order CCF event combinations and relies on industry-average alpha factors that are highly uncertain with respect to the high-order event probabilities.[226]

- A LOOP initiating event and subsequent failures of both EDGs leading to a SBO, with operators failing to restore required systems after AC power is successfully recovered. The four accident sequences (10-06-1) that comprise this scenario account for approximately 11 percent of the CDF.

- A transient initiating event and subsequent failures/unavailabilities of AFW, MFW, and feed and bleed cooling. The eight accident sequences (10-1) that comprise this scenario account for approximately 8 percent of the CDF.

---

[224] The final number (-1) contained in the L3PRA Project Level 1 internal events sequences indicates the transfer to the Level 2 model bridge event tree, which is inactive in the Level 1 model.

[225] In the L3PRA Project Level 1 model, there are four classes of LOOP initiating events (i.e., grid-related, weather-related, switchyard-centered, and plant-centered); therefore, four identical sequences (except for the LOOP initiating type) are present.

[226] The CCF alpha factors used to estimate failure probabilities are estimated from a population of observed CCFs that contains only 15 failure-to-run CCF events in total, about half of which involve service water system pumps. Of these, only one event was observed involving three pumps and the rest involved only two or were postulated to possibly affect more than two (impact vectors were assigned that postulated five in one case and four in another, but the postulated cases were assigned impact vector probabilities of 0.001 and 0.0001 respectively for the high order failures). The process of obtaining alpha factor estimates for higher-order systems is described in NUREG/CR-5485, Sections C.4.2 and C.4.3. The process requires an assessment of the nature of common cause shocks to the system as either “lethal” or “nonlethal”. Both cases require assumptions about how the observed events would appear in a more redundant system. In the lethal case, for example, an event involving 2 components in a system of 2 components is assumed to extrapolate to an event involving 6 components in a system of 6 components. In the nonlethal case, the extrapolation relies on estimating the parameters of a binomial failure rate model that is then used to estimate how counts in the low order system would appear in the higher-order systems. In both cases the extrapolated event counts cannot easily be validated using operational data that makes them highly uncertain.

9.2.2 Significant Cut Sets

Cut sets that are part of the summed 95 percent or contribute to at least 1 percent of the total CDF (per hazard group) are considered significant per the ASME/ANS Level 1 PRA standard. Appendix B contains the 3,188 significant cut sets for the L3PRA project Level 1 model for internal events. The top 10 cut sets (accounting for approximately 37 percent of the CDF) are provided in the Table 9-3.

9.2.3 Significant Basic Events

Basic events that have a Fussell-Vesely (FV) importance measure greater than or equal to 0.005 or risk achievement worth (RAW) importance measure greater than or equal to 2 are considered significant per the ASME/ANS Level 1 PRA standard. Table 9-4 provides the significant basic events with a FV importance measure greater than or equal to 0.005.[227] The significant basic events with a RAW importance measure greater than or equal to 2 are provided in Appendix C. The sections below discuss the top significant basic events for the categories of SSC unavailabilities, CCFs, and HFEs.

SSC Unavailabilities

The top SSC unavailabilities based on the FV importance measure are:

- *RCP Stage 2 Seal Integrity (Binding/Popping)*— The failure of the RCP seals due to the loss of seal cooling (i.e., seal injection and thermal barrier heat exchanger cooling) causes a LOCA. A failure probability of 0.20 is based on the WOG 2000 RCP seal leakage model.

- *Failure of EDG 1A or 1B to Run*— The failure of an EDG to run leads to a lack of electrical power to its associated safety-related 4.16 kV AC bus; therefore, rendering one train of safety-related components unavailable.

- *Failure Switchyard Breakers AA205 or BA301 to Open*— The failure of either of these two breakers prevents the applicable EDG from loading onto its associated safety-related 4.16 kV AC bus; therefore, rendering one train of safety-related components unavailable.

[227] The initiating events with FV importance measures greater than or equal to 0.005 have been removed from Table 9-4. The importance of the different initiating events is provided in Table 9-1 (i.e., the initiating event percent contribution to CDF is the same as their FV importance).

Table 9-3 L3PRA Project Level 1 Model Top 10 Dominant Cut Sets

#	CDF (per RCY)	Percent Contribution to CDF	Cut Set		Description
1	6.1E-06	9.5%	IE-LONSCW	Loss of NSCW	A CCF of all six NSCW pumps causes a loss of NSCW which leads operators to manually trip the reactor. The loss of NSCW causes a loss of ultimate heat sink. In addition, a loss of RCP seal injection [via the normal charging pump (NCP)] and thermal barrier heat exchanger cooling (via loss of ACCW) occurs. The stage 2 RCP seals fail causing a SLOCA. Core damage occurs due to the RCP seal LOCA and the loss of all ECCS injection systems (NSCW provides cooling to all ECCS pumps).
			IE-SWS-MDP-CR-123456	System generated event based upon RASP CCF event: 1-IE-SWS-MDP-CF-	
			RCS-MDP-LK-BP2	RCP seal stage 2 integrity (binding/popping open) fails	
2	4.3E-06	6.7%	IE-LOOPGR	Loss of offsite power (grid-related)	A grid-related LOOP occurs causing a reactor trip. The EDGs cannot load on their respective buses due to the CCF of the switchyard breakers AA205 and BA301 (the RAT feeder breakers) to open; therefore, causing a non-recoverable SBO. Once safety-related DC bus 1CD1 is deenergized when its associated safety-related battery is depleted (in 4 hours), control power for the turbine-driven AFW pump is lost, leading to core damage.
			ACP-CRB-CF-A205301	Switchyard AC breakers AA205 and BA301 fail from common cause to open	

#	CDF (per RCY)	Percent Contribution to CDF	Cut Set		Description
3	3.6E-06	5.7%	IE-LOOPSC	Loss of offsite power (switchyard-centered)	Analogous to cut set 2, except a different LOOP initiating event type (switchyard-centered) occurs.
			ACP-CRB-CF-A205301	Switchyard AC breakers AA205 and BA301 fail from common cause to open	
4	2.6E-06	4.1%	IE-LOOPGR	Loss of offsite power (grid-related)	A grid-related LOOP occurs causing a reactor trip. The EDGs cannot load on their respective buses due to the CCF of the sequencers; therefore, causing a non-recoverable SBO. Once safety-related DC bus 1CD1 is deenergized when its associated safety-related battery is depleted (in 4 hours), control power for the turbine-driven AFW pump is lost, leading to core damage.
			EPS-SEQ-CF-FOAB	Sequencers fail from common cause to operate	

Table 9-3 L3PRA Project Level 1 Model Top 10 Dominant Cut Sets (cont.)

#	CDF (per RCY)	Percent Contribution to CDF	Cut Set		Description
5	2.2E-06	3.5%	IE-LOOPSC	Loss of offsite power (switchyard-centered)	Analogous to cut set 4, except a different LOOP initiating event type (switchyard-centered) occurs.
			EPS-SEQ-CF-FOAB	Sequencers fail from common cause to operate	
6	1.4E-06	2.1%	IE-LOOPWR	Loss of offsite power (weather-related)	Analogous to cut sets 2 and 3, except a different LOOP initiating event type (weather-related) occurs.
			ACP-CRB-CF-A205301	Switchyard AC breakers AA205 and BA301 fail from common cause to open	
7	1.2E-06	1.8%	IE-MLOCA	Medium LOCA	A MLOCA initiating event occurs causing a reactor trip. High-pressure injection (HPI) is successful; however, core damage occurs when operators fail to align for high-pressure recirculation (HPR) from the containment sump.
			OAR_HPML-----H	Operator fails to establish high pressure recirculation - MLOCA	
8	8.6E-07	1.4%	IE-LOOPWR	Loss of offsite power (weather-related)	A weather-related LOOP occurs causing a reactor trip. Both EDGs fail-to-run. Operators fail to recover offsite power prior to the turbine building batteries being depleted (in 2 hours); convolution for the two EDGs failing to run is applied. Once safety-related DC bus 1CD1 is
			EPS-DGN-FR-G4001___	DG1A fails to run by random cause (24-hour mission time)	

#	CDF (per RCY)	Percent Contribution to CDF	Cut Set		Description
			EPS-DGN-FR-G4002___	DG1B fails to run by random cause (24-hour mission time)	deenergized when its associated safety-related battery is depleted (in 4 hours), control power for the turbine-driven AFW pump is lost, leading to core damage.
			OEP-XHE-XL-NR02HWR	Operator fails to recover offsite power in 2 hours (weather-related)	
			OEP-XHE-XX-NR02HWR2	Convolution factor for 2FTR-OPR (2HR-WR available)	
9	8.4E-07	1.3%	IE-LOOPWR	Loss of offsite power (weather-related)	Analogous to cut sets 4 and 5, except a different LOOP initiating event type (weather-related) occurs.
			EPS-SEQ-CF-FOAB	Sequencers fail from common cause to operate	
10	7.7E-07	1.2%	IE-LOOPGR	Loss of offsite power (grid-related)	A grid-related LOOP occurs causing a reactor trip. Both EDGs fail-to-run. Operators successfully recover offsite power prior to the turbine building batteries being depleted (in 2 hours); however, operators fail to restore systems after successful AC power recovery, leading to core damage.
			EPS-DGN-FR-G4001___	DG1A fails to run by random cause (24-hour mission time)	
			EPS-DGN-FR-G4002___	DG1B fails to run by random cause (24-hour mission time)	
			OA-ORS-------H	Operator fails to restore systems after ac recovered in SBO	

Table 9-4 Significant Basic Events with FV Importances Greater than 0.005

Name	Description	Probability/ Frequency	FV
1-IE-LOOPGR	LOSS OF OFFSITE POWER (GRID-RELATED)	1.23E-02	2.87E-01
1-ACP-CRB-CF-A205301	SWITCHYARD AC BREAKERS AA205 AND BA301 FAIL FROM COMMON CAUSE TO OPEN	3.50E-04	1.90E-01
1-IE-LOOPSC	LOSS OF OFFSITE POWER (SWITCHYARD-CENTERED)	1.04E-02	1.62E-01
1-IE-LOOPWR	LOSS OF OFFSITE POWER (WEATHER-RELATED)	3.91E-03	1.41E-01
1-IE-LONSCW	LOSS OF NSCW	1.00E+00	1.37E-01
1-EPS-SEQ-CF-FOAB	SEQUENCERS FAIL FROM COMMON CAUSE TO OPERATE	2.15E-04	1.34E-01
1-RCS-MDP-LK-BP2	RCP SEAL STAGE 2 INTEGRITY (BINDING/POPPING OPEN) FAILS	2.00E-01	1.34E-01
1-EPS-DGN-FR-G4001___	DG1A FAILS TO RUN BY RANDOM CAUSE (24 HR MISSION TIME)	3.30E-02	1.18E-01
1-EPS-DGN-FR-G4002___	DG1B FAILS TO RUN BY RANDOM CAUSE (24 HR MISSION TIME)	3.30E-02	1.13E-01
1-OA-ORS-------H	OPERATOR FAILS TO RESTORE SYSTEMS AFTER AC RECOVERED IN SBO	5.73E-02	1.06E-01

Name	Description	Probability/ Frequency	FV
1-IE-SWS-MDP-CR-123456	SYSTEM GENERATED EVENT BASED UPON RASP CCF EVENT: 1-IE-SWS-MDP-CF-	3.03E-05	1.05E-01
1-OEP-XHE-XL-NR02HGR	OPERATOR FAILS TO RECOVER OFFSITE POWER IN 2 HOURS (GRID-RELATED)	3.92E-01	9.02E-02
1-OEP-VCF-LP-CLOPT	CONSEQUENTIAL LOSS OF OFFSITE POWER - TRANSIENT	5.30E-03	8.88E-02
1-OEP-XHE-XL-NR02HWR	OPERATOR FAILS TO RECOVER OFFSITE POWER IN 2 HOURS (WEATHER-RELATED)	5.59E-01	7.67E-02
1-ACP-CRB-CC-AA0205__	RAT A SUPPLY CIRCUIT BREAKER FAILS TO OPEN BY RANDOM CAUSE	5.35E-03	6.19E-02
1-ACP-CRB-CC-BA0301__	RAT B SUPPLY CIRCUIT BREAKER FAILS TO OPEN BY RANDOM CAUSE	5.35E-03	6.15E-02
1-EPS-DGN-MA-G4001___	DG1A IN MAINTENANCE	1.26E-02	5.34E-02
1-EPS-DGN-MA-G4002___	DG1B IN MAINTENANCE	1.26E-02	5.00E-02
1-EPS-SEQ-FO-1821U302	SEQUENCER B FAILS TO OPERATE	3.33E-03	4.41E-02
1-EPS-SEQ-FO-1821U301	SEQUENCER A FAILS TO OPERATE	3.33E-03	4.33E-02
1-IE-OTRANS	OTHER TRANSIENT	3.99E-01	3.95E-02

Name	Description	Probability/ Frequency	FV
1-IE-MLOCA	MEDIUM LOCA	5.10E-04	3.66E-02
1-OEP-XHE-XX-NR02HWR1	CONVOLUTION FACTOR FOR 1FTR-OPR (2HR-WR AVAIL)	4.86E-01	3.42E-02
1-IE-LOOPPC	LOSS OF OFFSITE POWER (PLANT- CENTERED)	1.93E-03	3.00E-02
1-OEP-XHE-XX-NR02HGR1	CONVOLUTION FACTOR FOR 1FTR-OPR (2HR-GR AVAIL)	1.86E-01	2.88E-02
1-IE-SSBO	SECONDARY SIDE BREAK OUTSIDE OF MSIVS	7.70E-03	2.48E-02
1-DCP-BAT-MA-AD1B____	BATTERY 1AD1B IN MAINTENANCE	2.72E-03	2.44E-02
1-DCP-BAT-MA-BD1B____	BATTERY 1BD1B IN MAINTENANCE	2.72E-03	2.43E-02

Table 9-4 Significant Basic Events with FV Importances Greater than 0.005 (cont.)

Name	Description	Probability/ Frequency	FV
1-OAB_TR-------H	OPERATOR FAILS TO FEED AND BLEED - TRANSIENT	5.80E-02	2.41E-02
1-OA-NSCWFAN---H	OPERATOR FAILS TO START NSCW FAN MANUALLY (PLACE HOLDER)	1.00E+00	2.24E-02
1-IE-LO4160VA	LOSS OF 4.16 kV BUS A	1.09E-03	2.24E-02
1-RCS-XHE-XM-TRIP	OPERATOR FAILS TO TRIP REACTOR COOLANT PUMPS	3.30E-01	2.14E-02
1-EPS-DGN-FS-G4001___	DG1A FAILS TO START BY RANDOM CAUSE	2.94E-03	2.13E-02
1-EPS-DGN-FS-G4002___	DG1B FAILS TO START BY RANDOM CAUSE	2.94E-03	2.10E-02
1-NSCWCT-SPRAY	NSCW CTS IN SPRAY MODE (FRACTION OF TIME)	9.04E-01	2.09E-02
1-RCS-XHE-XM-TRIP-LONSCW	OPERATOR FAILS TO TRIP REACTOR COOLANT PUMPS (LONSCW)	5.40E-03	2.02E-02
1-EPS-DGN-CF-FRUN1	CCF OF UNIT 1 DGNS G4001/G4002 TO RUN	3.24E-04	1.90E-02
1-OAR_HPML-----H	OPERATOR FAILS TO ESTABLISH HIGH PRESSURE RECIRCULATION - MLOCA	2.31E-03	1.84E-02

Name	Description	Probability/ Frequency	FV
1-OA-OSW-------H-CD	OPERATOR FAILS TO ESTABLISH SINGLE PUMP NSCW PUMP OPERATION (COMPLETE DEPENDENCE)	1.00E+00	1.77E-02
1-IE-TTRIP	TURBINE TRIP	1.70E-01	1.67E-02
1-CVC-MDP-FR-NCP4001&	NORMAL CHARGING PUMP 1208P4001 FAILS TO RUN (1 YEAR)	1.82E-01	1.63E-02
1-IE-LOSINJ	LOSS OF SEAL INECTION	1.00E+00	1.62E-02
1-IE-RTRIP	REACTOR TRIP	1.56E-01	1.53E-02
1-OA-OSW-------H	OPERATOR FAILS TO ESTABLISH SINGLE PUMP NSCW PUMP OPERATION	2.00E-02	1.42E-02
1-IE-LO4160VB	LOSS OF 4.16 kV BUS B	1.09E-03	1.37E-02
1-OEP-XHE-XX-NR02HWR2	CONVOLUTION FACTOR FOR 2FTR-OPR (2HR-WR AVAIL)	3.64E-01	1.35E-02
1-IE-LO125BD1	LOSS OF DC BUS 1BD1 SPECIAL INITIATOR IDENTIFIER	1.00E+00	1.35E-02
1-DCP-BDC-FC-BD1&____	125 V DC BUS 1BD1 FAILS - 1 YR	2.06E-03	1.35E-02
1-AFW-TDP-FR-P4001___	TDAFWP (P4-001) FAILS TO RUN	3.80E-02	1.34E-02

Name	Description	Probability/ Frequency	FV
1-ACP-BAC-MA-AA02____	BUS 1AA02 IN MAINTENANCE	2.15E-04	1.33E-02
1-AFW-MDP-MA-P4002___	AFW MDP B (P4-002) UNAVAILABLE DUE TO TEST OR MAINT	3.00E-03	1.23E-02
1-RCS-MDP-LK-BP1	RCP SEAL STAGE 1 INTEGRITY (BINDING/POPPING OPEN) FAILS	1.25E-02	8.63E-03
1-IE-LOMFW	LOSS OF MAIN FEED WATER	6.61E-02	8.14E-03
1-OEP-VCF-LP-CLOPL	CONSEQUENTIAL LOSS OF OFFSITE POWER - LOCA	3.00E-02	8.10E-03
1-IE-LOCHS	LOSS OF CONDENSER HEAT SINK	6.01E-02	7.43E-03
1-OEP-XHE-XL-NR01HGR	OPERATOR FAILS TO RECOVER OFFSITE POWER IN 1 HOUR (GRID-RELATED)	6.59E-01	7.10E-03
1-ACP-BAC-MA-BA03____	4160 V BUS 1BA03 IN MAINTENANCE	2.15E-04	6.25E-03
1-NSCWCT-BYPASS	NSCW CTS IN BYPASS MODE (FRACTION OF TIME)	9.62E-02	6.18E-03
1-ACP-BAC-MA-BB16____	480 V SWITCHGEAR 1BB16 IN MAINTENANCE	2.15E-04	5.77E-03
1-AFW-PMP-CF-RUN	AFW PUMPS FAIL FROM COMMON CAUSE TO RUN (EXCLUDING DRIVER)	1.55E-05	5.76E-03

Name	Description	Probability/ Frequency	FV
1-ACP-INV-MA-AD1I11__	INVERTER 1AD1I11 IN MAINTENANCE	8.81E-04	5.63E-03
1-IE-LO125AD1	LOSS OF DC BUS 1AD1 SPECIAL INITIATOR IDENTIFIER	1.00E+00	5.62E-03
1-DCP-BDC-FC-AD1&____	125 V DC BUS 1AD1 FAILS - 1YR	2.06E-03	5.61E-03
1-ACP-BAC-MA-AB15____	480 V SWITCHGEAR 1AB15 IN MAINTENANCE	2.15E-04	5.53E-03
1-OAR_HPSLA----H-LD	OPERATOR FAILS TO ESTABLISH HPR - SLOCA WITH CCUS AVAILABLE (LOW DEPENDENCY)	5.06E-02	5.46E-03
1-OEP-XHE-XX-NR02HWR0	CONVOLUTION FACTOR FOR CCF-OPR (2HR-WR AVAIL)	4.86E-01	5.38E-03
1-EPS-DGN-CF-FSUN1	CCF OF UNIT 1 DGNS G4001/G4002 TO START	3.68E-05	5.35E-03
1-OAB_TR-------H-HD	OPERATOR FAILS TO FEED AND BLEED - TRANSIENT (HIGH DEPENDENCE)	5.29E-01	5.34E-03
1-EPS-MDP-FS-XFERPPS_-CC	CCF OF DG FUEL TRANSFER PUMPS TO START	3.53E-05	5.13E-03

- *Unavailability of EDG 1A or 1B due to Testing/Maintenance*— The unavailability of an EDG due to testing/maintenance causes a lack of electrical power to its associated safety-related 4.16 kV AC bus; therefore, rendering one train of safety-related components unavailable.

- *Failure Sequencers A or B*— The failure of either of the two sequencers during a LOOP or SI actuation prevents the applicable EDG from loading onto its associated safety-related 4.16 kV AC bus; therefore, rendering one train of safety-related components unavailable.

Additional key SSC unavailabilities based on the RAW importance measure are:

- *Failure of CST 1*— The failure of condensate storage tank (CST) 1 will cause the loss of the entire AFW system.[228]

- *Failure of 4.16 kV AC Bus 1AA02*— The failure of this safety-related 4.16 kV AC bus leads to the failure of one train of safety-related components.[229]

- *4.16 kV AC Bus 1AA02 in Maintenance*— The unavailability of this safety-related 4.16 kV AC bus leads to the unavailability of one train of safety-related components.

