ANP-10274NP
Revision 0

U.S. EPR Probabilistic Risk Assessment Methods Report

December 2006

AREVA NP Inc.

Non-Proprietary

(c) 2006 AREVA NP Inc.

Copyright © 2006

AREVA NP Inc.
All Rights Reserved

The design, engineering and other information contained in this document have been prepared by or on behalf of AREVA NP Inc., an AREVA and Siemens company, in connection with its request to the U.S. Nuclear Regulatory Commission for a pre-application review of the U.S. EPR nuclear power plant design. No use of or right to copy any of this information, other than by the NRC and its contractors in support of AREVA NP's pre-application review, is authorized.

The information provided in this document is a subset of a much larger set of know-how, technology and intellectual property pertaining to an evolutionary pressurized water reactor designed by AREVA NP and referred to as the U.S. EPR. Without access and a grant of rights to that larger set of know-how, technology and intellectual property rights, this document is not practically or rightfully usable by others, except by the NRC as set forth in the previous paragraph.

For information address: AREVA NP Inc.
An AREVA and Siemens Company
3315 Old Forest Road
Lynchburg, VA 24506

Disclaimer

Important Notice Concerning the Contents and Application of This Report

This report was developed based on research and development funded and conducted by AREVA NP Inc., and is being submitted by AREVA NP to the U.S. Nuclear Regulatory Commission (NRC) to facilitate technical discussions related to the NRC's pre-application review of the U.S. EPR nuclear power plant design. This report is not intended to be formally reviewed or approved by the NRC, nor is it intended or suitable for application by a licensee.

The information provided in this report is true and correct to the best of AREVA NP's knowledge, information, and belief, but only the design information contained in the design certification application shall be considered final.

Neither AREVA NP nor any person acting on behalf of AREVA NP makes any warranty or representation, express or implied, with respect to the accuracy, completeness, or usefulness of the information contained in this report.

ABSTRACT

This report is provided to the NRC to support the review of the Probabilistic Risk Assessment (PRA) for the U.S. EPR design certification. This report provides a description of the design certification PRA scope and objectives; the technical approach and methodology used for analysis of internal and external events; and computer codes used. This report provides the basis to demonstrate that the design certification PRA, when completed, will provide a comprehensive risk assessment of the U.S. EPR design and will meet the objectives for design certification.

Nature of Changes

Item	Section (s) or Page (s	Description and Justification

Contents

Page

1.0 INTRODUCTION 1-1
1.1 PRA Scope and Objectives to Support Design Certification 1-1
1.2 Design Features Contributing to Risk Reduction 1-3
1.3 AREVA EPR/PRA International Cooperation for the U.S. EPR PRA 1-4
1.4 PRA Technical Adequacy and Quality 1-5
1.5 Influence of PRA on the Plant Design 1-6
2.0 INTERNAL EVENTS PRA METHODOLOGY 2-1
2.1 Level 1 Accident Sequence Evaluation and Success Criteria 2-1
2.1.1 Selected Initiating Events 2-1
2.1.2 Accident Sequences 2-9
2.1.3 Success Criteria 2-12
2.2 Data and Common Cause Failure Analysis 2-12
2.2.1 Sources of Initiating Event Data 2-12
2.2.2 Sources of Component Failure Data 2-13
2.2.3 Common Cause Component Groups and CCF Parameters 2-14
2.2.4 Comparison to Other Sources 2-14
2.3 PRA Systems Analysis 2-15
2.3.1 Description of U.S. EPR Systems in the PRA 2-15
2.3.2 U.S. EPR Digital I&C PRA Model 2-22
2.4 Human Reliability Analysis 2-30
2.4.1 Human Reliability Analysis for Pre-Accident Operator Actions 2-30
2.4.2 Human Reliability Analysis for Post-Accident Operator Actions 2-31
2.4.3 Treatment of Dependencies Between Human Actions 2-34
2.5 Approach to Level 1 Uncertainty and Sensitivity Analyses 2-35
2.5.1 Uncertainty Analysis 2-35
2.5.2 Sensitivity Analysis 2-35
2.6 Level 2 PRA 2-36
2.6.1 Overview of Level 2 Methodology 2-36
2.6.2 Definition of Core Damage End States 2-36
2.6.3 Level 2 Systems Analysis 2-37
2.6.4 Analysis of Severe Accident Phenomena and Progression 2-38
2.6.5 Containment Event Tree Quantification 2-38
2.6.6 Source Term Evaluation 2-39
2.6.7 Approach to Level 2 Uncertainty and Sensitivity Analysis 2-39
2.7 Level 3 PRA 2-40