Common-Cause Failures

The top CCFs based on the FV importance measure are:

- *CCF of Switchyard Breakers AA205 and BA301 to Open*— The CCF of these two breakers prevents the EDGs from loading onto the two safety-related 4.16 kV AC buses; therefore, causing a non-recoverable loss of all 4.16 kV AC power and rendering all safety-related equipment unavailable.

- *CCF of Sequencers A and B*— The CCF of the two safeguards load sequencers during a LOOP prevents the EDGs from loading onto the two safety-related 4.16 kV AC buses; therefore, causing a non-recoverable loss of all safety-related 4.16 kV AC power and rendering all safety-related equipment unavailable.[230]

- *CCF of the NSCW Motor-Driven Pumps (SSIE Fault Tree Event)*— The CCF of all six of the NSCW motor-driven pumps causes a loss of the ultimate heat sink.

---

[228] Additional source of AFW inventory (e.g., CST 2) is not credited in the L3PRA Project Level 1 model if a CST ruptures.

[229] Bus 1AA02 supplies the battery chargers for DC trains A and C. DC train C provides power to the turbine-driven AFW pump; thus, accounting for the greater importance of Bus 1AA02 (as compared to Bus 1BA03).

[230] If both sequencers fail during an SI actuation without a LOOP (initiating event or consequential), normally running components such as the ACCW and NSCW pumps will remain running (i.e., the sequencers do not shed loads if neither of the 4.16 kV safety-related buses experience an under-voltage condition). However, the sequencers will prevent additional NSCW cooling tower fans from automatically starting (one fan in each train is assumed to be running). The L3PRA project Level 1 model assumes a 3 of 4 NSCW fan success criterion per train; therefore, both sequencers failing results in a loss of all NSCW. If a LOCA has occurred (e.g., initiating event, stuck-open pressurizer PORV, RCP seal failure) core damage is assumed because all ECCS require NSCW.

Additional key CCFs based on the RAW importance measure are:

- *CCF of four or more NSCW Motor-Driven Pumps*— The subsequent CCF of four or more NSCW motor-driven pumps (after an initiating event other than the loss of NSCW) causes a loss of the ultimate heat sink.[231]

- *CCF of Safety-Related 125 V DC Battery Chargers*— The CCF of the safety-related battery chargers will eventually lead to the loss of all 125 V DC safety-related power leading to the unavailability of AFW and subsequent core damage.[232]

- *CCF of 10 or More Control Rods to Insert into the Core*— The CCF of 10 or more control rods to insert into the core will lead to an unsuccessful reactor trip and subsequent ATWS.

- *CCF of Safety-Related 125 V DC Batteries*— The CCF of the safety-related batteries causes the loss of all 125 V DC safety-related power leading to the unavailability of AFW and subsequent core damage.

- *CCF of the AFW Pumps to Run*– The CCF of the AFW pumps to run causes the complete unavailability of the AFW system.

Operator Actions

The top human errors based on the FV importance measure are:

- *Operator Fails to Restore Systems after AC Power is Recovered from an SBO*— The failure of operators to restore systems (e.g., the motor-driven AFW pumps or alignment of battery charger to the DC train C to allow for continued operation of the turbine-driven AFW pump) after AC power is recovered to the safety-related 4.16 kV AC buses is assumed to result in core damage.

- *Operators Fail to Recover Offsite Power within 2 Hours of Grid-Related or Weather-Related LOOP*— The failure of operators to recover offsite power within 2 hours (i.e., the turbine building battery depletion time) during a LOOP and subsequent SBO is assumed to result in core damage.

- *Operators Fail to Trip the RCPs*— During a complete loss of RCP seal injection and cooling, operators have approximately 13 minutes to trip the RCPs. If operators fail to the trip the RCPs, seal failure is assumed to occur resulting in a SLOCA (480 gallons per minute per RCP).

---

[231] The pump success criterion for the NSCW system is two-of-three pumps successfully operate on either train. Therefore, only those CCF cross-combinations of four or more NSCW pumps that involve at least two pumps failing on each train (thereby resulting in system failure) are included in this CCF event.

[232] The importance of basic events that cause the loss of safety-related 125 V DC power is heavily influenced by the L3PRA Project Level 1 model assumptions of not crediting turbine-driven AFW pump operation after depletion of the safety-related batteries (see Section 8.1.2 for additional information). Note that the loss of safety-related 125 V DC power also renders feed and bleed cooling unavailable.

- *Operators Fail to Initiate Feed and Bleed Cooling during a Transient*— The failure of operators to initiate feed and bleed cooling (given the failure or unavailability of AFW and MFW) will result in core damage.

Additional key human errors based on the RAW importance measure are:

- *Operator Fails to Restore RWST Isolation Valve after Test/Maintenance*— The failure of operators to reopen the RWST isolation valve renders all applicable ECCS unavailable.

- *Operators Fail to Establish High-Pressure Recirculation during a MLOCA*— The operator failure to align the containment sump to the SI pumps/CCPs after successful HPI during a MLOCA leads directly to core damage.

- *Post-Test Mispositioning of Motor-Driven AFW Pump B Suction Valve*— The mispositioning of motor-driven AFW pump B suction manual valve causes the unavailability of the motor-driven AFW pump B.[233]

9.2.4 Parameter Uncertainty

The estimated mean CDF for the L3PRA project Level 1 model is 6.3×10^{-5} per RCY. Additional parameter uncertainty results are provided in Table 9-5 and in Figure 9-3. The state-of-knowledge correlation is satisfied using template events for correlated basic events and CCF alpha factors; see Section 7.2 for additional information.

Table 9-5 L3PRA Project Level 1 Model Parameter Uncertainty Calculation Results

Point Estimate CDF	Mean CDF	5th Percentile	Median	95th Percentile	Standard Deviation
6.39E-05	6.34E-05	1.74E-05	4.64E-05	1.61E-04	6.67E-05

[233] The train B suction valve has a higher importance than train A suction valve. This difference is because the concurrent closure of the train B suction valve and failure of safety-related 4.16 kV AC bus 1AA02 results in the loss of all three AFW pumps. Whereas, the concurrent closure of the train A suction valve and the failure of safety-related 4.16 kV AC bus 1BA03 only results in the loss of the two motor-driven pumps.

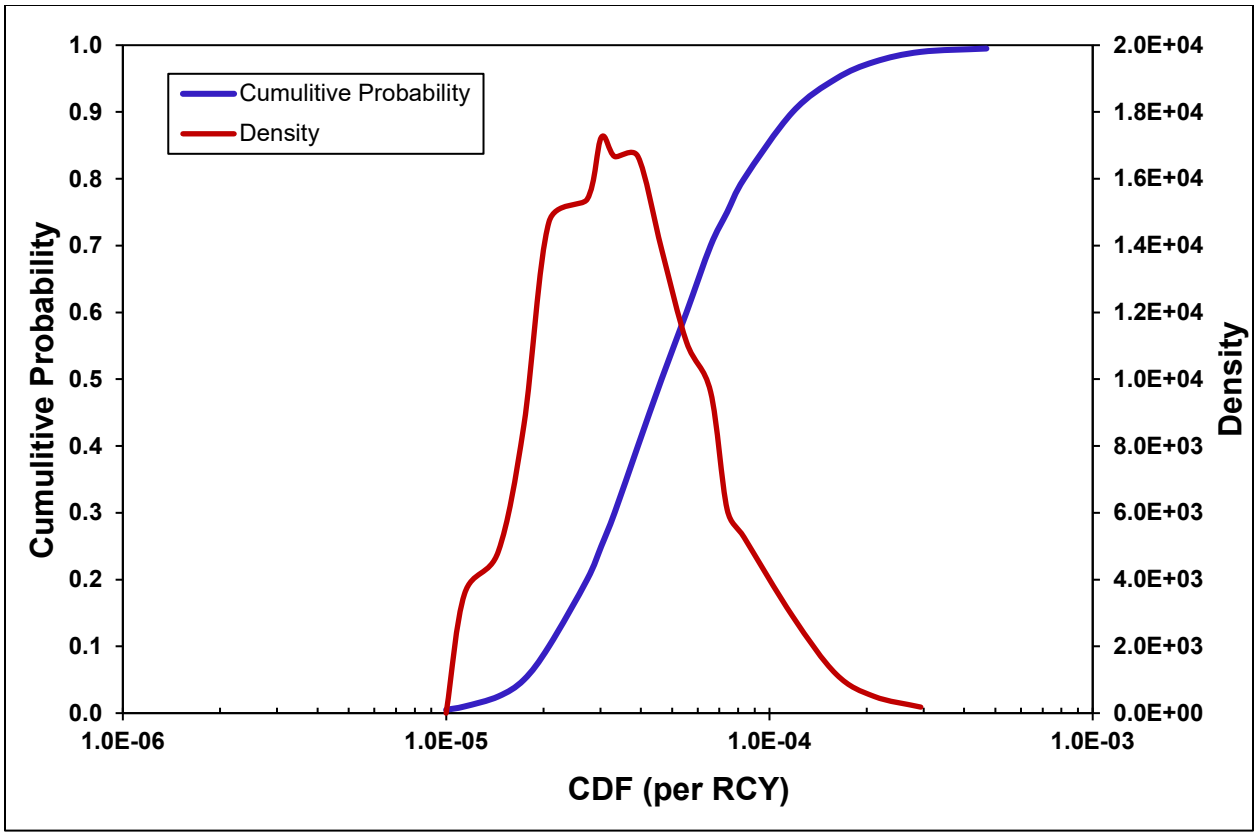


Figure 9-3 Probability Density and Cumulative Distribution Functions for Internal Event CDF

Truncation and Model Convergence

The quantification results for all PRA models are impacted by the truncation limits used during the quantification process. The truncation limit used should demonstrate convergence towards a stable result. ASME/ANS Level 1 PRA standard supporting requirements QU-B2 and QU-B3 dictate that:

- Accident sequences and associated system models are truncated at a sufficiently low cutoff value that dependencies associated with significant cut sets or accident sequences are not eliminated.

- An iterative process with convergence is considered sufficient when successive reductions in truncation value of one decade result in decreasing changes in CDF, and the final change is less than 5 percent.

The L3PRA project Level 1 model was quantified at various truncation levels to ensure model (i.e., CDF) convergence and to determine how many cut sets were removed at the various levels. The results of these calculations are provided in Table 9-6. Based on these results, a quantification level of 10^{-12} is deemed sufficient to satisfy supporting requirements QU-B2 and

QU-B3, even though some significant cut sets are not present at this level.[234] A review of the significant cut sets at the 10^{-13} truncation level show only four additional significant cut sets in the top 500 and none within the top 200 (when compared to the significant cut sets at the 10^{-12} truncation level). Note that using truncation levels below 10^{-12} substantially increases model solve times that will be further exacerbated when additional models (e.g., external hazards and Level 2) are integrated into the L3PRA project Level 1 model for internal events.

Table 9-6 L3PRA Project Level 1 Model Truncation Analysis Summary

Truncation	CDF	# of Cut Sets	# of Significant Cut Sets	Change in CDF (%)
1.0E-13	6.42E-05	437,072	3,422	0.4%
1.0E-12	6.39E-05	141,450	3,188	1.1%
1.0E-11	6.32E-05	41,883	2,746	1.8%
1.0E-10	6.20E-05	10,701	1,850	

9.3 Key Insights

This section discusses some key insights identified during the development of the L3PRA Level 1 model for internal events. Note that many of these insights are not solely relevant to this project, but likely affect PRAs at other plants. Some of these issues are discussed in Section 8 and/or are identified as key modeling uncertainties in Section 10 of this report.

AC Power Recovery

Model results indicate that LOOP/SBO is the dominant risk contributor for the reference plant. This is likely the case for many plants in the U.S., given similar modeling assumptions are used. Several LOOP/SBO modeling assumptions used in the L3PRA Level 1 model are potentially conservative (as discussed in Section 8.1). In most cases, these assumptions, described below, result from the lack of information (e.g., operating experience or applicable testing data). Discussions with industry experts could reduce the extent of modeling conservativism. It is also important to note that future modeling considerations (e.g., incorporation of FLEX mitigations strategies) could reduce the impact of these potential conservatisms.

- AC power recovery is not applied to SBO scenarios that are a result of SSC failures that would render AC power either unrecoverable or ineffective. The two most notable examples are the failure of the RAT breakers to open and sequencer failures. It is likely (as in most SSC failures) that recovery is possible in some cases. For example, it may

[234] The L3PRA project Level 1 model applies dependency between HFEs using post-processing rules. These post-processing rules are applied after the cut sets have been solved and truncation has been applied. Therefore, some cut sets that contain dependent HFE combinations will be truncated prior to the application of the dependency. The effects of this "premature" truncation were evaluated as part of the dependency evaluation and are estimated to be approximately 1 percent of the overall CDF.

be possible to realign power through the RAT breakers if they are mechanically failed shut, but not electrically faulted. Failure of the sequencers could still allow the operators to manually start safety-related SSCs. Discussions with system experts and a detailed data review may decrease uncertainties associated with recovery of key SSC failures.

- No credit was allowed for recovery of offsite power following depletion of the (most limiting) plant batteries required to realign offsite power to a safety-related bus (i.e., the turbine building batteries, with a 2-hour design lifetime). The SBO procedure (ECA-0.0) provides direction for shedding unnecessary DC loads on the safety-related batteries, but does not address prolonging the life of the turbine building batteries.

- Realignment of offsite power requires that DC power be available to operate some of the breakers and switchers. It is not clear how operators would respond if the procedural prerequisite for DC power is not met. Some of the breakers and switchers that are needed to restore offsite power to the safety-related 4.16 kV AC buses can be operated manually with a local hand crank, while some cannot be operated manually without DC power. Given this, the L3PRA project Level 1 model uses the potentially conservative assumption that AC power must be recovered prior to depletion of the most limiting plant batteries required to realign offsite power to a safety-related bus.

- Developing procedures for restoring offsite power to the safety-related buses in the absence of DC power (assuming such capability exists) would allow such credit in PRAs. In addition, analyses could potentially demonstrate that the limiting batteries can support the manipulation of the necessary components to restore offsite power beyond their design lifetime, or procedures for extending the lifetime of these batteries could be developed allowing such credit in PRAs.

- No credit was provided for continued operation of the turbine-driven AFW pump after DC power is lost. Since the L3PRA project Level 1 model assumes that AC power recovery must occur prior to depletion of the most limiting plant batteries (i.e., the turbine building batteries), if AC power is not recovered within 2 hours, “blind” operation of the turbine-driven AFW pump would only delay core damage, not prevent it, due to continual RCP seal leakage. Also, even though the action to operate the turbine-driven AFW pump without DC power is proceduralized, with no reliable indication of SG water level (after the safety-related batteries are depleted at 4 hours), there is significant potential for unsustainable operation (e.g., overfilling the steam generators and flooding the steam lines, including the AFW pump turbine). Therefore, any potential credit would be minimal. Further testing and training on this action would facilitate greater credit for it in PRAs for delaying core damage (or preventing core damage if accomplished in combination with actions to restore AC power following the loss of DC power).

Safe/Stable End States

The American Society of Mechanical Engineers/American Nuclear Society (ASME/ANS) PRA standard (ASME/ANS, 2009) defines a safe/stable state as “a plant condition, following an initiating event, in which RCS conditions are controllable at or near desired values.” Supporting requirement AS-A2 states, “for each modeled initiating event, identify the key safety functions that are necessary to reach a safe, stable state and prevent core damage.” Supporting requirement SC-A5 elaborates by stating that (for capability category II/III) additional evaluations must be performed for sequences where stable plant conditions are not achieved at 24 hours.

MELCOR calculations performed for the L3PRA project identified some SGTR sequences where core damage is expected to occur shortly after 30 hours. In addition, sequences involving an RCP seal leakage rate of less than or equal to 21 gallons per minute (gpm) per RCP with AFW available can eventually result in core damage if primary system make-up is not available.

After considering various options for those event tree sequences that are safe (i.e., no core damage), but not stable, at 24 hours (i.e., they would result in core damage at some point after 24 hours), the L3PRA project Level 1 model generally extends these accident sequences to 72 hours (see Section 8.3 for additional information). Although a sensitivity analysis on this issue (documented in Section 10.5) showed little impact on total CDF in the L3PRA model, this is an area that may be appropriate for additional evaluation.

Initiating Event Frequencies

There are some initiating event frequencies associated with very rare events that have a significant risk impact (e.g., grid-related LOOP, medium LOCA, and loss of 4.16 kV safety-related AC bus). Some of these events have not occurred at a U.S. nuclear power plant, while others have only occurred at a handful of plants. Regardless of the technique used to calculate the initiating event frequency (e.g., Bayesian update process or expert elicitation), the uncertainties associated with these events are likely higher than most other parameters considered in the L3PRA project Level 1 model for internal events. Specifically with regard to calculating grid-related LOOP frequency, other techniques, as described in the sensitivity analysis provided in Section 10.2 or WCAP-16565, "Considerations for Risk Informed Modeling of Grid Centered Loss of Offsite Power Events," could be reviewed to determine if these provide better estimates.[235]

Consequential LOOP

LOOP is modeled in PRAs as an initiating event. Offsite power can also be lost after other initiating events that are modeled in the PRA. This subsequent loss of offsite power can be completely random, or can be influenced by the events occurring at the plant. Following a reactor trip, the offsite electrical grid is taxed not only by the loss of voltage support from the reactor, but also due to the transfer of plant nonsafety-related loads from the unit auxiliary transformer to the RATs, which are supplied from the offsite grid. Also, following an SI actuation, the grid is further stressed by the in-rush current that accompanies the starting of the ECCS loads and, therefore, increasing the potential that the safety-related bus degraded voltage protection relays will actuate, resulting in a consequential LOOP.

In the L3PRA project, consequential LOOPs are modeled explicitly in the Level 1 model AC power fault tree logic, consistent with the current state-of-practice. The modeling of the potential for consequential LOOPs using the fault tree approach has the major benefit of not impacting the events trees and other fault trees; however, as discussed in Section 8.2, there are a number of limitations with this approach. In addition, a recent review of the LOOP database revealed concerns with the classification of several of the consequential LOOPs following a reactor trip, and also noted that the probability of a consequential LOOP following a reactor trip or SI actuation does not reflect recent operating experience (the data period considered for consequential LOOP following a reactor trip was 1997–2004, and the data period considered for

[235] WCAP-16565 is not publicly available and has not been reviewed by the NRC.

a consequential LOOP following an SI actuation was 1986–2006). As such, estimations of the risk impacts of consequential LOOPs would benefit from a new data evaluation and other research into improved consequential LOOP modeling.

Large Common-Cause Failure Groups

The uncertainties associated with CCFs for components in common-cause component groups (CCCGs) of greater than four are likely to have larger uncertainties. CCF events are rare, and the population of observed events consists mostly of low-order failures. However, the dominant cut sets in the model include some high-order failure events (e.g., NSCW pumps and fans). The scaling methodology used to estimate alpha factors for high-order groups based on events observed in low-order groups may be state-of-practice, but it is not easily validated for high-order CCCGs. A detailed review of the CCF data could help to determine the level of potential conservatism in CCF parameters of high-order CCCGs.

10 KEY SOURCES OF MODEL UNCERTAINTY

The American Society of Mechanical Engineers/American Nuclear Society (ASME/ANS) probabilistic risk assessment (PRA) standard (ASME/ANS, 2009) has several supporting requirements (e.g., IE-D3, AS-D3, SC-C3, SY-C3, HR-I3, DA-E3, and QU-E1) that direct that the sources of modeling uncertainty be documented. In addition, QU-E4 directs that the sources of model uncertainty be characterized. The key sources of model uncertainty for the L3PRA project Level 1 internal event model are provided in Table 10-1.

Table 10-1 L3PRA Project Level 1 Model Key Sources of Modeling Uncertainty

Technical Element	Topic	Description	Characterization
Initiating Event Analysis	Steam Generator Tube Rupture (SGTR) Break Size	For both initiator and pressure-induced SGTRs, the modeling assumes that the break is a double-ended guillotine break of a single tube. And like pipe breaks, there is a spectrum of possibilities that could be modeled in a PRA, ranging from leaks just exceeding normal makeup capacity all the way to the rupture of multiple tubes.	Larger breaks would be generally less frequent, while smaller breaks would be generally less consequential. The use of a single break size to represent this range is reflective of the state-of-practice. Nevertheless, finer discretization of this break range (which would require the development of separate accident sequence assumptions) would be expected to produce a somewhat different result.
	LOCA Initiating Events Frequencies	There are uncertainties associated with the LOCA initiating frequencies given the lack of data.	This uncertainty can impact all LOCA initiating event frequencies, of which the medium LOCA is most risk-significant. A sensitivity analysis using an alternative medium LOCA initiating event frequency is provided in Section 10.1.

Table 10-1 L3PRA Project Level 1 Model Key Sources of Modeling Uncertainty (cont.)

Technical Element	Topic	Description	Characterization
Initiating Event Analysis (cont.)	CCF of Isolation Valves Resulting in Interfacing-Systems Loss-of-Coolant Accident (ISLOCA)	In the screening of potential ISLOCA pathways, a 3-valve screening rule was applied to eliminate pathways that have very low combined failure frequencies (see Section 3.5 for additional information). However, CCF of these valves was not explicitly considered as part of this evaluation. [Note, for the ISLOCA pathways modeled, conditional failure of a second isolation valve in series given failure of the first isolation valve, was included and quantified based on expert elicitation (see Section 3.5.1 for additional information).]	The potential exists for CCF to dominate the combined valve failure frequency. Depending on the calculated CCF probabilities, the application of the 3-valve pathway screening rule may prematurely eliminate ISLOCA pathways that have frequencies that are not negligible. However, most of the screened ISLOCA pathways also have at least one source of mitigation and some valve diversity; and therefore, are not expected to contribute substantially to ISLOCA core damage frequency.
	Service Water System Initiating Event Frequencies	Total loss of service water has not been seen in the industry operational experience. Service water systems vary widely in design, and in the extent to which they are influenced by environmental factors, so an industry average estimate of initiating event frequency is only loosely applicable to any given system.	Initiating event fault tree methodology is used to obtain a plant-specific estimate of the NSCW system initiating event frequency. The estimate results are dominated by CCF events that are subject to the CCF uncertainties described in this table. CCF modeling issues with the greatest impact on the frequency estimate include mapping of failure events observed in small component groups to larger ones and limiting causal influence on components of identical type.
	LOOP Initiating Event Frequency	Grid-related offsite power events have the potential to affect multiple units at the same time. This introduces dependency (i.e., double-counting) in the frequency estimate that is currently ignored, leading to conservative estimates of grid LOOP frequency.	Grid-related LOOP initiating event frequency is an upper bound. A sensitivity analysis using an alternative grid-related LOOP initiating event frequency is provided in Section 10.2.
Initiating Event	Partial LOOPs Are Not	Some portion of the partial LOOP frequency is neglected. The loss of AC bus data	Partial LOOPs in which emergency power is available are not explicitly considered in the L3PRA project

Analysis (cont.)	Explicitly Modeled	collection captures partial LOOP events for which emergency power is unavailable to the bus. However, partial LOOP events with emergency power available are not included, and therefore neglected currently in the L3PRA project Level 1 model.	Level 1 model. These events would not be expected to contribute substantially to the overall CDF because emergency power would have to fail to cause a transient. In addition, offsite power can usually be realigned to the affected bus via an alternate path for these scenarios.
Accident Sequence Analysis	Consequential LOOP Modeling	The impact of consequential LOOP events is considered within the AC power fault trees for applicable structures, systems, and components (SSCs).	The fault tree approach used to model consequential LOOPs in the L3PRA project Level 1 model has certain limitations. For example, credit for AC power recovery needed to be implemented using post-processing rules; and therefore, recovery was applied after the cut sets were initially calculated. This approach was conservative because only the dominant consequential LOOP contributors were reviewed to determine if credit for offsite power recovery could be applied.
Accident Sequence Analysis (cont.)	Continued Equipment Operation after Battery Depletion	During a SBO with the subsequent depletion of safety-related batteries given the failure to restore AC power to a safety-related 4.16 kV bus, the L3PRA project Level 1 model assumes the turbine-driven auxiliary (AFW) pump is rendered unavailable. Even though procedures may exist to manually run the pump locally, no instrumentation [e.g., steam generator (SG) level] is available for the operators; therefore, the potential for under- or over-filling the SGs exists.	The modeling assumption to not credit continued turbine-driven AFW pump operation after battery depletion in the L3PRA project Level 1 model is conservative. However, it is difficult to assess the potential credit for success of this operator action given the lack of instrumentation and the AFW flow control needed for the complete mission time and to reach a safe/stable end state. This modeling uncertainty has substantial effect on CDF because successful turbine-driven AFW pump operation after battery depletion could allow operators to place the plant in a safe/stable end state without AC power recovery. The impact of this modeling approach is amplified by the related assumptions regarding the limiting battery lifetime (see "Battery Depletion Times" in this table) and AC power recovery (see "AC Power Recovery Not Credited after Battery Depletion" in this table). A sensitivity analysis crediting

			continued turbine-driven AFW pump operation after battery depletion is provided in Section 10.3.
	Pressure-Induced SGTR	The model considers pressure-induced SGTRs in a few different contexts, as discussed in Section 8.5. That section describes assumptions made in the modeling (both in the estimates of a SGTR occurring as well as when it was necessary to explicitly consider SGTR versus when it was not).	The modeling employed for pressure-induced SGTR is generally conservative based on the assessment performed (i.e., assumptions generally defaulted to over-representing induced SGTR contribution). However, given the numerous uncertainties involved in the overall assessment, different analysts could arrive at different models for this issue. Pressure-induced SGTR is a substantially smaller CDF contributor than SGTR initiating events (approximately 1 percent of the overall SGTR CDF) in the L3PRA project Level 1 model.
Accident Sequence Analysis (cont.)	Late Depressurization	The model considers late operator-induced depressurization for many sequences, while not considering it for many others. The latter category includes multiple instances where depressurization might be attempted based on some interpretations of the procedures or technical support center (TSC) guidance, but where it is not clear that it would be attempted due to the procedural pathway (e.g., being in a holding pattern awaiting restoration of certain equipment).	Different modeling assumptions might result in a larger number of sequences querying late depressurization, and thus, a higher proportion of sequences either avoiding core damage (due to recovery using low-pressure systems) or proceeding to core damage with lower pressure. What effect this alternate modeling would have on CDF and release categorization is not clear.
	AC Power Recovery Not Credited after Battery Depletion	The L3PRA project Level 1 model uses the potentially conservative assumption that AC power recovery must occur prior to depletion of the most limiting plant batteries required to realign offsite power to a safety related bus, which are the turbine building batteries (with a 2-hour lifetime). See Section 8.1.1 for additional information.	This modeling assumption is potentially conservative and has a significant effect on the overall CDF. Plant or ex-plant operators may be able to manipulate breakers that do not have their normal supply of direct current (DC) power via portable equipment. Procedural guidance is needed to credit these actions. The impact of this modeling assumption is amplified by the related assumptions regarding the limiting battery lifetime (see “Battery Depletion Times” in this table) and not crediting operation

			of the turbine-driven AFW pump after battery depletion (see "Continued Equipment Operation after Battery Depletion" in this table). A sensitivity analysis crediting the restoration of offsite power without DC power is provided in Section 10.4.
Accident Sequence Analysis (cont.)	Different Break Sizes within LOCA Categories	Each of the traditional LOCA categories (e.g., small, medium, and large) cover a break size range. However, thermal hydraulic calculations often show different behavior at the different ends of the LOCA category break size spectrum. These differences are especially noticeable for small and medium break LOCAs.	An attempt was made to reduce these uncertainties by selecting break sizes near the ends of the spectrum for supporting thermal hydraulic analyses; however, the entire break-size spectrum was not covered. Analyses using the complete spectrum of break sizes would likely yield additional LOCA categories, which would, in turn, allow the use of more realistic (i.e., less conservative) success criteria.
	Anticipated Transient without Scram (ATWS) during Large and Medium LOCAs	Failure of the reactor to trip after a large or medium LOCA initiating event is conservatively assumed to result in core damage. During these scenarios the reactor core is expected to experience voiding that may be sufficient to shut down the reactor.	This assumption has negligible impact on CDF.
	Consequential LOCA Modeling Following AC Power Recovery during an SBO	The SBO-1 tree is based on the same general modeling assumptions as the small LOCA (including consequential) event trees. As such, its success criteria and sequence timing presume that conditions prior to AC power recovery are not significantly degraded beyond those associated with non-SBO small LOCAs (e.g., no consideration is given to the potential effects of loss of RCS inventory for 1–2 hours prior to initiating high-pressure injection or cooldown/depressurization); however, no scenario-specific thermal-hydraulic calculations have been performed to validate this assumption. New plant-	Refinement of this modeling assumption would be expected to lead to an increase in the fraction of CDF stemming from LOOP events with AC power recovery and consequential LOCAs.

		specific thermal-hydraulic calculations would be needed to address this uncertainty.	
Accident Sequence Analysis (cont.)	AC Power Recovery to 4.16 kV Buses	The L3PRA project Level 1 model assumes that if AC power is recovered, power is available to both 4.16 kV safety-related buses. However, the offsite power recovery data is applicable for restoration of a single safety-related bus. In addition, it is possible that the LOOP and subsequent SBO is due (at least partially) to SSC failures that would preclude recovery of AC power to 1 of the 2 buses. Note that the L3PRA project Level 1 model does not credit AC power recovery if both safety-related 4.16 kV buses experience non-recoverable failures or recovery of AC power to the nonsafety-related buses (a potentially conservative assumption). Also, note that identification of the electrical-related failures that preclude offsite power recovery was based on review of the dominant SBO contributors.	This modeling assumption is potentially non-conservative, though it is difficult to assess the potential impact on CDF. In many cases, SSC failures that would preclude offsite power recovery on 1 of the 2 safety-related buses are accounted for in the electrical dependency portion of the applicable, post-SBO recovery fault trees. However, there are exceptions (e.g., RAT breaker failures to open). A review of the applicable fault trees and dominant cut sets appears to indicate that the overall CDF impact of this potential non-conservative modeling assumption would be minimal. A complete evaluation would need to be performed to determine additional electrical-related failures that would prevent the recovery of offsite power.
	Modeling Safe/Stable End States	Many PRAs only assume core damage if it occurs within 24 hours of accident initiation, or shortly thereafter. The LPRA Project Level 1 model generally extends accident sequences to 72 hours given that they are safe (i.e., no core damage), but not stable, at 24 hours (i.e., they would result in core damage at some point after 24 hours). See Section 8.3 for additional information.	A sensitivity analysis assuming a safe/stable end state is reached if core damage does not occur at or near 24 hours is provided in Section 10.5, and demonstrates that extending the mission time to 72 hours for sequences that are not stable at 24 hours does not have a significant impact on CDF.
Success Criteria	RCP Seal Failure Modeling	The L3PRA project Level 1 model uses the Westinghouse Owner's Group (WOG) 2000 RCP seal leakage model (Westinghouse, 2002) to determine the probability of failure of RCP seals given the	The WOG 2000 RCP seal leakage model is a consensus model; however, it is still believed to be a key source of modeling uncertainty. Note, RCP seal LOCAs are a major contributor to CDF.

		loss of all seal injection/cooling. In addition, the WOG 2000 model provides timing assumptions used to evaluate the recovery of RCP seal injection and elevated seal leakage rates given a loss of seal injection with no seal failure.	
	NSCW System Success Criteria	The success criteria for the NSCW pumps and fans were not verified with thermal-hydraulic calculations, nor was the timing for aligning for single pump operation. The time available used to evaluate the applicable human failure event (HFE), OA-OSW-------H, is believed to be conservative.	Additional thermal-hydraulic calculations could be used to reduce potential uncertainties with NSCW pump and fan success criteria and the potential conservatism associated with the applicable HFE. Note, loss of the NSCW system is a major contributor to CDF.
	Loss of Room Cooling	The dependency on room cooling for mitigating systems was screened out the L3PRA project Level 1 model.	The following key components could be impacted given a loss of room cooling (not an exhaustive list): • AFW pumps • Emergency core cooling system (ECCS) pumps • Emergency diesel generators (EDGs) • Auxiliary component cooling water (ACCW) pumps • Safety-related electrical buses
Success Criteria (cont.)	RCP Performance under Degraded Conditions	The NRC MELCOR calculations assume that the RCPs trip at 10 percent voiding (if they have not already tripped for other reasons).	This is primarily of importance only for sequences where the RCPs may continue to operate during the time of core uncovery, because this is the phase of the accident where these pumps would be most influential in delaying core damage until RCS pressure reaches the level for alternate systems to inject (namely, accumulators or low-pressure injection).
	Feed and Bleed Criteria for Transients	The current criteria for feed and bleed during transients do not allow for success if the charging pumps are unavailable [i.e., 1 safety injection (SI) pump and 2 power-operated relief valves (PORVs) is discounted], because the underlying evaluations	Success with 1 SI train and 2 PORVs during a transient could be successful for many cases, and it is possible that alternate thermal-hydraulic assumptions in the underlying assessment could render this a viable success path in this model.

		suggest that success during this situation is very uncertain.	A sensitivity analysis crediting 1 SI train and 2 PORVs during a transient is provided in Section 10.6.
	Crediting of the Broken Loop for Injection during Small LOCAs	The L3PRA project Level 1 model credits the broken loop for injection during small LOCAs, but not medium LOCAs. This assumption is based on experience with other PRA models and assertions about the downcomer behavior.	Though the existing criteria and basis are reasonable, this is an area that can potentially benefit from additional thermal-hydraulic analysis. Alternatively, parametric changes to the success criteria in the PRA model might also be used to demonstrate the importance, or lack thereof, of this assumption.
	SG Feed/Steam Relief Criteria	The success criteria for SG feed/steam relief have been noted to vary across licensee models and are known to be variable depending on the precise conditions in question (e.g., status of intact/broken loops, available steam relief paths, primary-side water level).	The SG success criteria used in the model are thought be reasonable; however, it is acknowledged that there is potential variability and uncertainty associated with these criteria.
Success Criteria (cont.)	Reflux Condensation Modeling	Some of the MAAP and MELCOR calculations that form the basis for some of the success criteria and sequence timing assumptions rely on reflux condensation. That is, there are periods of time during the calculations where the SG tubes are drained, and decay heat removal is either partially or fully accomplished via condensation of steam in the SG tubes that in turn drains back to the loops and reactor pressure vessel. This includes situations where operator-induced, secondary-side depressurization is credited in cooling down and depressurizing the primary side (e.g., safe/stable top events in SBO with AC power recovery or FR-C actions during small/medium LOCAs). MAAP and MELCOR model conservation of mass and energy, but do not have the types of physical models/closure relationships and associated validation needed to model	Additional effort to validate the modeling in this regard could lead to changes in sequence timing and success criteria. The extent to which these changes would affect the model results is not well understood but is thought to be tempered for two reasons. For success criteria, these code results are generally one input to the determination, which also considers other experience and information. For sequence timing, only some human error probabilities (HEPs) are sensitive to the available time.

		interfacial drag and counter-current flow limitations in a highly accurate way. As such, the results from these calculations are uncertain.	
Systems Analysis	24-Hour SSC Mission Times	As discussed in Section 8.3, while safe and stable conditions were considered in the accident sequence analysis, resulting in timelines for some scenarios out to 72 hours, the SSC mission times for reliability/availability estimation were kept at 24 hours.	Using SSC mission times consistent with the longer accident sequence timeline for such sequences will result in higher failure probabilities, thus resulting in a larger CDF. This increase in CDF may be unrealistic given the lack of credit for repair and recovery.
Systems Analysis (cont.)	Battery Depletion Times	There is substantial uncertainty associated with the assumed depletion times for the key batteries credited in the L3PRA project Level 1 model (both the 4-hour depletion time for the safety-related and switchyard batteries and, more significantly, the 2-hour depletion time for the turbine building batteries). Note that load shedding is not explicitly considered in the L3PRA project Level 1 model.	Battery depletion times have a significant effect on LOOP/SBO results. The assumptions on the depletion times for the various batteries used in the L3PRA project Level 1 model are potentially conservative. However, there is currently no information that would justify different battery life assumptions. In the L3PRA project Level 1 model, the uncertainties associated with battery depletion times are increased due to other model assumptions (e.g., not crediting turbine-driven AFW pump operation or AC power recovery after battery depletion). A sensitivity analysis using the safety-related battery depletion time of 4 hours as limiting offsite power recovery during a station blackout is provided in Section 10.7.
	Shutdown Seal Reliability	The RCP shutdown seals currently installed at the reference plant, are not credited in the L3PRA project, since these seals were not installed at the time modeling efforts began.	The contribution to CDF from RCP seal LOCAs (which are a major CDF contributor) could be substantially reduced if the newer shutdown seals were credited. A sensitivity analysis crediting the RCP shutdown seals is provided in Section 10.8.
Systems Analysis (cont.)	Crediting Recovery of Key SSC failures	Recovery for failures of key SSCs—specifically, the reserve auxiliary transformer (RAT) breakers and load sequencers—was not credited in the L3PRA	The lack of recovery credit for failure of the RAT breakers and load sequencers is potentially conservative. A sensitivity analyses

		project Level 1 model because no information was available to justify recovery credit.	crediting repair for these components is provided in Section 10.9. In addition, the manual starting of NSCW fans was not credited following a SI or LOOP signal, consistent with the reference plant PRA. However, a placeholder basic event (1-OA-NSCWFAN---H) is contained in the applicable fault tree logic. The Fussell-Vesely importance measure for this basic event indicates an approximately 2 percent contribution to CDF.
Human Reliability Analysis	HFE Delineation	HFE delineation is the discrimination of those HFEs that are to be modeled and the conditions under which they are characterized. There are hundreds of individual HFEs that could be modeled.	The human reliability analysis (HRA) for the L3PRA project Level 1 model relied heavily on the HRA performed by the reference plant licensee. However, due to different modeling assumptions and event/fault tree structures between the two models, some reference plant model HFEs were not used in the L3PRA project Level 1 model. In addition, some new HFEs were added to the L3PRA project Level 1 model.
Human Reliability Analysis (cont.)	Operator Action Time Windows	Some operator actions involve the same function, but under different scenario conditions that only impact the time available to act. For example, containment spray actuation or the number of running ECCS pumps can affect the RWST depletion rate during LOCA scenarios, which determines the available time.	In some cases, two HFEs that only differed in terms of time available were separately quantified because the event/fault tree logic allowed evaluation of the time differences [e.g., OAR_LPSL-----H (operator fails to establish LPR after depressurization per ES-1.2 - SLOCA, RHR failed, with CCUs available) and OAR_LPSL2----H (operator fails to establish LPR after depressurization per ES-1.2 – SLOCA, CCUs failed)]. In other cases, the same HFE is used (conservatively) to cover multiple scenarios that differ only in terms of time available. It is not believed that these conservative time estimates have a significant effect on the HEPs for HFEs that are not time critical because the Cause-Based Decision Tree (CBDT) method, which is used in these cases, is relatively insensitive to most timing differences (the main exception being if the conservative

			time used eliminated the potential for self-recovery).
	Crew-to-Crew Variability	Crew-to-crew variability was not included as part of the HRA. Aspects include the following: • Overall experience • Experience with event(s) • Staffing level (minimum versus maximum) • Back shift maintenance resources • Crew personalities • Creativity	The L3PRA project Level 1 model HRA does not consider crew-to-crew variability or individual differences.
Human Reliability Analysis (cont.)	Organizational Interfaces	The plant-specific organizational interfaces during an event may be difficult to capture in the HRA and may strongly depend on the personalities involved. Relevant organizations include: • Operations/Maintenance • Staff/Management • Control Room/TSC • Ex-Plant (e.g., Grid Operator)	The organizational culture of the plant and individual differences between crew members is not captured within the L3PRA project Level 1 model HRA.
	Minimum Joint Human Error Probability (HEP) Cutoff	The L3PRA project Level 1 model for internal events does not apply a minimum joint HEP; however, other portions of the L3PRA project do use one (e.g., low power/shutdown) given larger uncertainties expected in these models. The current ASME/ANS PRA standard does not require a minimum joint HEP, but one may be recommended as part of future revisions.	The lack of use of a minimum joint HEP is potentially non-conservative. A sensitivity analyses applying a 10^{-5} minimum joint HEP cutoff is provided in Section 10.10.
	Multi-Unit Events	Multiple units may provide both significant benefit—by the sharing of equipment and personnel—and significant challenges if all units require accident mitigation simultaneously.	This analysis was focused on Unit 1 only. Help or interference by Unit 2 was not considered.
	Evaluation of Stress in	Given the lack of guidance on evaluating stress between HFEs	The assumption of high/moderate stress is potentially conservative. A

	Dependency Evaluation	using the dependency tree from the Electric Power Research Institute (EPRI) HRA Calculator, the dependency evaluation of HFE pairs in the L3PRA Level 1 internal event PRA model used the higher branch for the stress node in the decision tree (i.e., high/moderate stress), without evaluating stress explicitly.	sensitivity analyses removing stress from the dependency evaluation is provided in Section 10.11. Note, after completion of the L3PRA project Level 1 model for internal events, a project decision was made to remove the consideration of stress from the dependency analysis, as documented in the HRA dependency characterization section of the L3PRA project report on the low power and shutdown Level 1 PRA.
Human Reliability Analysis (cont.)	Crew Response Times	Although the aggregated time required for time prior to receiving cue for action (T_{Delay}) plus time required for diagnosis ($T_{1/2}$) could be reasonably estimated, the explicit distinction in these timing estimates was not performed.	The timing estimate for $T_{1/2}$ is presented as a combination of both the time for diagnosis as well as the time from initiating event to cue presentation (T_{Delay}). The simulator, crew, and job performance measure response times are sources of information for crew response times. All sources are not consistent and can be either optimistic or pessimistic.
	Distractions (e.g., Fatigue, Problems Outside of Work, etc.)	The crew work schedule and individual crew member conditions are not generally included as part of the shaping factors of the HRA.	The consideration of these issues is typically beyond the state-of-practice.
	Crew Awareness to Conditions	Training can alter crew awareness. The awareness of the crew to specific accident conditions varies with the training cycle and current industry experiences that are promulgated to the crews.	
	Circadian Clock	Time of day is not generally included in the HRA despite evidence that the most serious crew errors occur between midnight and 6 a.m.	
	Scenario Dependent Recovery and Repair	The accident sequence level of discrimination regarding plant conditions, timing, operator interface, and use of non-safety systems can significantly impact associated uncertainty. The finite nature of the level of delineation collapses the continuum of possible sequences	Except for offsite power recovery (which is supported by extensive data), recovery/repair of failed SSCs is not considered in the model (due to lack of data).