3.0 INTERNAL FLOODING, INTERNAL FIRES, AND EXTERNAL EVENTS METHODOLOGY 3-1
3.1 U.S. EPR Spatial Arrangements 3-1
3.2 Internal Flooding Analysis 3-2
3.3 Internal Fire Analysis 3-2
3.4 Seismic Methodology 3-3
3.4.1 Seismic Hazard Input 3-4
3.4.2 Seismic Fragility Evaluation 3-4
3.4.3 Systems/Accident Sequence Analysis 3-6
3.4.4 HCLPF Sequence Assessment 3-6
3.5 Other External Events 3-7
4.0 LOW POWER SHUTDOWN ANALYSIS 4-1
4.1 Scope of the Low Power Shutdown Analysis 4-1
4.2 Plant Operating States 4-1
4.3 Selected Initiating Events for LPSD 4-2
4.4 Success Criteria for LPSD 4-3
4.5 Systems Analysis for LPSD 4-3
4.6 Human Reliability for LPSD 4-4
5.0 COMPUTER CODES 5-1
5.1 PRA Level 1 and 2 Codes 5-1
5.2 PRA Level 3 Codes 5-6
5.2.1 MACCS2 Code Description 5-6
5.2.2 RiskIntegrator 5-7
6.0 SUMMARY/CONCLUSIONS 6-1
7.0 REFERENCES 7-1

Tables

Table 2-1—Example Table of Initiating Events Selection for at Power 2-41
Table 2-2—Example U.S. EPR Initiating Event List 2-42
Table 2-3—Example U.S. EPR PRA Component Failure Database 2-43
Table 2-4—Example Table of Failure Data Comparison 2-44
Table 2-5—Example Common Cause Failure Data Comparison 2-45
Table 2-6—Example U.S. EPR System Dependency Matrix 2-46
Table 2-7—SPAR-H Dependency Formula 2-47
Table 3-1—Example U.S. EPR Spatial Database 3-8
Table 4-1—Example U.S. EPR Plant Operating States 4-5

Figures

Figure 2-1—Safety Injection Systems 2-48
Figure 2-2—RCS Safety and Severe Accident Depressurization Valves 2-49
Figure 2-3—Severe Accident Heat Removal System 2-50
Figure 2-4—Diverse Architecture of a Single Division 2-51
Figure 2-5—Arrangement of the Reactor Trip Breakers 2-52
Figure 2-6—Pre-Accident HEP Evaluation 2-53
Figure 2-7—Post-Accident Time Window 2-54
Figure 2-8—SPAR-H Dependency Rating System 2-55
Figure 3-1—Example of U.S. EPR Arrangement of Buildings 3-9
Figure 3-2—Safety Systems Spatial Allocation 3-10

Nomenclature

Acronym	Definition
AC	Alternating Currant
ALU	Actuator Logic Unit
ALWR	Advanced Light Water Reactor
APU	Acquisition and Processing Unit
ASEP	Accident Sequence Evaluation Program
ATWS	Anticipated Transient Without Scram
BTP	Branch Technical Position
CBDTM	Cause-Based Decision Tree Method
CCF	Common Cause Failure
CCW (S)	Component Cooling Water (System)
CDES	Core Damage End State
CDF	Core Damage Frequency
CET	Containment Event Tree
CFR	Code of Federal Regulations
CPM	Conditional Probability Matrix
CRDM	Control Rod Drive Mechanism
CVCS	Chemical and Volume Control System
DBA	Design Basis Accident
DC	Direct Current
DCA	Design Certification Application
DCD	Design Control Document
DNBR	Departure from Nucleate Boiling Ratio
EBS	Extra Borating System
EDG	Emergency Diesel Generator
EFW	Emergency Feedwater
EOP	Emergency Operating Procedure
EPRI	Electric Power Research Institute
ESD	Event Sequence Diagram