		to a limited set. Repair and recovery of failures is an area of significant judgment in the PRA model. It involves the designation of sufficient time, access, personnel, and guidance to either recovery (manual action) or repair of a failed SSC.	
Human Reliability Analysis (cont.)	Basis for HEPs	HFE identification was generally accepted from the HRA performed by the reference plant licensee (with a few additions and deletions due to modeling differences). The quantification of those HFEs also generally accepted the analysis performed by the reference plant licensee, and therefore, adopted the same uncertainties. In addition, for two HFEs, a minimum HEP of 10^{-4} was assessed based on a simplistic evaluation that significant time was available [i.e., align alternate condensate storage tank (CST) and refueling water storage tank (RWST) refill].	The select set of HFEs that were reanalyzed were done so consistent with the current state-of-practice.
Data Analysis	Consequential LOOP Probabilities	The current consequential LOOP probabilities for transient-type initiating events (OEP-VCF-LP-CLOPT) is taken from NUREG/CR-6890 (NRC, 2005a). Recent reviews indicate that the number of consequential LOOPs has changed due to the recoding of events. An additional decade of operating experience is available to update OEP-VCF-LP-CLOPT and the consequential LOOP probability given a SI actuation (OEP-VCF-LP-CLOPL). See Section 8.2.2 for additional information.	The revision of the consequential LOOP probabilities based on updated operating experience is a candidate for future study.
Data Analysis (cont.)	CCF Modeling of Large Common-Cause Component Groups (CCCGs)	CCF events are rare, and the population of observed events consists mostly of low-order failures. However, the dominant cut sets in the model include high-order failure events. The	The true frequency of high-order CCF events is unknown, but possibly overestimated.

		scaling methodology used to estimate alpha factors for high order groups based on events observed in lower order groups may be state-of-practice, but it is not easily validated for high order CCCGs.	
	CCF Group Identification	CCF groups are limited to identical components in a redundant functional group, even though there may be many identical components in the system, or even distributed across multiple systems.	CCF impact may be greater than estimated using current state-of-practice methodology.
	Sump Plugging Probability	There is limited data to support quantification of the failure probability for sump plugging, which is a high-impact basic event.	Sensitivity studies can be readily made for different (postulated) sump plugging probabilities.
Quantification	Use of Post-Processing Rules to Apply HFE Dependency	In the L3PRA project Level 1 model, new dependent HFEs are substituted in for the associated independent HFEs. These substitutions are implemented via SAPHIRE project event tree post-processing rules.	Because these post-processing rule substitutions occur after truncation, some cut sets with the identified HFE combinations will be truncated prior to the substitutions with the dependent HEPs. Calculations performed revealed that the truncation of the L3PRA project Level 1 model at the 10^{-12} level results in approximately 6×10^{-7} contribution (approximately 1 percent of the internal event CDF) that is "prematurely" truncated.
	Mincut Upper Bound is Conservative	The solution method used by SAPHIRE results in an upper bound on CDF. An alternate method (e.g., binary decision diagram) that gives an exact result is available, but sometimes fails on large models.	The CDF estimate is an upper bound; the true CDF is slightly smaller.

A summary of the results of all sensitivity analyses associated with key modeling uncertainties is provided in Section 10.12.

10.1 MLOCA Initiating Event Frequency

Description. Due to the rarity of occurrence of some initiating events, methods other than standard data collection and statistical methods were sometimes used to estimate the

frequencies of these initiators. One method that was sometimes used is expert elicitation, which has been used to determine the initiating event frequencies for LOCAs (including medium LOCAs). NUREG-1829, "Estimating Loss-of-Coolant Accident (LOCA) Frequencies through the Elicitation Process," provides the MLOCA initiating event frequency (5×10^{-4}/year) used in the L3PRA project. This NUREG notes that there are significant uncertainties associated with the frequencies (including MLOCA) provided in the report. Note that this frequency was more than an order-of-magnitude higher than the value provided in NUREG/CR-5750, "Rates of Initiating Events at U.S. Nuclear Power Plants: 1987–1995," (NRC, 1999a). Given the large uncertainties and differences between the results of these two diverse methods, a sensitivity analysis was performed using the NUREG/CR-5750 initiating event frequency of 4×10^{-5}/year for MLOCAs for pressurized-water reactors.

Sensitivity Case. For this sensitivity case, the MLOCA initiating event frequency was modified to 4×10^{-5}/year.

Results. This sensitivity analysis resulted in a decrease in the overall internal event CDF from 6.39×10^{-5}/RCY to 6.17×10^{-5}/RCY (an approximate 3 percent decrease). This decrease was due to the CDF for MLOCA decreasing from 2.34×10^{-6}/year to 1.81×10^{-7}/year.

10.2 Grid-Related LOOP Initiating Event Frequency

Description. The L3PRA Level 1 internal event PRA model used an industry-average grid-related LOOP initiating event frequency that included grid-related LOOP events that have occurred at commercial nuclear power plants across the U.S. during the 1997–2010 period. However, the southeastern U.S. had not had any grid-related LOOP events, which leads to a concern that the industry-average value may be conservative for nuclear power plants in this region. In addition, statisticians at Idaho National Laboratory have expressed concerns that the plant-based counting of grid-LOOP events and reactor-critical years neglects the dependency between counted events that occur when more than one plant observes the same grid event. Addressing this second issue required the use of a denominator in the rate estimate that was limited to observed grid-years, which was a small number compared to the reactor-critical years used in the industry-average estimate.

Sensitivity Case. This sensitivity case represents an attempt to address both concerns using the methodology provided in "The theory and quantification of common cause shock events for redundant standby systems," Jussi K. Vaurio, Reliability Engineering and System Safety, 43, (1994) 289–305.

The Vaurio paper provides a methodology for estimating event rates when a given event may affect multiple devices, in this case, nuclear plant sites. The following assumptions were used in this implementation using the available data provided in Table 10-2:

- When a grid-related LOOP event occurs, it affects all units at an affected plant site.
- While grid-related LOOP events have only been observed to affect up to six sites (2003 North East Blackout), the potential exists that a grid event could affect all sites in a region.
- The South East region has not experienced any grid events in the past 20 years; however, if one should occur, the conditional probabilities that multiple sites will be

affected are the same as for the North East region (with consideration given to the different number of sites in the two regions).

- There are 23 sites in the North East region that could be affected by a single grid event.
- There are 21 sites in the South East region that could be affected by a single grid event.

Table 10-2 Grid-related LOOP events that occurred in the US in the past 20 years

Date	Plant	Region
8/14/2003	Ginna	North East
	Nine Mile Point 1	
	Nine Mile Point 2	
	Indian Point 2	
	Indian Point 3	
	Fitzpatrick	
	Fermi	
	Perry	
9/15/2003	Peach Bottom 2	North East
	Peach Bottom 3	
6/14/2004	Palo Verde 1	South West
	Palo Verde 2	
	Palo Verde 3	
7/12/2009	Oyster Creek	North East
7/23/2012	Oyster Creek	North East
10/14/2013	Pilgrim	North East
4/7/2015	Calvert Cliffs 1	North East

Date	Plant	Region
	Calvert Cliffs 2	

Vaurio provides the following definitions as adapted for this estimate:

$\boldsymbol{\Lambda_{k/n}}$ is the rate of events failing the grid supply to exactly k sites on a grid with n sites.

$\boldsymbol{\lambda_{k/n}}$ is the rate of events failing the grid supply to a specific set of k sites on a grid with n sites.

Then

$$\boldsymbol{\Lambda_{k/n} = \binom{n}{k} \lambda_{k/n}}$$

and

$$\boldsymbol{\lambda_n = \sum_{i=1}^{n} \binom{n-1}{i-1} \lambda_{i/n}}$$

where $\boldsymbol{\lambda_n}$ is the total rate (grid events per site-year) of grid events affecting a specific site on a grid with n sites. This last quantity is the grid LOOP initiating event rate at a specific site.

In Section 3.5 of his paper, Vaurio provides estimators and uncertainty distributions for $\boldsymbol{\Lambda_{k/n}}$ and $\boldsymbol{\lambda_{k/n}}$ in terms of the event counts accumulated for some observation time T. He defines the event counts, $\boldsymbol{N_{i/n}}$, as the sum of events affecting i sites on a grid with n sites. He then provides the estimator for $\boldsymbol{\Lambda_{k/n}}$ as:

$$\boldsymbol{\bar{\Lambda}_{i/n} = \frac{N_{i/n} + 1/2}{T}}$$

and

$$\boldsymbol{\bar{\lambda}_{i/n} = \frac{\bar{\Lambda}_{i/n}}{\binom{n}{i}}}$$

The above definition of $\boldsymbol{\Lambda_{k/n}}$ leads to excessive conservatism when there are many sites in the region, so an alternative formulation was used in this implementation. In this estimate, the 1/2 term was changed to 0.5/n, which had the effect of making the overall estimate of the frequency of grid events in the region equivalent to what would be obtained using a Jeffrey's noninformative prior.

Vaurio provides for the definition of common-cause failure alpha factors using:

$$\boldsymbol{\Lambda_n = \sum_{i=1}^{n} \Lambda_{i/n} = \sum_{i=1}^{n} \binom{n}{i} \lambda_{i/n}}$$

and

$$\alpha_{k/n} = \frac{\Lambda_{k/n}}{\Lambda_n} \ .$$

In this calculation, the alpha factors characterizing the conditional probabilities of grid events in the North East region were estimated, mapped, and then applied to the observed South East region event rate to provide the event rate for a plant site in the South East region. Vaurio provided the mapping method in Section 5.1 of the referenced paper. Once the alpha factors for the North East region were estimated and mapped, the following relations were used to get the South East region grid-related LOOP frequency:

$$\lambda_n = \mu \sum_{k=1}^{n} \left(\frac{k}{n}\right) \alpha_{k/n} = \mu \left(\frac{\alpha_T}{n}\right)$$

Where μ is the observed grid event rate for the South East region defined by

$$\mu = \frac{N + 1/2}{T_c}$$

The above calculations are demonstrated on the following pages. The result for a plant site in the South East region is 3.05×10^{-3} grid LOOP events per site-year.

Results. The sensitivity analysis with the different grid-related LOOP initiating event frequency resulted in a decrease in the overall internal events CDF from 6.39×10^{-5}/RCY to 5.01×10^{-5}/RCY (an approximate 22 percent decrease). This decrease was due to the CDF for grid-related LOOPs decreasing from 1.83×10^{-5}/RCY to 4.54×10^{-6}/RCY.

Table 10-3 Grid-related LOOP events that occurred in the US in the past 20 years - Calculations for North East grid LOOP rate

Data Summary			
Grid Years (T) = 20	Sites (n) = 23	Total Events = 6	Grid Rate (μ) = 0.325

Event Count	Sites Affected per Event (k)	Prior	Est. $\Lambda_{k/n}$	Est. $\lambda_{k/n}$	Est. α_k	λ_n
5	1	2.17E-02	2.51E-01	1.09E-02	7.73E-01	1.09E-02
0	2	2.17E-02	1.09E-03	4.30E-06	3.34E-03	1.10E-02
0	3	2.17E-02	1.09E-03	6.14E-07	3.34E-03	1.12E-02
0	4	2.17E-02	1.09E-03	1.23E-07	3.34E-03	1.13E-02
0	5	2.17E-02	1.09E-03	3.23E-08	3.34E-03	1.16E-02
1	6	2.17E-02	5.11E-02	5.06E-07	1.57E-01	2.49E-02
0	7	2.17E-02	1.09E-03	4.43E-09	3.34E-03	2.52E-02
0	8	2.17E-02	1.09E-03	2.22E-09	3.34E-03	2.56E-02
0	9	2.17E-02	1.09E-03	1.33E-09	3.34E-03	2.60E-02
0	10	2.17E-02	1.09E-03	9.50E-10	3.34E-03	2.65E-02
0	11	2.17E-02	1.09E-03	8.04E-10	3.34E-03	2.70E-02
0	12	2.17E-02	1.09E-03	8.04E-10	3.34E-03	2.76E-02
0	13	2.17E-02	1.09E-03	9.50E-10	3.34E-03	2.82E-02
0	14	2.17E-02	1.09E-03	1.33E-09	3.34E-03	2.89E-02
0	15	2.17E-02	1.09E-03	2.22E-09	3.34E-03	2.96E-02

0	16	2.17E-02	1.09E-03	4.43E-09	3.34E-03	3.03E-02
0	17	2.17E-02	1.09E-03	1.08E-08	3.34E-03	3.11E-02
0	18	2.17E-02	1.09E-03	3.23E-08	3.34E-03	3.20E-02
0	19	2.17E-02	1.09E-03	1.23E-07	3.34E-03	3.29E-02
0	20	2.17E-02	1.09E-03	6.14E-07	3.34E-03	3.38E-02
0	21	2.17E-02	1.09E-03	4.30E-06	3.34E-03	3.48E-02
0	22	2.17E-02	1.09E-03	4.73E-05	3.34E-03	3.59E-02
0	23	2.17E-02	1.09E-03	1.09E-03	3.34E-03	3.70E-02
			3.25E-01			3.70E-02

Table 10-4 Scaled Alpha Factors from a Common Cause Group Size (i.e., number of plants per grid) of 23 (North East) to 21 (South East)

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	Scaled	Normalized
1	9.1E-01	1.7E-01	1.2E-02																					7.1E-01	7.6E-01
2		8.3E-01	2.4E-01	2.4E-02																				3.6E-03	3.9E-03
3			7.5E-01	3.0E-01	4.0E-02																			3.6E-03	3.9E-03
4				6.8E-01	3.6E-01	5.9E-02																		1.3E-02	1.4E-02
5					6.0E-01	4.0E-01	8.3E-02																	6.6E-02	7.0E-02
6						5.4E-01	4.4E-01	1.1E-01																8.6E-02	9.3E-02
7							4.7E-01	4.7E-01	1.4E-01															3.6E-03	3.9E-03

8								4.2 E-01	5.0 E-01	1.8 E-01														3.6E-03	3.9E-03
9									3.6 E-01	5.1 E-01	2.2 E-01													3.6E-03	3.9E-03
10										3.1 E-01	5.2 E-01	2.6 E-01												3.6E-03	3.9E-03
11											2.6 E-01	5.2 E-01	3.1 E-01											3.6E-03	3.9E-03
12												2.2 E-01	5.1 E-01	3.6 E-01										3.6E-03	3.9E-03
13													1.8 E-01	5.0 E-01	4.2 E-01									3.6E-03	3.9E-03
14														1.4 E-01	4.7 E-01	4.7 E-01								3.6E-03	3.9E-03
15															1.1 E-01	4.4 E-01	5.4 E-01							3.6E-03	3.9E-03

16																8.3E-02	4.0E-01	6.0E-01				3.6E-03	3.9E-03
17																	5.9E-02	3.6E-01	6.8E-01			3.6E-03	3.9E-03
18																		4.0E-02	3.0E-01	7.5E-01		3.6E-03	3.9E-03
19																			2.4E-02	2.4E-01	8.3E-01	3.6E-03	3.9E-03
20																				1.2E-02	1.7E-01	9.1E-01	3.6E-03	3.9E-03
21																					4.0E-03	8.7E-02	1.0	3.6E-03	3.9E-03
																								9.3E-01	1.0E+00

α_k =	7.7E-01	3.3E-03	3.3E-03	3.3E-03	3.3E-03	1.6E-01	3.3E-03	3.3E-03	3.3E-03	3.3E-03	3.3E-03	3.3E-03	3.3E-03	3.3E-03	3.3E-03	3.3E-03	3.3E-03	3.3E-03	3.3E-03	3.3E-03	3.3E-03	3.3E-03	3.3E-03

Table 10-5 Grid-related LOOP events that occurred in the US in the past 20 years – Calculations for South East Grid LOOP Rate

Data Summary					
Grid Years (T) =	20	Sites (n) =	21	Total Events =	0	Grid Rate (μ) =	2.5E-02

Use scaled alpha factors

from North East estimate

Event Count	Sites Affected per Event (k)	Prior	Est. $\Lambda_{k/n}$	Est. $\lambda_{k/n}$	Est. α_k	λ_n	α_k (from NE est.)	$k\alpha_k$
0	1	2.38E-02	1.19E-03	5.67E-05	4.76E-02	5.67E-05	7.57E-01	7.57E-01
0	2	2.38E-02	1.19E-03	5.67E-06	4.76E-02	1.70E-04	3.91E-03	7.82E-03
0	3	2.38E-02	1.19E-03	8.95E-07	4.76E-02	3.40E-04	3.91E-03	1.17E-02
0	4	2.38E-02	1.19E-03	1.99E-07	4.76E-02	5.67E-04	1.37E-02	5.48E-02
0	5	2.38E-02	1.19E-03	5.85E-08	4.76E-02	8.50E-04	7.04E-02	3.52E-01
0	6	2.38E-02	1.19E-03	2.19E-08	4.76E-02	1.19E-03	9.26E-02	5.55E-01
0	7	2.38E-02	1.19E-03	1.02E-08	4.76E-02	1.59E-03	3.91E-03	2.74E-02
0	8	2.38E-02	1.19E-03	5.85E-09	4.76E-02	2.04E-03	3.91E-03	3.13E-02

0	9	2.38E-02	1.19E-03	4.05E-09	4.76E-02	2.55E-03	3.91E-03	3.52E-02
0	10	2.38E-02	1.19E-03	3.38E-09	4.76E-02	3.12E-03	3.91E-03	3.91E-02
0	11	2.38E-02	1.19E-03	3.38E-09	4.76E-02	3.74E-03	3.91E-03	4.30E-02
0	12	2.38E-02	1.19E-03	4.05E-09	4.76E-02	4.42E-03	3.91E-03	4.69E-02
0	13	2.38E-02	1.19E-03	5.85E-09	4.76E-02	5.16E-03	3.91E-03	5.08E-02
0	14	2.38E-02	1.19E-03	1.02E-08	4.76E-02	5.95E-03	3.91E-03	5.48E-02
0	15	2.38E-02	1.19E-03	2.19E-08	4.76E-02	6.80E-03	3.91E-03	5.87E-02
0	16	2.38E-02	1.19E-03	5.85E-08	4.76E-02	7.71E-03	3.91E-03	6.26E-02
0	17	2.38E-02	1.19E-03	1.99E-07	4.76E-02	8.67E-03	3.91E-03	6.65E-02
0	18	2.38E-02	1.19E-03	8.95E-07	4.76E-02	9.69E-03	3.91E-03	7.04E-02
0	19	2.38E-02	1.19E-03	5.67E-06	4.76E-02	1.08E-02	3.91E-03	7.43E-02
0	20	2.38E-02	1.19E-03	5.67E-05	4.76E-02	1.19E-02	3.91E-03	7.82E-02
0	21	2.38E-02	1.19E-03	1.19E-03	4.76E-02	1.31E-02	3.91E-03	8.21E-02
		μ =	2.50E-02		λ_{21} =	1.31E-02	α_T =	2.56

Result with SE alphas

λ_{21} = 3.05E-3

Result with scaled alpha factors

10.3 Credit for Blind Turbine-Driven AFW Pump Operation

Description. The L3PRA Level 1 PRA model for internal events did not credit continued turbine-driven AFW pump operation after all safety-related DC power was lost. No credit was provided because with no steam generator (SG) water level indication, the potential of operators to either over- or under-fill the SGs (during the PRA mission time of 24 hours) was high. See Section 8.1.2 for additional information.

Sensitivity Case. To credit continued turbine-driven AFW pump operation after battery depletion, a new top event (1-BLINDAFW) was added to the SBO event tree after the 1-OPR top event. There was only a single branch point in which continued turbine-driven AFW pump operation could bring the plant to safe/stable end state. Specifically, this operation was credited when initial turbine-driven AFW pump operation was successful, the pressurizer PORVs successfully reclosed (if opened), and RCP seals did not fail (i.e., elevated leakage was limited to 21 gallons per minute (gpm) per RCP). In other scenarios, core uncovery occurred unless offsite power was recovered and either AFW was initiated (for scenarios in which AFW fails initially) or RCS makeup can be initiated (LOCAs caused by RCP seal failures or stuck-open PORV). See Figure 10-1 for the revised SBO event tree used in this sensitivity analysis.

The 1-BLINDAFW fault tree was composed of two basic events, 1-OA-OFC_2-----H (*operator fails to continue TDAFWP after bat depletion - SBO*) and 1-CAD-XHE-SAFESTABLE-2 (*additional operator actions to reach safe/stable end state*). The first basic event, 1-OA-OFC_2-----H, was assigned an HEP of 0.3 in an earlier version of the L3PRA Level 1 PRA model for internal events (though, as stated above, this action is no longer credited in the current version of the Level 1 internal event model).[236] The second basic event, 1-CAD-XHE-SAFESTABLE-2 was a simplified representation of the other requirements needed to reach a safe/stable end state given elevated RCP seal leakage (21 gpm per RCP). These other requirements included depressurization of the RCS using the SG atmospheric relief valves (ARVs), which will allow the accumulators to provided RCS inventory makeup.[237] In addition, operators must provide makeup to the condensate storage tank (CST) to allow continued decay heat removal via the SGs. Given a LOOP and subsequent SBO, additional inventory for AFW will not be available after battery depletion.[238] Therefore, an alternate strategy for providing makeup to the CST (e.g., use of the portable pump to transfer water from the firewater storage tank) would need to be used.

Given the large uncertainties associated with both basic events, 1-OA-OFC_2-----H and 1-CAD-XHE-SAFESTABLE-2, three sensitivity cases were run. Case A assumes the HEP for both events is 0.3, while Cases B and C assume the HEP for both events is 0.1 and 0.03, respectively.

---

[236] While not credited in the current Level 1 PRA model for internal events, the action to continue turbine-driven AFW pump operation after battery depletion is credited in the current Level 2 PRA model for internal events.

[237] ECA 0.0, "Loss of All AC Power," directs an operator to be dispatched to prepare for local operation of SG ARVs. The capability of operators to locally open the SG ARVs was not explicitly modeled in the Level 1 internal event model. This operator action was expected to be dominated by the HEP (i.e., hardware failures were not expected to have a significant impact on the potential failure of this operator action).

[238] Typically, the normally aligned CST was automatically refilled from the demineralizer water system. If automatic makeup was unavailable, operators were procedurally directed to align the alternate CST to provide additional inventory for continued AFW operation. However, both methods were rendered unavailable during an SBO after depletion of the safety-related batteries.

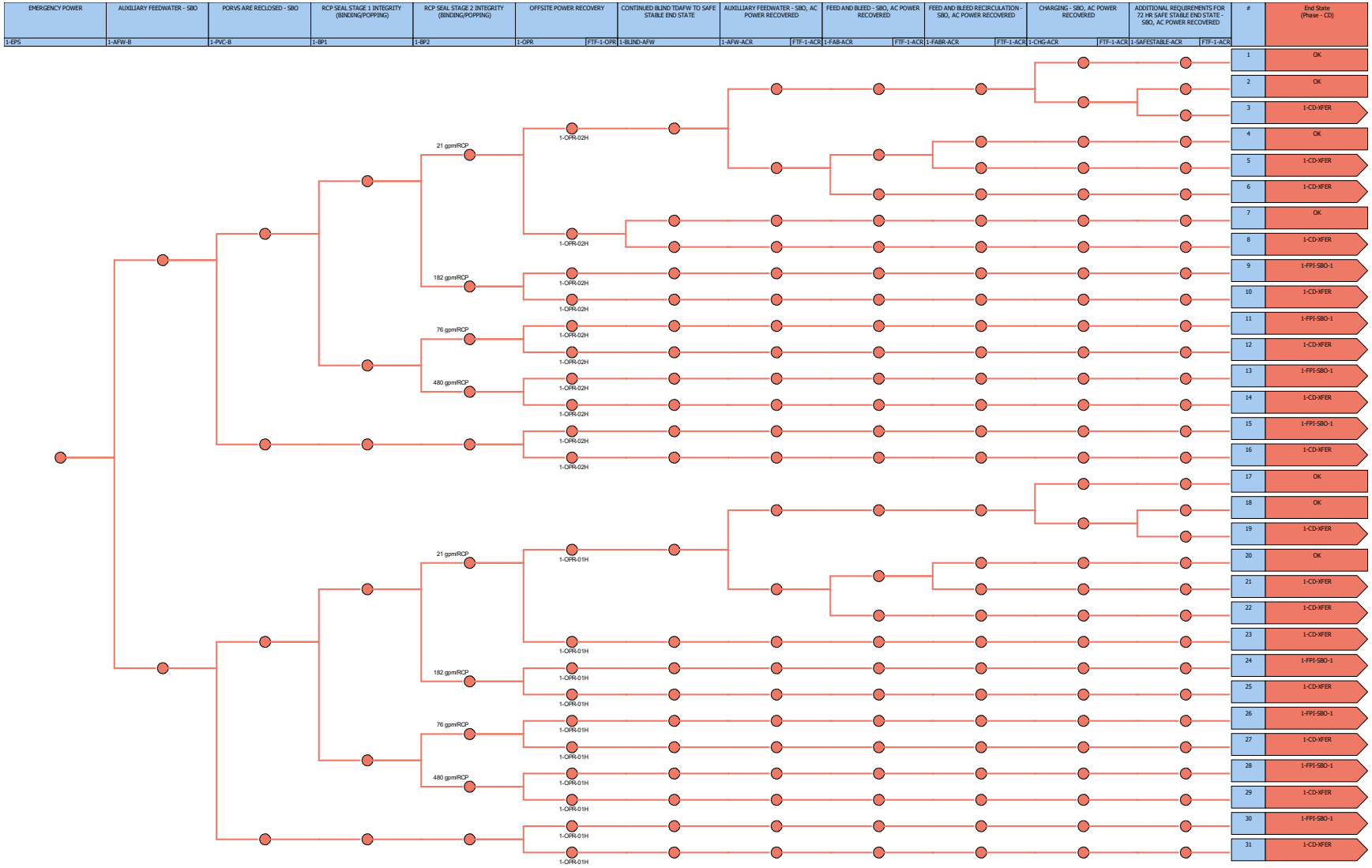


Figure 10-1 Revised SBO Event Tree for Crediting Continued Turbine-Driven AFW Pump Operation

Results and Insights. This sensitivity analysis resulted in the following changes to the CDF contribution:

Table 10-6 Sensitivity Analysis Results for Credit for Blind Turbine Driven AFW Pump Operation

Name	Base CDF (per RCY)	Sensitivity Case A CDF (per RCY)	Sensitivity Case B CDF (per RCY)	Sensitivity Case C CDF (per RCY)
Grid-Related LOOP	1.83E-5	1.60E-5	1.03E-5	8.35E-6
Switchyard-Centered LOOP	1.04E-5	9.37E-6	6.48E-6	5.47E-6
Weather-Related LOOP	9.02E-6	7.69E-6	4.66E-6	3.60E-6
Plant-Centered LOOP	1.91E-6	1.73E-6	1.20E-6	1.01E-6
LOOP Total	3.96E-5	3.48E-5	2.27E-5	1.84E-5
Internal Events Total	6.39E-5	5.91E-5	4.69E-5	4.27E-5

10.4 Restoring Offsite Power without DC Power

Description. As discussed for Sensitivity Case 3, the L3PRA Level 1 PRA model for internal events assumed DC power was required to recover offsite power and, therefore, offsite power must be recovered before the limiting batteries were depleted. In some PRAs, offsite power recovery is based on time until core damage. If this time is greater than the lifetime of the limiting batteries, then the implication is that offsite power can be recovered in the absence of DC power. Note, these scenarios may also require the operation of turbine-driven AFW after the safety-related batteries are depleted (which was also not credited in the L3PRA Level 1 PRA model for internal evens).

Sensitivity Case. The L3PRA Level 1 PRA model for internal events was modified to allow offsite power recovery up until the occurrence of core damage. For some scenarios with longer time frames, this also assumed that turbine-driven AFW continued to run after the safety-related batteries were depleted. For this sensitivity analysis, three new offsite power recovery fault trees, 1-OPR-4H (*offsite power recovery in 4 hours*), 1-OPR-8H (*offsite power recovery in 8 hours*), and 1-OPR-10H (*offsite power recovery in 10 hours*), were created. These fault trees were based on the 1-OPR-2H (*offsite power recovery in 2 hours*) fault tree, with a few modifications. First, the offsite power recovery basic events were changed from 2 hours (e.g., 1-OEP-XHE-XL-NR02HGR) to 4 hours (e.g., 1-OEP-XHE-XL-NR04HGR), 8 hours (1-OEP-

XHE-XL-NR08HGR), and 10 hours (1-OEP-XHE-XL-NR10HGR), respectively. Second, the basic event associated with alignment of the alternate switchyard was changed from 2 hours (1-OA-ALIGNPW-02HR) to 4 hours (e.g., 1-OA-ALIGNPW-02HR), 8 hours (1-OA-ALIGNPW-08HR), and 10 hours (1-OA-ALIGNPW-10HR), respectively. In addition to these fault tree changes, the SBO event tree required some modifications to the substitutions for the OPR (*offsite power recovery*) fault tree. Specifically, the substitutions for the upper branches that result from successful AFW and successful reclosing of the pressurizer PORV(s) for the 182, 76, and 21 gpm per RCP seal leakage rates were changed from 2 hours (1-OPR-2H) to 4 hours (1-OPR-4H), 8 hours (1-OPR-8H), and 10 hours (1-OPR-10H), respectively. The remaining branches (e.g., failed AFW, stuck-open PORV) were kept at their base model offsite power recovery options because these sequence times were based on times to core uncovery. The revised SBO event treed used in this sensitivity analysis is shown in Figure 10-2.

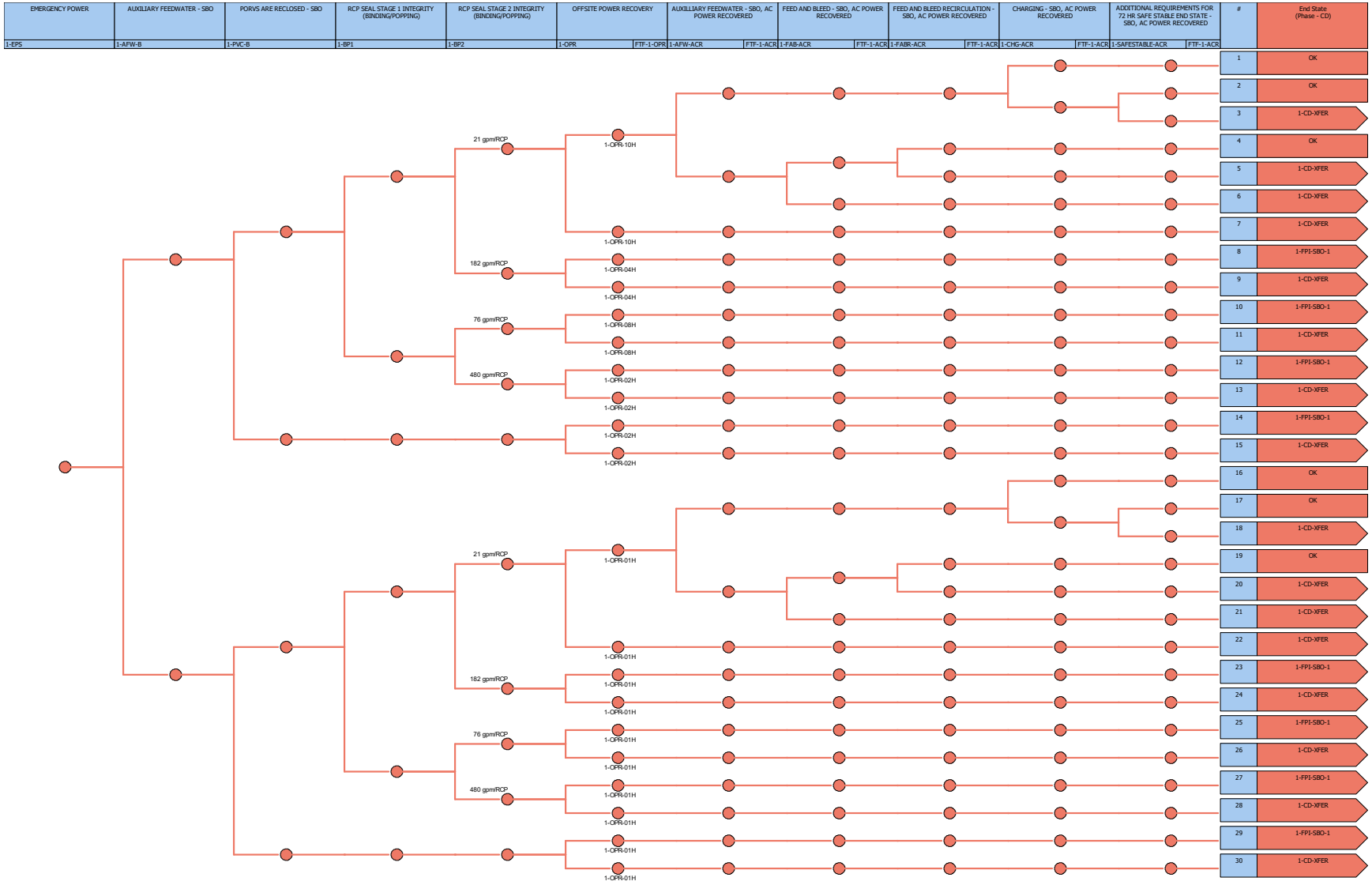


Figure 10-2 Revised SBO Event Tree for Crediting Restoration of Offsite Power without DC Power

Results and Insights. This sensitivity analysis resulted in the following changes to the CDF contribution:

Table 10-7 Sensitivity Analysis Results for Restoring Offsite Power without DC Power

Name	Base CDF (per RCY)	Sensitivity CDF (per RCY)
Grid-Related LOOP	1.83E-5	1.37E-5
Switchyard-Centered LOOP	1.04E-5	1.03E-5
Weather-Related LOOP	9.02E-6	8.00E-6
Plant-Centered LOOP	1.91E-6	1.90E-6
LOOP Total	3.96E-5	3.39E-5
Internal Events Total	6.39E-5	5.82E-5

Similarly to Sensitivity Case 3, the decrease in LOOP CDF was limited due to the influence of non-recoverable failures (e.g., RAT breakers, sequencers).

10.5 Modeling 24-Hour Safe/Stable End State

Description. The American Society of Mechanical Engineers/American Nuclear Society (ASME/ANS) PRA standard defines a safe/stable state as "a plant condition, following an initiating event, in which RCS conditions are controllable at or near desired values." Supporting requirement AS-A2 states, "for each modeled initiating event, identify the key safety functions that are necessary to reach a safe, stable state and prevent core damage." Supporting requirement SC-A5 elaborates by stating that (for capability category II/III) additional evaluations must be performed for sequences where stable plant conditions are not achieved at 24 hours. Only in the definition of "success path" does the standard provide a later back-stop time (72 hours), and the success path concept is only invoked in the seismic margins assessment.

In the L3PRA project Level 1 internal event PRA model, for event tree sequences that were safe (i.e., no core damage), but not stable, at 24 hours (i.e., they would result in core damage at some point after 24 hours), the model generally extended the accident sequence to 72 hours. If core damage would occur before 72 hours, additional mitigation actions (e.g., CST refill, alternate charging alignment, or FR-C.1, "Response to Inadequate Core Cooling" manual depressurization of the SGs) were queried or the sequences were modeled as core damage sequences. If core damage does not occur before 72 hours, these sequences were modeled as "OK," even though they were not "stable." It was reasoned that a 72-hour window, since the onset of the plant upset condition, allows sufficient time that some unmodeled action using onsite or offsite resources can be taken to prevent core damage. See Section 8.3 for additional information. It is believed that the current state-of-practice for internal event PRA modeling

typically uses a 24-hour safe/stable end state, with model developers ensuring sequences would not result in core damage soon (e.g., several hours) after this.

Sensitivity Case. To evaluate the L3PRA Level 1 internal event PRA model with a 24-hour safe/stable end state, the 1-CHG and 1-CHG-ACR events (associated with the 1-CHG and 1-CHG-ACR fault trees) were modified. Specifically, the process flag for both events was changed to Y-FAILURE => DEVELOPED EVENT | SUCCESS => /DEVELOPED EVENT and their failure probability was set to FALSE. These changes eliminate the accident sequences and cut sets from requiring charging or other mitigation after 24 hours.

Results. This sensitivity analysis resulted in a decrease in the overall internal event CDF from 6.39×10^{-5}/RCY to 6.33×10^{-5}/RCY (less than a 1 percent decrease). Most of this decrease was associated with the elimination of the two significant sequences associated with the loss of safety-related 4.16 kV buses, LO4160VA 07-1 and LO4160VA 07-1 (see Table 9-2).

10.6 Credit for SI Pumps for Feed and Bleed Cooling during Transients

Description. Thermal-hydraulic calculations using MELCOR for Byron (a plant like the reference plant) indicated that successful prevention of core damage was marginal for non-LOCAs using 1 of 2 SI pumps and 2 of 2 PORVs for feed and bleed. Other studies, EPRI 1023032, "Technical Framework for Management of Safety Margins—Loss of Main Feedwater Pilot Application," and NUREG/CR-7177, "Compendium of Analyses to Investigate Select Level 1 Probabilistic Risk Assessment End-State Definition and Success Criteria Modeling Issues," indicated that there are conditions under which the use of SI pump(s) and both PORVs for feed and bleed cooling will not prevent core damage. Given these uncertainties, the L3PRA Level 1 internal event PRA model only credited 1 of 2 centrifugal charging pumps (CCPs) with 1 of 2 PORVs for feed and bleed cooling during transients. For LOCAs, the L3PRA Level 1 internal event PRA model also applied the success criterion of 1 of 2 SI pumps (in addition to the 1 of 2 CCPs) and 2 of 2 PORVs for feed and bleed.

Sensitivity Case. To include the success criterion of 1 of 2 SI pumps and 2 of 2 PORVs (in addition to 1 of 2 CCPs and 1 of 2 PORVs) for feed and bleed during transients in the L3PRA Level 1 internal event PRA model, the FAB (*feed and bleed*) fault tree was modified. Specifically, the logic associated with the 1 of 2 SI pumps and 2 of 2 PORVs contained in the FAB (*feed and bleed – small LOCA*) was reproduced in the FAB fault tree. The logic from gate 1-FAB-SLOCA-04 was copied and pasted in the FAB fault tree under new AND gate 1-FAB-01-B. Gate 1-FAB-01-B was inserted under the existing top gate in the FAB fault tree. The revised FAB fault tree is provided in Figure 10-3.

Results. This sensitivity analysis resulted in a decrease in the overall internal event CDF from 6.389×10^{-5}/RCY to 6.388×10^{-5}/RCY (a negligible decrease).

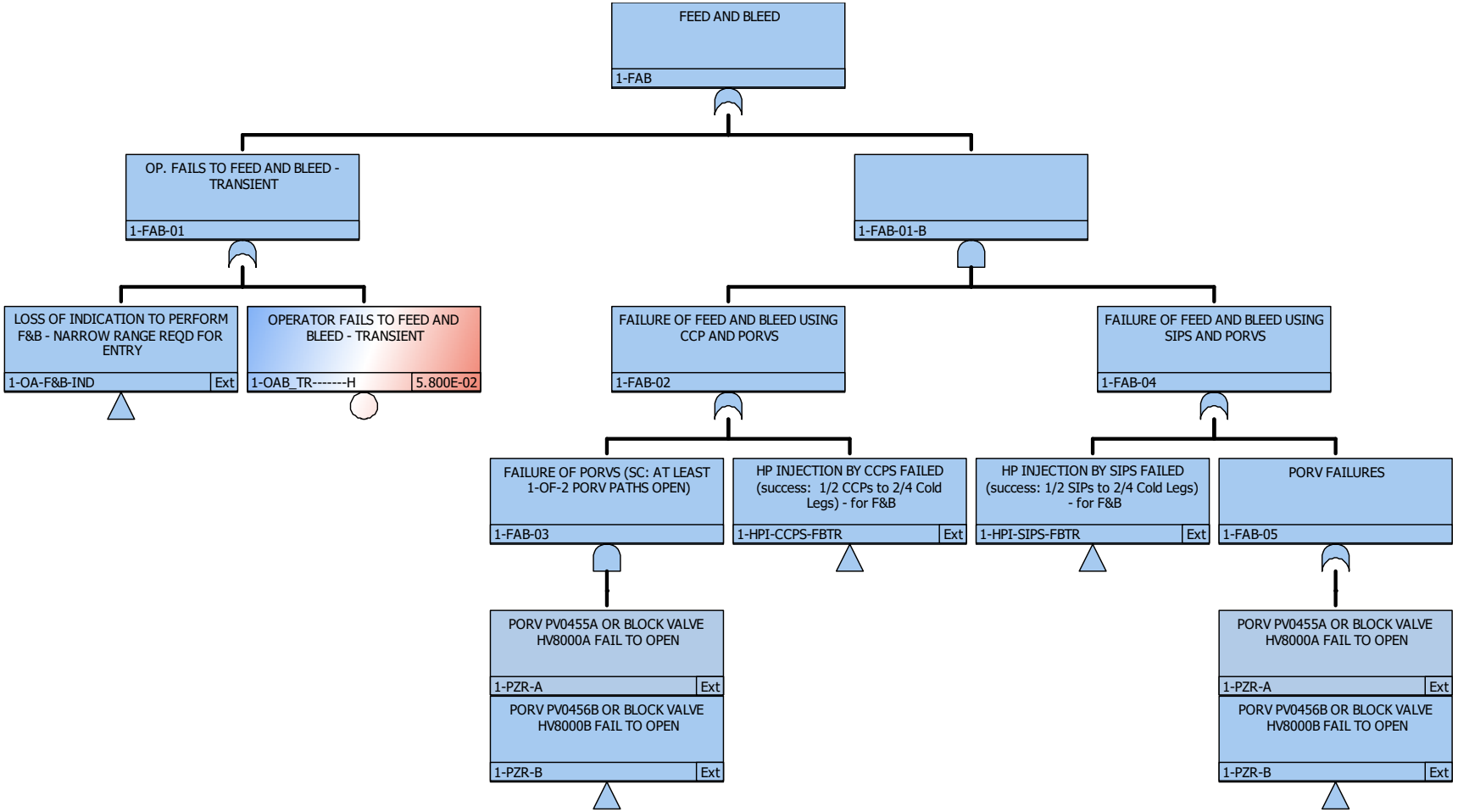


Figure 10-3 Revised FAB Fault Tree

10.7 Limiting Batteries for Offsite Power Recovery during SBO

Description. The L3PRA Level 1 PRA model for internal events assumes that DC power is required to manipulate the applicable breaker(s) to restore offsite power to the safety-related AC buses during an SBO. During a LOOP initiating event and subsequent SBO, DC power is provided by the plant batteries. The L3PRA Level 1 PRA model has three different sets of batteries: (1) the safety-related batteries (4-hour battery life) that supply DC power to the breakers/switchers downstream of the reserve auxiliary transformers (RATs); (2) the turbine building batteries (2-hour battery life) that supply DC power to circuit switchers directly upstream of the RATs; and (3) the switchyard batteries (4-hour battery life) that supply DC control power to the circuit breakers that are located in the high-voltage switchyard (immediately downstream of 230kV buses 1 and 2). The SBO procedure (ECA-0.0) provides direction for shedding unnecessary DC loads on the safety-related batteries; however, there are no procedural actions to prolong the life of the turbine building batteries. Therefore, the turbine building batteries were assumed to have the limiting depletion time for realigning offsite power to the safety-related 4.16 kV AC buses in the L3PRA Level 1 internal event PRA model. This modeling was potentially conservative because the turbine building batteries may have longer depletion times due to decreased loads during an SBO.