Acronym	Definition
ESF	Engineering Safety Feature
ESFAS	Engineered Safety Features Actuation System
ESW (S)	Essential Service Water (System)
ET	Event Tree
EUR	European Utility Requirements
FCD	Fast Cooldown
FLBI	Feedwater Line Break Inside Containment
FLBO	Feedwater Line Break Outside Containment
FMEA	Failure Modes and Effects Analysis
FW	Feedwater
GTR	General Transient
HCLPF	High Confidence Low Probability Failure
HCR	Human Cognitive Reliability
HEP	Human Error Probability
HFE	Human Failure Events
HRA	Human Reliability Analysis
HVAC	Heating, Ventilation, and Air Conditioning
I&C	Instrumentation and Controls
IRWST	In-containment Refueling Water Storage Tank
ISLOCA	Interfacing System Loss of Coolant Accident
LERF	Large Early Release Frequency
LHSI (S)	Low Head Safety Injection System
LLOCA	Large Break Loss of Coolant Accident
LMFW	Loss of Main Feedwater
LOC	Loss of Condenser Heat Sink
LOCA	Loss of Coolant Accident
LOOP	Loss of Offsite Power
LPSD	Low Power Shutdown
LRF	Large Release Frequency
MAAP	Modular Accident Analysis Program

Acronym	Definition
MCR	Main Control Room
MCS	Minimum Cut Set
MFW (S)	Main Feedwater (System)
MGL	Multiple Greek Letter
MHSI (S)	Medium Head Safety Injection (System)
MLOCA	Medium Break LOCA
MOV	Motor Operated Valve
MS (S)	Main Steam (System)
MSB	Main Steam Bypass
MSIV	Main Steam Isolation Valve
MSRCV	Main Steam Relief Control Valve
MSRIV	Main Steam Relief Isolation Valve
MSRT	Main Steam Relief Train
MSRV	Main Steam Relief Valve
MSSV	Main Steam Safety Valve
MTTR	Mean Time-to-Repair
NSM	Non-Self-Monitored
NSSS	Nuclear Steam Safety System
ORE	Operator Reactor Experiment
PAS	Process Automation System
PC	Personal Computer
PCD	Partial Cooldown
PE	Phenomenological Evaluation
PGA	Peak Ground Acceleration
POS	Plant Operating States
PRA	Probabilistic Risk Assessment
PS	Protection System
PSF	Performance Shaping Factor
PSV	Pressurizer Safety Valve
PWR	Pressurized Water Reactor

Acronym	Definition
RC	Release Category
RCM	Release Category Matrix
RCP	Reactor Coolant Pump
RCS	Reactor Coolant System
RCCA	Rod Cluster Control Assembly
RCSL	Reactor Control, Surveillance and Limitation
RELAP	Reactor Excursion and Leak Analysis Program
RHR (S)	Residual Heat Removal (System)
RPS	Reactor Protection System
RPV	Reactor Pressure Vessel
SADV	Severe Accident Depressurization Valve
SAHR (S)	Severe Accident Heat Removal (System)
SAMDA	Severe Accident Mitigation Design Alternative
SAS	Safety Automation System
SBO	Station Blackout
SCWS	Safety Chilled Water System
SEL	Seismic Equipment List
SFP	Spent Fuel Pool
SG	Steam Generator
SGTR	Steam Generator Tube Rupture
SHARP	Systematic Human Action Reliability Procedure
SI	Safety Injection
SIS	Safety Injection System
SLBI	Steam Line Breaks Inside Containment
SLBO	Steam Line Breaks Outside Containment
SLOCA	Small Break LOCA
SM	Self-Monitored
SNL	Sandia National Laboratory
SPAR-H	Standardized Plant Analysis Risk – Human Reliability Analysis
SSC	Systems, Structures, and Components

Acronym	Definition
SSE	Safe Shutdown Earthquake
SSS	Start-up and Shutdown System
SSSS	Stand-Still Seal System
THERP	Techniques for Human Errors Rate Prediction
TXP	TELEPERM XP
TXS	TELEPERM XS
UHS	Ultimate Heat Sink
UPS	Uninterruptible Power Supply

1.0 INTRODUCTION

Title 10, Part 52, of the Code of Federal Regulations (CFR) (Reference 1) requires that an applicant for a design certification submit a comprehensive Probabilistic Risk Assessment (PRA). To satisfy this requirement, AREVA NP is performing a Level 3 PRA to support the U.S. EPR design certification. The design certification PRA is being developed in parallel with the ongoing U.S. EPR design development.