Sensitivity Case. Typically, DC power limitations during SBO scenarios are based on the depletion times of the safety-related batteries. For this sensitivity analysis, a new offsite power recovery fault tree, 1-OPR-4H (*offsite power recovery in 4 hours*), was created. The fault tree was based on the 1-OPR-2H (*offsite power recovery in 2 hours*) fault tree, with a few modifications. First, the offsite power recovery basic events were changed from 2 hours (e.g., 1-OEP-XHE-XL-NR02HGR) to 4 hours (e.g., 1-OEP-XHE-XL-NR04HGR). Second, the basic event associated with alignment of alternate switchyard was changed from 2 hours (1-OA-ALIGNPW-02HR) to 4 hours (1-OA-ALIGNPW-04HR). In addition to these fault tree changes, the SBO event tree required some modifications to the substitutions for the OPR (*offsite power recovery*) fault tree. Specifically, the substitutions for the upper branches that result from successful AFW and successful reclosing of the pressurizer PORV(s) for the 21, 76, and 182 gpm per RCP seal leakage rates were changed from 2 hours (1-OPR-2H) to 4 hours (1-OPR-4H). The remaining branches (e.g., failed AFW, stuck-open PORV) were kept at their base model offsite power recovery options because these sequence times were based on times to core uncovery. The revised SBO event tree used in this sensitivity analysis is shown in Figure 10-4.

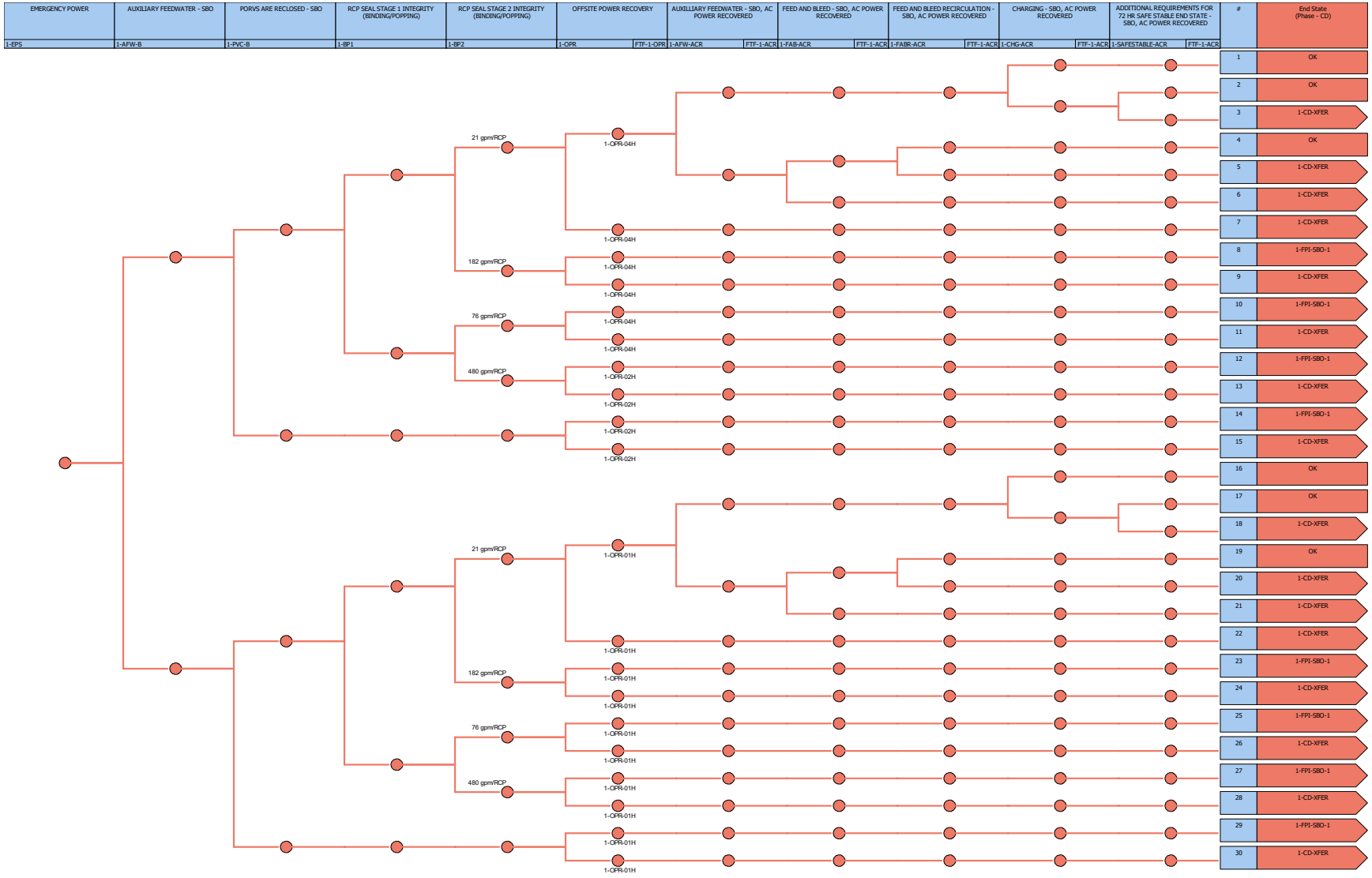


Figure 10-4 Revised SBO Event Tree for Crediting 4-Hour Battery Life during SBO Scenarios

Results and Insights. This sensitivity analysis resulted in the following changes to the CDF contribution:

Table 10-7 Sensitivity Analysis Results for Limiting Batteries for Offsite Power Recovery during SBO

Name	Base CDF (per RCY)	Sensitivity CDF (per RCY)
Grid-Related LOOP	1.83E-5	1.53E-5
Switchyard-Centered LOOP	1.04E-5	1.03E-5
Weather-Related LOOP	9.02E-6	8.25E-6
Plant-Centered LOOP	1.91E-6	1.91E-6
LOOP Total	3.96E-5	3.58E-5
Internal Events Total	6.39E-5	6.00E-5

This decrease in the LOOP CDF was limited because of the following factors:

- For all LOOP types, the dominant SBO contributors were due to failures that preclude offsite power recovery (e.g., failure of RAT breakers and load sequencers).
- For weather-related LOOPs, an additional 2 hours available for offsite power recovery resulted in a relatively small decrease in the non-recovery probability (0.56 decreased to 0.42).
- For switchyard- and plant-centered LOOPs, the scenarios that include potential for offsite power recovery were already (relatively) low because the alignment of the alternate switchyard were also credited for these LOOP types.

10.8 Crediting Improved RCP Shutdown Seals

Description. To assess the impact on risk from improvements in RCP Shutdown seals, a sensitivity study was done based on low leakage RCP seals (Westinghouse SHIELD® Passive Shutdown Seal). For these seals, RCP seal leakage was assumed to be 1 gpm per RCP after seal actuation. The inclusion of these seals can have a significant effect on the model results.

Sensitivity Case. To evaluate the effect of the RCP shutdown RCP seals on the L3PRA Level 1 PRA internal event model results, basic event 1-RCS-SDS-FC-ACTUATE (*shutdown seals fail*

to actuate), which is set to TRUE in the base L3PRA model, was assigned a failure probability.[239] This basic event is located in the 1-SDS (*shutdown seal actuation*), 1-RCPSC (*RCP seal cooling/integrity*), 1-RCPSC-BP (*RCP seal integrity–binding/popping*), and 1-OPR-RCPS (*RCP seal integrity lost during SBO*) fault trees. In addition to the failure of the shutdown seals to actuate, there was potential that the seals may not remain sealed. Therefore, an additional basic event, 1-RCS-SDS-SEALED (*shutdown seals fail to remain sealed*), was added under the same OR gates (1-SDS, 1-RCPSC2223, 1-RCPS-BP21, and 1-OPR-RCPS-02, respectively) with basic event 1-RCS-SDS-FC-ACTUATE. The assumed hourly failure rate is based on the NRC's evaluation of the improved RCP seal (NRC, 2017).

In addition to these changes, revisions to the SBO event tree were required. The 1-SDS fault tree was added to the event tree prior to the query of the 1-BP1 (*RCP seal stage 1 integrity (binding/popping)*) and 1-BP2 (*RCP seal stage 2 integrity (binding/popping)*) top events. Additional branching was developed that required the recovery of offsite power and subsequent decay heat removal. The requirement for additional mitigation actions to reach 72-hour safe/stable end state were not queried if the shutdown seals successfully actuated and remained sealed because of the minimal leakage expected (less than or equal to 2 gpm). See Figure 10-5 for the revised SBO event tree used in this sensitivity analysis.

Results. This sensitivity analysis resulted in a decrease in the overall internal event CDF from 6.39×10^{-5}/RCY to 5.64×10^{-5}/RCY (an approximate 12 percent decrease).

[239] The failure probability for the low leakage RCP seals was taken from the Final Safety Evaluation by the Office Of Nuclear Reactor Regulation, PWROG-14001-P, Revision 1, "PRA Model for the Generation III Westinghouse Shutdown Seal," (NRC, 2017). This failure probability is proprietary and is redacted from the public version of the safety evaluation report.

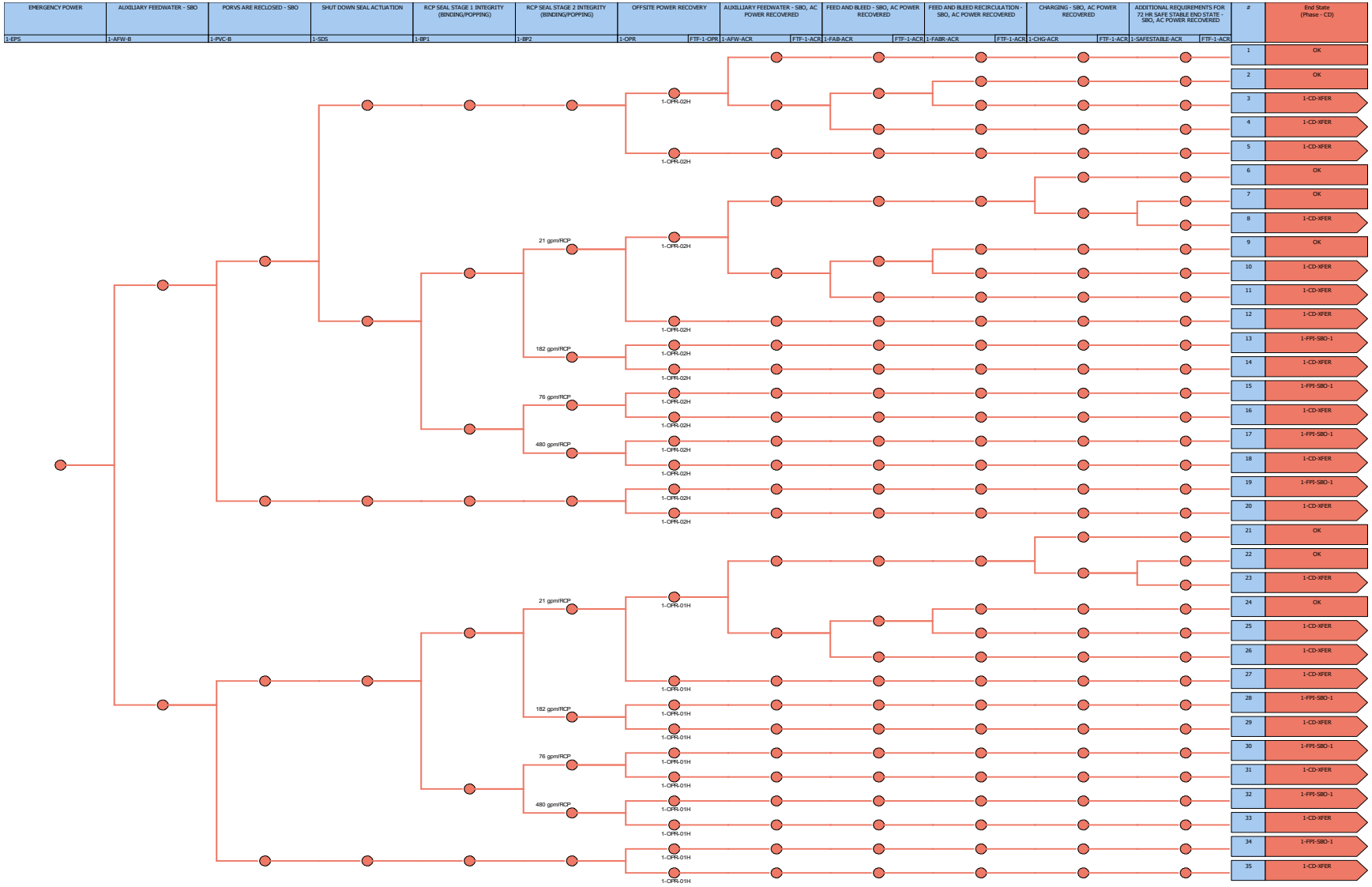


Figure 10-5 Revised SBO Event Tree for Crediting Improved RCP Shutdown Seals

10.9 Crediting Recovery for Failures of RAT Breakers and Load Sequencers

Description. The failures of the RAT breakers to open and/or load sequencers during LOOPs (including consequential) were dominant contributors to the overall CDF of the L3PRA project because these failures were assumed to preclude offsite power recovery. While this modeling assumption was potentially conservative, sufficient basis could not be developed from Reference Plant specific information to credit offsite power recovery given these failures. In addition to recovery (i.e., opening) of the RAT breakers, operators may be able to align offsite electrical power to the safety-related AC buses through the failed (closed) breaker if the failure cause does not preclude it (e.g., failure of the trip-latch mechanism).

During LOOP scenarios in which the RAT breaker(s) fail to open, a subsequent SBO will occur due to the EDG(s) being unable to load onto their respective safety-related AC buses. Although these breakers were in the closed position, they should be considered faulted and, therefore, offsite power should not be realigned through these breakers. Operating experience (failure data) of breakers seems to indicate that most failures-to-open were the result of a failed latch mechanism. These types of failures may be recoverable by operators manually unlatching or racking out the breakers locally. However, credit for recovery of hardware failures by troubleshooting/repair was not typically provided in base PRA models (except for recovering offsite power), which was consistent with the current state-of-practice.

Load sequencer failures may result in the following during a LOOP:

- Failure of RAT breakers to open,
- Failure of EDG output breakers to close, and/or
- Failure of sequencing of key plant SSCs (e.g., NSCW pumps).

No credit was provided for recovery of load sequencer failures in the L3PRA project. This modeling assumption may be conservative because operators may be able to manipulate breakers and necessary equipment; however, there was insufficient Reference Plant specific information available to justify recovery credit for load sequencer failures.

Sensitivity Case. To evaluate the effect of potential credit for operator actions to open RAT breakers (locally) and manually sequence equipment onto the respective EDGs, four fault trees were modified. Fault tree 1-AA0205-FTO-RANCC (*RAT A supply circuit breaker FTO due to random or common cause failure*) was modified by placing the two current basic events (representing the independent failure of a single RAT breaker and CCF of both RAT breakers) under a new OR gate (1-AA0205-FTO-RANCC2). In addition, new basic event 1-ACP-XHE-RATBRK (*operators fail to manually rack out RAT breakers*) was inserted under the top gate. A screening value of 0.1 was used for this HEP. The revised 1-AA0205-FTO-RANCC fault tree is provided in Figure 10-6. Similar changes were made to the 1-BA0301-FTO-RANCC (*RAT B supply circuit breaker FTO due to random or common cause failure*) fault tree.

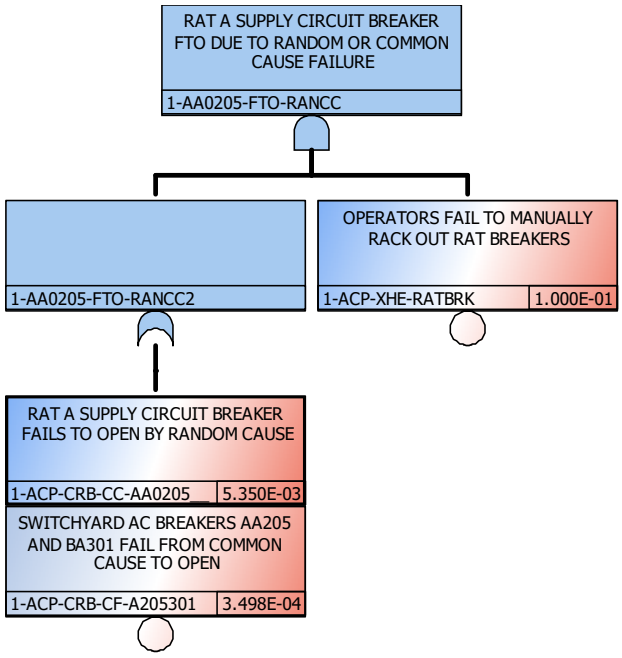


Figure 10-6 Revised 1-AA0205-FTO-RANCC Fault Tree

To model the recovery of load sequencer failures, fault tree 1-EPS-SEQ-A (*load sequencer A is unavailable*) was modified. For the 1-EPS-SEQ-A fault tree, a new AND gate (1-EPS-SEQ-A02) was inserted under existing gate 1-EPS-SEQ-A4. Gate 1-EPS-SEQ-A41 was moved under 1-EPS-SEQ-A02. In addition, new basic event 1-EPS-SEQ-XHE-MANUAL (*operators fail to manually sequence equipment*) was inserted under gate 1-EPS-SEQ-A02. A screening value of 0.1 was used for this HEP. The revised 1-EPS-SEQ-A fault tree is provided in Figure 10-7. Similar changes were made to the 1-EPS-SEQ-B (*load sequencer B is unavailable*) fault tree.

Results. This sensitivity analysis resulted in a decrease in the overall internal event CDF from 6.39×10^{-5}/RCY to 3.44×10^{-5}/RCY (an approximate 46 percent decrease).

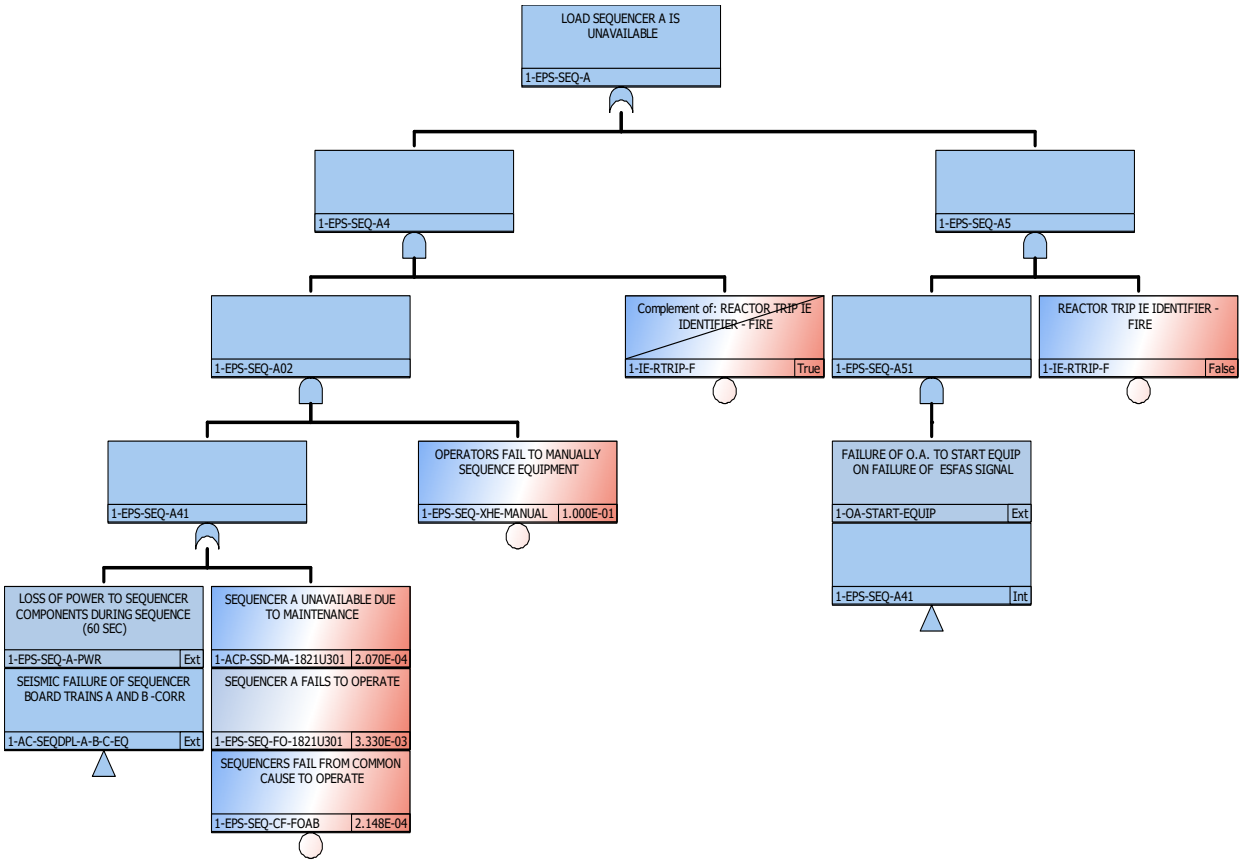


Figure 10-7 Revised 1-AA0205-FTO-RANCC Fault Tree

Applying a Minimum Joint HEP

Description. NUREG-1792, "Good Practices for Implementing Human Reliability Analysis (HRA)," states,

The total combined probability of all the HFEs in the same accident sequence/cut set should not be less than a justified value. It is suggested that the value not be below ~0.00001 since it is typically hard to defend that other dependent failure modes that are not usually treated (e.g., random events such as even a heart attack) cannot occur. Depending on the independent HFE values, the combined probability may need to be higher.

The 10^{-5} joint HEP was not meant to be an absolute "floor," but rather to ensure dependence was considered between HFEs within the same cut set, with a focus on dependency between HFEs that result in very low joint (independent) HEPs. The NRC staff's view is that there is

some joint HEP level below which the results are unreasonable. However, no consensus value or approach has been developed, to date.[240]

Sensitivity Case. To see the potential impact that applying a minimum joint HEP threshold has on the L3PRA Level 1 internal event PRA model results, a sensitivity analysis was performed using a minimum joint HEP of 10^{-5}. This minimum joint HEP was applied to all HFE combinations that have an independent or dependent joint HEP of less than 10^{-5}.[241] The following post-processing rules were developed to apply the minimum joint HEP value to the applicable HFE combinations[242]:

| HFE Combination 49

elsif 1-OA-SAGD-CHG--H * 1-OA-XFER-NON1EH-LT * 1-OA-ALTAFW----H * 1-OAR_LTFB-TRA-H then

DeleteEvent = 1-OA-SAGD-CHG--H;

DeleteEvent = 1-OA-XFER-NON1EH-LT;

DeleteEvent = 1-OA-ALTAFW----H;

DeleteEvent = 1-OAR_LTFB-TRA-H;

AddEvent = 1-HEP-JOINTMINIMUM49;

| HFE Combination 48

elsif 1-OA-SAGD-CHG--H * 1-OA-XFER-NON1EH-LT * 1-OA-ALTAFW----H * 1-OAB_TR-------H-LT then

DeleteEvent = 1-OA-SAGD-CHG--H;

DeleteEvent = 1-OA-XFER-NON1EH-LT;

DeleteEvent = 1-OA-ALTAFW----H;

DeleteEvent = 1-OAB_TR-------H-LT;

AddEvent = 1-HEP-JOINTMINIMUM48;

| HFE Combination 47

elsif 1-OA-SAGD-CHG--H * 1-OA-ALTAFW----H * 1-OAF_MFW------H * 1-OAB_TR-------H-LT then

DeleteEvent = 1-OA-SAGD-CHG--H;

DeleteEvent = 1-OA-ALTAFW----H;

DeleteEvent = 1-OAF_MFW------H;

DeleteEvent = 1-OAB_TR-------H-LT;

AddEvent = 1-HEP-JOINTMINIMUM47;

| HFE Combination 46

elsif 1-OA-SAGD-CHG--H * 1-OA-ALTAFW----H * 1-OAF_MFW------H * 1-OAR_LTFB-TRA-H then

[240] Recent work in this area has been completed by EPRI, as documented in EPRI 3002003150, "A Process for HRA Dependency Analysis and Considerations on the Use of Minimum Joint HEP Values." However, this approach does not provide a strict minimum joint HEP, but rather, describes a risk-informed approach.

[241] The joint HEPs of interest for each HFE combination are either the independent or dependent values (based on the results of the dependency evaluation).

[242] The post-processing rules associated with HFE combinations that had independent or dependent joint HEPs greater than or equal to 10^{-5} were not adjusted for this sensitivity analysis and are not shown.

```
  DeleteEvent = 1-OA-SAGD-CHG--H;

  DeleteEvent = 1-OA-ALTAFW----H;

  DeleteEvent = 1-OAF_MFW------H;

  DeleteEvent = 1-OAR_LTFB-TRA-H;

  AddEvent = 1-HEP-JOINTMINIMUM46;


| HFE Combination 42

elsif 1-OA-XFER-NON1EH-LT * 1-OA-
ALTAFW----H * 1-OAR_LTFB-TRA-H then

  DeleteEvent = 1-OA-XFER-NON1EH-LT;

  DeleteEvent = 1-OA-ALTAFW----H;

  DeleteEvent = 1-OAR_LTFB-TRA-H;

  AddEvent = 1-HEP-JOINTMINIMUM42;


| HFE Combination 41

elsif 1-OA-XFER-NON1EH-LT * 1-OA-
ALTAFW----H * 1-OAB_TR-------H-LT then

  DeleteEvent = 1-OA-XFER-NON1EH-LT;

  DeleteEvent = 1-OA-ALTAFW----H;

  DeleteEvent = 1-OAB_TR-------H-LT;

  AddEvent = 1-HEP-JOINTMINIMUM41;


| HFE Combination 40

elsif 1-OA-XFER-NON1EH-LT * 1-OA-
ALTAFW----H * 1-CAD-XHE-SGTR-LT then

  DeleteEvent = 1-OA-XFER-NON1EH-LT;

  DeleteEvent = 1-OA-ALTAFW----H;

  DeleteEvent = 1-CAD-XHE-SGTR-LT;

  AddEvent = 1-HEP-JOINTMINIMUM40;


| HFE Combination 39

elsif 1-OA-XFER-NON1EH-LT * 1-OAN_SL-
------H * 1-OA-ALTAFW----H then

  DeleteEvent = 1-OA-XFER-NON1EH-LT;

  DeleteEvent = 1-OA-ALTAFW----H;

  DeleteEvent = 1-OAN_SL-------H;

  AddEvent = 1-HEP-JOINTMINIMUM39;


| HFE Combination 31

elsif 1-OA-SAGD-CHG--H * 1-OA-ALTAFW-
---H * 1-OAR_LTFB-TRA-H then

  DeleteEvent = 1-OA-SAGD-CHG--H;

  DeleteEvent = 1-OA-ALTAFW----H;

  DeleteEvent = 1-OAR_LTFB-TRA-H;

  AddEvent = 1-HEP-JOINTMINIMUM31;


| HFE Combination 30

elsif 1-OA-SAGD-CHG--H * 1-OA-ALTAFW-
---H * 1-OAB_TR-------H-LT then

  DeleteEvent = 1-OA-SAGD-CHG--H;

  DeleteEvent = 1-OA-ALTAFW----H;

  DeleteEvent = 1-OAB_TR-------H-LT;

  AddEvent = 1-HEP-JOINTMINIMUM30;


| HFE Combination 27
```

```
elsif 1-OA-RWSTLOACC-H * 1-OA-
ALTAFW----H * 1-OAR_LTFB-TRA-H then

  DeleteEvent = 1-OA-RWSTLOACC-H;

  DeleteEvent = 1-OA-ALTAFW----H;

  DeleteEvent = 1-OAR_LTFB-TRA-H;

  AddEvent = 1-HEP-JOINTMINIMUM27;


| HFE Combination 26

elsif 1-OA-RWSTLOACC-H * 1-OA-
ALTAFW----H * 1-OAB_TR-------H-LT then

  DeleteEvent = 1-OA-RWSTLOACC-H;

  DeleteEvent = 1-OA-ALTAFW----H;

  DeleteEvent = 1-OAB_TR-------H-LT;

  AddEvent = 1-HEP-JOINTMINIMUM26;


| HFE Combination 25

elsif 1-OAI_SG-------H * 1-OA-XFER-
NON1EH-LT * 1-OA-ALTAFW----H then

  DeleteEvent = 1-OAI_SG-------H;

  DeleteEvent = 1-OA-XFER-NON1EH-LT;

  DeleteEvent = 1-OA-ALTAFW----H;

  AddEvent = 1-HEP-JOINTMINIMUM25;


| HFE Combination 24

elsif 1-OAD_SGR------H * 1-OA-XFER-
NON1EH-LT* 1-OA-ALTAFW----H then

  DeleteEvent = 1-OAD_SGR------H;

  DeleteEvent = 1-OA-XFER-NON1EH-LT;

  DeleteEvent = 1-OA-ALTAFW----H;

  AddEvent = 1-HEP-JOINTMINIMUM24;


| HFE Combination 21

elsif 1-OA-CCP-ALIGN---H * 1-OAC_NC-----
--H * 1-OAR_LTFB-TRA-H then

  DeleteEvent = 1-OA-CCP-ALIGN---H;

  DeleteEvent = 1-OAC_NC-------H;

  DeleteEvent = 1-OAR_LTFB-TRA-H;

  AddEvent = 1-HEP-JOINTMINIMUM21;


| HFE Combination 20

elsif 1-OA-CCP-ALIGN---H * 1-OA-
ALTAFW----H * 1-OAB_TR-------H-LT then

  DeleteEvent = 1-OA-CCP-ALIGN---H;

  DeleteEvent = 1-OA-ALTAFW----H;

  DeleteEvent = 1-OAB_TR-------H-LT;

  AddEvent = 1-HEP-JOINTMINIMUM20;


| HFE Combination 19

elsif 1-OA-ALTAFW----H * 1-OAF_MFW-----
-H * 1-OAR_LTFB-TRA-H then

  DeleteEvent = 1-OA-ALTAFW----H;

  DeleteEvent = 1-OAR_LTFB-TRA-H;

  DeleteEvent = 1-OAF_MFW------H;

  AddEvent = 1-HEP-JOINTMINIMUM19;


| HFE Combination 18
```

```
elsif 1-OA-ALTAFW----H * 1-OAF_MFW-----
-H * 1-OAB_TR-------H-LT then
  DeleteEvent = 1-OA-ALTAFW----H;
  DeleteEvent = 1-OAB_TR-------H-LT;
  DeleteEvent = 1-OAF_MFW------H;
  AddEvent = 1-HEP-JOINTMINIMUM18;

| HFE Combination 14
elsif 1-OAN_SL-------H * 1-OAR_LPSL-----H
then
  DeleteEvent = 1-OAN_SL-------H;
  DeleteEvent = 1-OAR_LPSL-----H;
  AddEvent = 1-HEP-JOINTMINIMUM14;

| HFE Combination 9
elsif 1-OAD_SGR------H * 1-RFL-XHE-
REFILL-LT then
  DeleteEvent = 1-OAD_SGR------H;
  DeleteEvent = 1-RFL-XHE-REFILL-LT;
  AddEvent = 1-HEP-JOINTMINIMUM9;

| HFE Combination 8
elsif 1-OAD_SGR------H * 1-OA-ALTAFW----
H then
  DeleteEvent = 1-OAD_SGR------H;
  DeleteEvent = 1-OA-ALTAFW----H;
  AddEvent = 1-HEP-JOINTMINIMUM8;

| HFE Combination 5
elsif 1-OA-ALTAFW----H * 1-OA-
SUMPMOV---H then
  DeleteEvent = 1-OA-ALTAFW----H;
  DeleteEvent = 1-OA-SUMPMOV---H;
  AddEvent = 1-HEP-JOINTMINIMUM5;

| HFE Combination 4
elsif 1-OA-ALTAFW----H * 1-OAB_TR-------
H-LT then
  DeleteEvent = 1-OA-ALTAFW----H;
  DeleteEvent = 1-OAB_TR-------H;
  AddEvent = 1-HEP-JOINTMINIMUM4;

| HFE Combination 3
elsif 1-OA-ALTAFW----H * 1-OAR_LTFB-
TRA-H then
  DeleteEvent = 1-OA-ALTAFW----H;
  DeleteEvent = 1-OAR_LTFB-TRA-H;
  AddEvent = 1-HEP-JOINTMINIMUM3;

| HFE Combination 2
elsif 1-CHG-XHE-NORMAL * 1-CAD-XHE-
SAFESTBLE then
  DeleteEvent = 1-CHG-XHE-NORMAL;
  DeleteEvent = 1-CAD-XHE-SAFESTBLE;
  AddEvent = 1-HEP-JOINTMINIMUM2;
```

| HFE Combination 1	DeleteEvent = 1-OA-ALTAFW----H;
elsif 1-OA-ALTAFW----H * 1-CAD-XHE-SGTR-LT then	DeleteEvent = 1-CAD-XHE-SGTR-LT; AddEvent = 1-HEP-JOINTMINIMUM1;

Results and Insights. This sensitivity analysis results in an increase in the overall internal event CDF from 6.39×10^{-5}/RCY to 6.42×10^{-5}/RCY (less than a 1 percent increase). The minor increase in CDF is largely from HFE Combination 2. The top cut set with the joint minimum HEP applied has a CDF of 1.23×10^{-7}/RCY. HFE combinations 1, 8, and 9 are minor contributors. Since the post-processing rules in SAPHIRE were applied after truncation (that used a limit of 10^{-12}/RCY), the minor increase in CDF shown in this sensitivity analysis could be greater. Therefore, the same sensitivity analysis was run using a truncation limit of 10^{-13}/RCY to see the effect on CDF. This resulted in an increase in the overall internal event CDF from 6.42×10^{-5}/RCY to 6.45×10^{-5}/RCY (less than a 1 percent increase). A further lowering of the truncation limit would increase the overall CDF; however, applying the minimum joint HEP was not expected to result in a significant increase in the overall CDF even when using a lower truncation limit.

10.10 Removing Stress from Dependency Evaluation

Description. Given the lack of guidance on evaluating stress between HFEs using the dependency tree from the EPRI HRA Calculator, the dependency evaluation of HFE pairs in the L3PRA Level 1 internal event PRA model made the conservative assumption to use the higher branch for the stress node in the decision tree (i.e., high/moderate stress), without evaluating stress explicitly. If the lower branch is used (i.e., low stress), HFE pairs that have a time difference of greater than 60 minutes were considered to have zero dependence.[243] In addition, the 15-minute intervals up to 60 minutes will have decreased dependency. The Figure 10-8 shows the revised dependency decision tree assuming low stress:

[243] Assuming the HFEs do not share a "common cognitive" function.

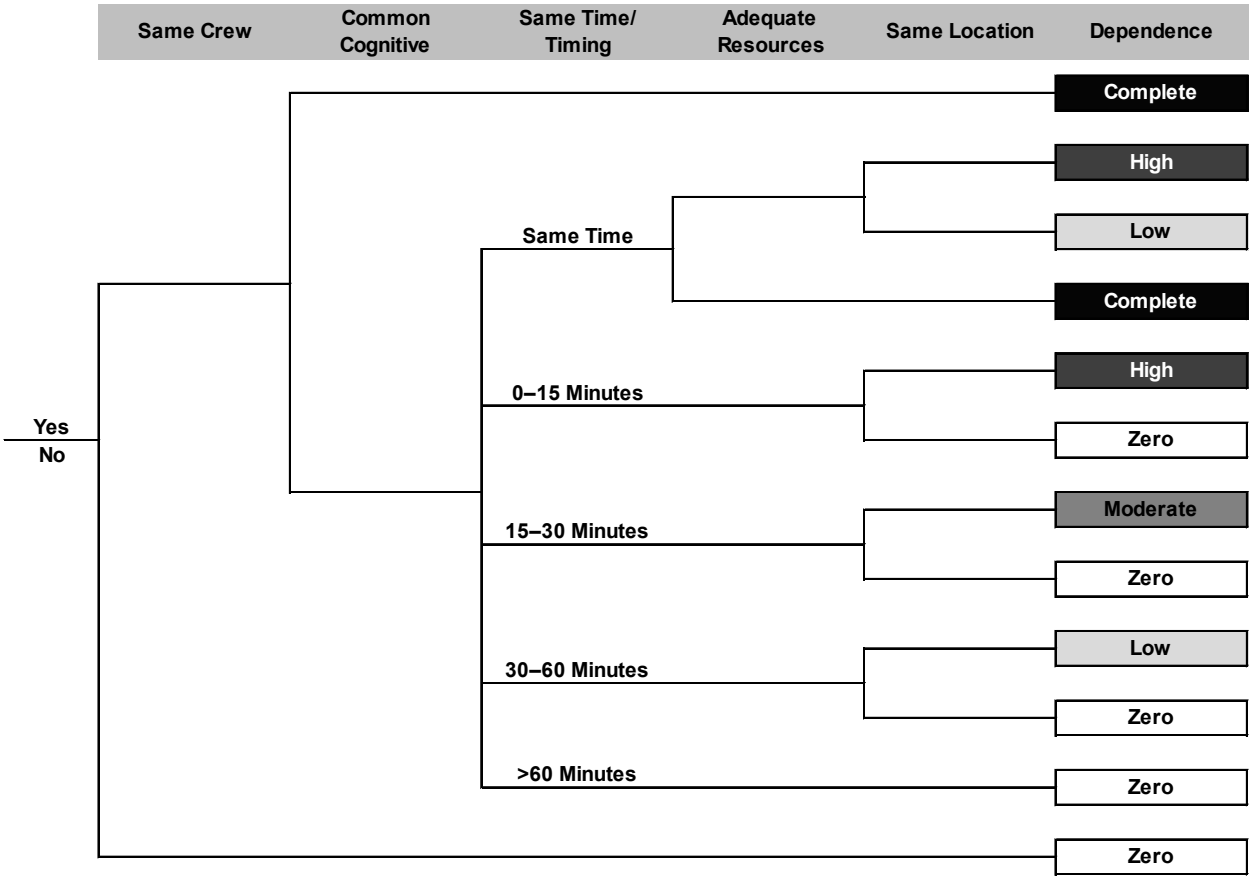


Figure 10-8 Revised Dependency Decision Tree Assuming Low Stress

Sensitivity Case. The dependency evaluation results were modified using the revised dependency decision tree shown above. The table (shown on the following page) provides the revised dependency results for this sensitivity case. In addition, as shown in Table 10-9, the following post-processing rule changes were made to account for the revised dependency analysis:

Table 10-8 L3PRA Project Level 1 Model Revised Dependency Analysis Post Processing Rule Changes

#	1St HFE	2nd HFE	Independent HEP	Base Model Dependence Level	Sensitivity Dependence Level	Dependent HEP	Notes
1	CAD-XHE-SGTR-LT	OA-ALTAFW----H	1.0E-4	Zero			
2	CHG-XHE-NORMAL	CAD-XHE-SAFESTABLE	7.5E-4	Zero			
3	OA-ALTAFW----H	OAB_TR-------H-LT	2.9E-3	Low	Zero		No common-cognitive function; >60 minutes
4	OA-ALTAFW----H	OAF_MFW------H	2.7E-2	Low	Zero		
5	OA-ALTAFW----H	OAR_LTFB-TRA-H	6.0E-4	Zero			
6	OA-ALTAFW----H	OA-SUMPMOV---H	1.8E-3	Zero			
7	OAC_NC-------H	OAR_HPSLA----H	6.0E-4	Low	Zero		No common-cognitive function; >60 minutes between HFEs
8	OAC_NC-------H	OA-HPR-ACRA--H	1.2E-3	Low	Zero		

#	1St HFE	2nd HFE	Independent HEP	Base Model Dependence Level	Sensitivity Dependence Level	Dependent HEP	Notes
9	OA-CCP-ALIGN---H	OA-ALTAFW----H	1.0E-4	Zero			
10	OA-CCP-ALIGN---H	OAC_NC-------H	9.1E-4	Moderate	Low	5.1E-2	No common-cognitive function; 35 minutes between HFEs; same location
11	OA-CCP-ALIGN---H	OAN_SL-------H	1.1E-3	Low	Zero		No common-cognitive function; >60 minutes between HFEs
12	OAD_SGR------H	OA-ALTAFW----H	1.0E-4	Zero			
13	OAD_SGR------H	RFL-XHE-REFILL-LT	1.0E-4	Zero			
14	OAD_SGR------H	OA-XFER-NON1EH-LT	2.7E-3	High	Moderate	0.15	No common-cognitive function; 15–30 minutes between HFEs; same location
15	OAF_MFW------H	OAB_TR-------H	5.8E-2	High	Moderate	0.19	
16	OAF_MFW------H	OAB_TR-------H-LT	2.9E-3	Low	Zero		No common-cognitive function; >60 minutes between HFEs
17	OAF_MFW------H	OA-HURGXFMR--H	3.4E-3	Low	Zero		

#	1St HFE	2nd HFE	Independent HEP	Base Model Dependence Level	Sensitivity Dependence Level	Dependent HEP	Notes
18	OAF_MFW------H	OAR_LTFB-TRA-H	6.0E-4	Low	Zero		
19	OAF_MFW------H	OA-SUMPMOV---H	1.8E-3	Low	Zero		
20	OAI_SG-------H	OA-ALTAFW----H	1.0E-4	Zero			
21	OAI_SG-------H	RFL-XHE-REFILL-LT	1.0E-4	Zero			
22	OAI_SG-------H	OA-XFER-NON1EH-LT	2.7E-3	Moderate	Low	5.3E-2	No common-cognitive function; 39 minutes between HFEs; same location

Table 10-9 L3PRA Project Level 1 Model Revised Dependency Analysis Post Processing Rule Changes (cont.)

#	1St HFE	2nd HFE	Independent HEP	Base Model Dependence Level	Sensitivity Dependence Level	Dependent HEP	Notes
23	OAN_SL-------H	OA-ALTAFW----H	1.0E-4	Zero			
24	OAN_SL-------H	OAR_LPSL-----H	1.1E-3	Low	Zero		No common-cognitive function; >60 minutes between HFEs
25	OA-RWSTLOACC-H	OA-ALTAFW----H	1.0E-4	Zero			
26	OA-RWSTLOACC-H	OAN_SL-------H	1.1E-3	Low	Zero		No common-cognitive function; >60 minutes between HFEs
27	OA-RWSTLOACC-H	OAC_NC-------H	9.1E-4	Moderate	Low	5.1E-2	No common-cognitive function; 35 minutes between HFEs; same location
28	OA-SAGD-CHG--H	OA-ALTAFW----H	1.0E-4	Zero			
29	OA-SAGD-CHG--H	OA-XFER-NON1EH-LT	2.7E-3	Low	Zero		No common-cognitive function; >60 minutes between HFEs
30	OA-SAGD-CHG--H	OAT----------H	2.6E-4	Low	Zero		

Table 10-9 L3PRA Project Level 1 Model Revised Dependency Analysis Post Processing Rule Changes (cont.)

#	1St HFE	2nd HFE	Independent HEP	Base Model Dependence Level	Sensitivity Dependence Level	Dependent HEP	Notes
31	OA-SAGD-CHG--H	OAF_MFW------H	2.7E-2	Low	Zero		
32	OA-START-AFW-H	OAF_MFW------H	2.7E-2	Complete	Complete	1.0	HFEs share common-cognitive function
33	OAT----------H	OAC_NC-------H	9.1E-4	High	Moderate	0.14	No common-cognitive function; 25 minutes between HFEs; same location
34	OA-XFER-NON1EH-LT	CAD-XHE-SGTR-LT	1.9E-3	Low	Zero		No common-cognitive function; >60 minutes between HFEs
35	OA-XFER-NON1EH-LT	OA-ALTAFW----H	1.0E-4	Zero			
36	OA-XFER-NON1EH-LT	OAN_SL-------H	1.1E-3	Low	Zero		No common-cognitive function; >60 minutes between HFEs
37	RCS-XHE-XM-TRIP	OAC_NC-------H	9.1E-4	High	Moderate	0.14	No common-cognitive function; 30 minutes between HFEs; same location

Table 10-9 L3PRA Project Level 1 Model Revised Dependency Analysis Post Processing Rule Changes (cont.)

#	1St HFE	2nd HFE	Independent HEP	Base Model Dependence Level	Sensitivity Dependence Level	Dependent HEP	Notes
38	RCS-XHE-XM-TRIP-LONSCW	OA-CCP-ALIGN----H	0.13	Complete	Complete	1.0	HFEs share common-cognitive function
39	RCS-XHE-XM-TRIP-LONSCW	OAC_NC-------H	9.1E-4	Moderate	Low	5.1E-2	No common-cognitive function; 37 minutes between HFEs; same location
40	RCS-XHE-XM-TRIP-LONSCW	OA-RWSTLOACC-H	0.13	Complete	High	0.57	No common-cognitive function; 2 minutes between HFEs; same location
41	RCS-XHE-XM-TRIP-LONSCW	OA-OSW-------H	2.0E-2	Complete	Complete	1.0	HFEs share common-cognitive function

```
| HFE Combination 53
if 1-RCS-XHE-XM-TRIP-LONSCW * 1-OA-
RWSTLOACC-H * 1-OAN_SL-------H * 1-
OAR_LPSL-----H then
  DeleteEvent = 1-OA-RWSTLOACC-H;
  AddEvent = 1-OA-RWSTLOACC-H-HD;

| HFE Combination 52
elsif 1-RCS-XHE-XM-TRIP-LONSCW * 1-OA-
RWSTLOACC-H * 1-OAC_NC-------H * 1-
OAR_HPSLA----H then
  DeleteEvent = 1-OA-RWSTLOACC-H;
  AddEvent = 1-OA-RWSTLOACC-H-HD;
  DeleteEvent = 1-OAC_NC-------H;
  AddEvent = 1-OAC_NC-------H-LD;

| HFE Combination 51
elsif 1-RCS-XHE-XM-TRIP-LONSCW * 1-OA-
CCP-ALIGN---H * 1-OAN_SL-------H * 1-
OAR_LPSL-----H then
  DeleteEvent = 1-OA-CCP-ALIGN---H;
  AddEvent = 1-OA-CCP-ALIGN---H-CD;

| HFE Combination 50
elsif 1-RCS-XHE-XM-TRIP-LONSCW * 1-OA-
CCP-ALIGN---H * 1-OAC_NC-------H * 1-
OAR_HPSLA----H then
  DeleteEvent = 1-OA-CCP-ALIGN---H;
  AddEvent = 1-OA-CCP-ALIGN---H-CD;
  DeleteEvent = 1-OAC_NC-------H;
  AddEvent = 1-OAC_NC-------H-LD;

| HFE Combination 45
elsif 1-OA-SAGD-CHG--H * 1-OAT----------H *
1-OAC_NC-------H * 1-OAR_HPSLA----H then
  DeleteEvent = 1-OAC_NC-------H;
  AddEvent = 1-OAC_NC-------H-MD;

| HFE Combination 44
elsif 1-RCS-XHE-XM-TRIP-LONSCW * 1-
OAC_NC-------H * 1-OAR_HPSLA----H then
  DeleteEvent = 1-OAC_NC-------H;
  AddEvent = 1-OAC_NC-------H-LD;

| HFE Combination 43
elsif 1-RCS-XHE-XM-TRIP * 1-OAC_NC-------
H * 1-OAR_HPSLA----H then
  DeleteEvent = 1-OAC_NC-------H;
  AddEvent = 1-OAC_NC-------H-LD;

| HFE Combination 38
  AddEvent = 1-OAF_MFW------H-CD;

| HFE Combination 35
elsif 1-OA-START-AFW-H * 1-OAF_MFW-----
-H * 1-OAB_TR-------H then
  DeleteEvent = 1-OAF_MFW------H;
  AddEvent = 1-OAF_MFW------H-CD;
  DeleteEvent = 1-OAB_TR-------H;
  AddEvent = 1-OAB_TR-------H-MD;

| HFE Combination 34
elsif 1-OA-START-AFW-H * 1-OAF_MFW-----
-H * 1-OA-HURGXFMR--H then
  DeleteEvent = 1-OAF_MFW------H;
  AddEvent = 1-OAF_MFW------H-CD;

| HFE Combination 32
elsif 1-OA-SAGD-CHG--H * 1-OAF_MFW-----
-H * 1-OAB_TR-------H then
  DeleteEvent = 1-OAB_TR-------H;
  AddEvent = 1-OAB_TR-------H-MD;

| HFE Combination 29
elsif 1-OA-RWSTLOACC-H * 1-OAC_NC------
-H * 1-OAR_HPSLA----H then
  DeleteEvent = 1-OAC_NC-------H;
  AddEvent = 1-OAC_NC-------H-LD;

| HFE Combination 25
elsif 1-OAI_SG-------H * 1-OA-XFER-
NON1EH-LT * 1-OA-ALTAFW----H then
  DeleteEvent = 1-OA-XFER-NON1EH;
  AddEvent = 1-OA-XFER-NON1EH-LT-LD;

| HFE Combination 24
elsif 1-OAD_SGR------H * 1-OA-XFER-
NON1EH-LT* 1-OA-ALTAFW----H then
  DeleteEvent = 1-OA-XFER-NON1EH-LT;
  AddEvent = 1-OA-XFER-NON1EH-LT-MD;

| HFE Combination 22
elsif 1-OA-CCP-ALIGN---H * 1-OAC_NC-------
H * 1-OAR_HPSLA----H then
  DeleteEvent = 1-OAC_NC-------H;
  AddEvent = 1-OAC_NC-------H-LD;

| HFE Combination 17
elsif 1-RCS-XHE-XM-TRIP-LONSCW * 1-OA-
OSW-------H then
  DeleteEvent = 1-OA-OSW-------H;
  AddEvent = 1-OA-OSW-------H-CD;
```

```
elsif 1-OAT----------H * 1-OAC_NC-------H * 1-
OAR_HPSLA----H then
  DeleteEvent = 1-OAC_NC-------H;
  AddEvent = 1-OAC_NC-------H-MD;

| HFE Combination 37
elsif 1-OA-START-AFW-H * 1-OAF_MFW-----
-H *1-OA-SUMPMOV---H then
  DeleteEvent = 1-OAF_MFW------H;
  AddEvent = 1-OAF_MFW------H-CD;

| HFE Combination 36
elsif 1-OA-START-AFW-H * 1-OAF_MFW-----
-H * 1-OAR_LTFB-TRA-H then
  DeleteEvent = 1-OAF_MFW------H;

| HFE Combination 16
elsif 1-OA-START-AFW-H * 1-OAF_MFW-----
-H then
  DeleteEvent = 1-OAF_MFW------H;
  AddEvent = 1-OAF_MFW------H-CD;

| HFE Combination 10
elsif 1-OAF_MFW------H * 1-OAB_TR-------H
then
  DeleteEvent = 1-OAB_TR-------H;
  AddEvent = 1-OAB_TR-------H-MD
```

Results and Insights. This sensitivity analysis results in a decrease in the overall internal event CDF from 6.39×10^{-5}/RCY to 6.32×10^{-5}/RCY (approximately a 1 percent decrease).

10.11 Summary of Results

A summary of the results of the sensitivity cases documented in this report is provided below. As evident from the table, the largest decrease in CDF occurs when crediting the recovery of RAT breaker and load sequencer failures, reducing total Level 1 internal event CDF by nearly a factor of two. Other significant decreases in CDF occur when crediting turbine-driven AFW pump operation in the absence of safety-related AC and DC power (when the associated HEPs are 0.1 or lower) and when using the alternative approach for calculating grid-related LOOP initiating event frequency.

Table 10-11 Summary of Sensitivity Cases Results

#	Description	Base CDF (per RCY)	Sensitivity CDF (per RCY)	Percent Change
1	Change in medium LOCA initiating event frequency	6.39×10^{-5}	6.17×10^{-5}	-3%
2	Change in grid-related LOOP initiating event frequency	6.39×10^{-5}	5.01×10^{-5}	-22%
3	"Blind" turbine-driven AFW pump operation Case A (HEPs = 0.3) Case B (HEPs = 0.1) Case C (HEPs = 0.03)	6.39×10^{-5}	5.91×10^{-5} 4.69×10^{-5} 4.27×10^{-5}	-8% -27% -33%
4	Restoring offsite power without DC power	6.39×10^{-5}	5.82×10^{-5}	-9%
5	Safe/stable end state at 24 hours	6.39×10^{-5}	6.33×10^{-5}	-1%
6	Credit SI pumps for feed and bleed cooling for transients	6.39×10^{-5}	6.39×10^{-5}	–
7	Increased turbine building battery depletion time	6.39×10^{-5}	6.00×10^{-5}	-6%
8	New RCP shutdown seals	6.39×10^{-5}	5.64×10^{-5}	-12%
9	Recovery of RAT breaker and load sequencer failures	6.39×10^{-5}	3.44×10^{-5}	-46%
10	Applying a minimum joint HEP	6.39×10^{-5}	6.42×10^{-5}	+<1%
11	Removing stress from HFE dependency evaluation	6.39×10^{-5}	6.32×10^{-5}	-1%

11 REFERENCES

ASME/ANS, 2009 — American Society of Mechanical Engineers (ASME)/American Nuclear Society (ANS), "Addenda to ASME RA-Sa-2008 Standard for Level 1/Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications," ASME/ANS RA-Sa-2009, February 2009. *(Available for a fee from ASME).*

BNL, 2006 — Brookhaven National Laboratory, "Generic Probability of a LOOP after a Large LOCA: An Evaluation," November 2006. (Agencywide Documents Access and Management System (ADAMS) Accession No. ML071430462).

EPRI, 1990 — Electric Power Research Institute (EPRI), "Operator Reliability Experiments Using Power Plant Simulators," NP-6937, August 1990.

EPRI, 1992 — Electric Power Research Institute, "An Approach to the Analysis of Operator Actions in PRA," TR-100259, June 1992.

EPRI, 2008 — Electric Power Research Institute, "Support Systems Initiating Events," TR-1016741, December 2008.

EPRI, 2011 — Electric Power Research Institute, "Human Reliability Analysis Calculator Version 4.21," TR-1022814, June 2011. *(Available for a fee from EPRI).*

IEEE, 2013 — Institute of Electrical and Electronic Engineers (IEEE), "Standard Criteria for Class 1E Power Systems for Nuclear Power Generating Stations," Standard 308-2012, January 2013. *(Available for a fee from IEEE).*

INL, 2016 — Idaho National Laboratory, "System and Component Descriptions, Boundaries, and Failure Modes," April 2016.

LLNL, 1997 — Lawrence Livermore National Laboratory, "Recommendations for Probabilistic Seismic Hazard Analysis: Guidance on Uncertainty and Use of Experts," NUREG/CR-6372, Volumes 1 and 2, April 1997 (ADAMS Accession Nos. ML080090003 and ML080090004).

McCormick, 1981 — McCormick, N., "Reliability and Risk Analysis Methods and Nuclear Power Applications," 1981. *(Available for purchase online).*

NEI, 2013 — Nuclear Energy Institute, "Regulatory Assessment Performance Indicator Guideline," NEI 99-02, Revision 7, August 2013 (ADAMS Accession No. ML13261A116).

NRC, 1975 U.S. Nuclear Regulatory Commission, “The Reactor Safety Study,” WASH-1400, October 1975.

NRC, 1983 U.S. Nuclear Regulatory Commission, "Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications," NUREG/CR-1278, August 1983 (ADAMS Accession No. ML071210299).

NRC, 1987 U.S. Nuclear Regulatory Commission, "Accident Sequence Evaluation Program Human Reliability Analysis Procedure," NUREG/CR-4772, February 1987.

NRC, 1998 U.S. Nuclear Regulatory Commission, “Guidelines on Modeling Common-Cause Failures in Probabilistic Risk Assessment,” NUREG/CR-5485, November 1998.

NRC, 1999a U.S. Nuclear Regulatory Commission, “Rates of Initiating Events at U.S. Nuclear Power Plants: 1987–1995,” NUREG/CR-5750, February 1999 (ADAMS Accession No. ML070580080).

NRC, 1999b U.S. Nuclear Regulatory Commission, “Reliability Study: Westinghouse Reactor Protection System, 1984-1985,” NUREG/CR-5500, Volume 2, December 1998.

NRC, 2003a U.S. Nuclear Regulatory Commission, “Handbook of Parameter Estimation for Probabilistic Risk Assessment,” NUREG/CR-6823, September 2003 (ADAMS Accession No. ML032900131).

NRC, 2003b U.S. Nuclear Regulatory Commission, “Operating Experience Assessment—Effects of Grid Events on Nuclear Power Plant Performance,” NUREG-1784, December 2003 (ADAMS Accession No. ML033530400).

NRC, 2003c U.S. Nuclear Regulatory Commission, “Safety Evaluation of Topical Report WCAP-15603, Revision 1, WOG 2000 Reactor Coolant Pump Seal Leakage Model for Westinghouse PWRs," May 2003 (ADAMS Accession No. ML031400376).

NRC, 2005a U.S. Nuclear Regulatory Commission, “Reevaluation of Station Blackout Risk at Nuclear Power Plants,” NUREG/CR-6890, Volumes 1 and 2, December 2005 (ADAMS Accession Nos. ML060200477 and ML060200479).

NRC, 2005b U.S. Nuclear Regulatory Commission, “Good Practices for Implementing Human Reliability Analysis,” NUREG-1792, April 2005 (ADAMS Accession No. ML051160213).

NRC, 2007 U.S. Nuclear Regulatory Commission, “Industry-Average performance for Components and Initiating Events at U.S.

Commercial Nuclear Power Plants," NUREG/CR-6928, February 2007 (ADAMS Accession No. ML070650650).

NRC, 2011 — U.S. Nuclear Regulatory Commission, "Industry Performance of Relief Valves at U.S. Commercial Nuclear Power Plants through 2007," NUREG/CR-7037, March 2011 (ADAMS Accession No. ML110980205).

NRC, 2012a — U.S. Nuclear Regulatory Commission, "Practical Implementation Guidelines for SSHAC Level 3 and 4 Hazard Studies," NUREG-2117, Revision 1, April 2012 (ADAMS Accession No. ML12118A445).

NRC, 2013 — U.S. Nuclear Regulatory Commission, "Glossary of Risk-Related Terms in Support of Risk-Informed Decisionmaking," NUREG-2122, November 2013 (ADAMS Accession No. ML13311A353).

NRC, 2017 — U.S. Nuclear Regulatory Commission, Final Safety Evaluation by the Office of Nuclear Reactor Regulation PWROG-14001-P, Revision 1, "PRA Model for the Generation III Westinghouse Shut-Down Seal," August 23, 2017 (ADAMS Accession No. ML17200C876).

Westinghouse, 1974 — Westinghouse, "Westinghouse Anticipated Transients without Trip Analysis," WCAP-08330, August 1974 (ADAMS Accession No. ML061790274).

Westinghouse, 2002 — Westinghouse, "WOG 2000 Reactor Coolant Pump Seal Leakage Model for Westinghouse PWRs," WCAP-15603, Revision 1, May 2002 (ADAMS Accession No. ML021500485).

Westinghouse, 2007 — Westinghouse, "WOG Risk-Informed ATWS Assessment and Licensing Implementation Process," WCAP-15831, Revision 2, August 2007 (ADAMS Accession No. ML072550560).

NRC FORM 335
(12-2010)
NRCMD 3.7

U.S. NUCLEAR REGULATORY COMMISSION

BIBLIOGRAPHIC DATA SHEET

(See instructions on the reverse)

1. REPORT NUMBER
(Assigned by NRC, Add Vol., Supp., Rev., and Addendum Numbers, if any.)

2. TITLE AND SUBTITLE

U.S. NRC Level 3Probabilistic RiskAssessment (PRA) Project

Volume 3a: Reactor, At-Power, Level 1 PRA for Internal Events

3. DATE REPORT PUBLISHED

MONTH	YEAR
Month	20xx

4. FIN OR GRANT NUMBER

5. AUTHOR(S)

List names from Cover of NUREG Report of individuals who contributed to this publication

6. TYPE OF REPORT

Technical

7. PERIOD COVERED (Inclusive Dates)

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

Performing Organization's Name and Address

9. SPONSORING ORGANIZATION - NAME AND ADDRESS (If NRC, type "Same as above", if contractor, provide NRC Division, Office or Region, U. S. Nuclear Regulatory Commission, and mailing address.)

Division

Office

10. SUPPLEMENTARY NOTES

First initial. Lastname

11. ABSTRACT (200 words or less)

Copy and paste Abstract here (200 words or less)

12. KEY WORDS/DESCRIPTORS (List words or phrases that will assist researchers in locating the report.)

List of keywords or phrases that will assist researchers in locating this NUREG.

13. AVAILABILITY STATEMENT

unlimited

14. SECURITY CLASSIFICATION

(This Page)

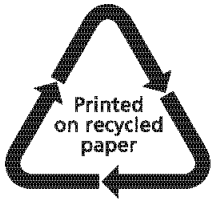
unclassified

(This Report)

unclassified

15. NUMBER OF PAGES

16. PRICE



Federal Recycling Program

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, DC 20555-0001

OFFICIAL BUSINESS