Development of the U.S. EPR PRA has benefited from European experience and from the sharing of technology through international cooperation among the AREVA regions. Preliminary PRA insights have influenced the design both in Europe and in the U.S.

This PRA Methods Report provides an overview of the scope, objectives, basic approach, methodology, and computer codes to be employed in the design certification PRA.

1.1 *PRA Scope and Objectives to Support Design Certification*

The AREVA NP probabilistic design objectives for the U.S. EPR are:

- Core Damage Frequency $<10^{-5}$ per year
- Large Release Frequency $<10^{-6}$ per year

These probabilistic design objectives include internal and external events, excluding sabotage and seismic events, and are consistent with NRC objectives defined in SECY 90-016 (Reference 2).

The scope of the U.S. EPR design certification PRA includes the following:

- Level 1—Core Damage Frequency (CDF)
- Level 2—Large (and Large Early) Release Frequency (LRF/LERF)
- Level 3—Offsite Dose Consequence

The scope of initiating events considered in the PRA for design certification includes:

- Internal Events—at power and low power shutdown (LPSD)
- External Events—includes evaluation of the following:
  - Internal flood events and internal fire events for at power and LPSD conditions
  - Seismic (PRA-based margins) assessment for at power and shutdown conditions
  - Other external hazards (e.g., high winds and tornado) are addressed qualitatively.

The approach to the design certification PRA is summarized as follows:

- During the design certification phase, the PRA is being developed in parallel with design development activities. When specific detailed design information is not available, bounding, as close-to-realistic, assumptions are used.
- Consider the guidance in Regulatory Guide 1.200 (Reference 3) and Regulatory Guide 1.174 (Reference 4), as applicable to design certification. AREVA NP will continue to monitor and, as applicable, implement nuclear industry consensus standards and good practices regarding PRA methods.
- Advantage will be taken of initial technical development and risk insights gained from the AREVA European EPR design process and PRA development, including component failure data, as applicable to design certification.

The objectives of the design certification PRA are to:

- Meet regulatory requirements for U.S. design certification.
- Demonstrate the robustness of the U.S. EPR design and that the design satisfies the AREVA NP design objectives and NRC probabilistic safety objectives with margin.

- Provide a useful tool to support design decision making to further enhance plant safety (e.g., Design Reliability Assurance Program and Severe Accident Mitigation Design Alternatives) and to support developments of risk-informed programs.

1.2 *Design Features Contributing to Risk Reduction*

The U.S. EPR is a 4590 MWt evolutionary pressurized water reactor (PWR) that incorporates proven technology with innovative system configurations to enhance safety. The EPR was originally developed through a joint effort between Framatome ANP and Siemens KWU in the 1990s by incorporating key technological and safety features from the French and German reactor fleets. The U.S. EPR version has been adapted to conform to U.S. codes, standards, and regulatory requirements. The design features that contribute to the plant's low CDF and LRF are listed below.

- Safety system redundancy and independence
- Separation and physical protection of safety systems for internal and external hazards
- Capabilities to mitigate severe accidents
- State-of-the-art digital instrumentation and controls (I&C)
- Use of active components and technology with proven reliability, as demonstrated by the current operating fleet

More details about the systems, structures, and components (SSC) that play a role in these features are provided throughout this report.

1.3 *AREVA EPR/PRA International Cooperation*

The U.S. EPR design development and probabilistic evaluation of its design features has benefited as a result of international cooperation between the U.S. and European divisions of AREVA. This cooperation has led to the sharing of PRA experience and technology through technical review meetings, independent reviews, and collaborative

work assignments. This technical exchange has led to greater understanding of the PRA scope, methods, data, and regulatory requirements among the different AREVA regions. Although the EPR PRAs in the U.S. and Europe are in progress, this interaction has helped development of the U.S. EPR PRA models and provides added assurance that the U.S. EPR PRA approach is technically adequate, uses mature PRA techniques, and is sufficient to meet the PRA objectives for design certification.

1.4 *PRA Technical Adequacy and Quality*

The U.S. EPR PRA is developed considering guidance from Regulatory Guide 1.200 (Reference 3) and Regulatory Guide 1.174 (Reference 4), as applicable to design certification. In general, the AREVA NP approach is to use bounding, as close-to-realistic, assumptions as necessary when specific detailed design information is not available. This approach is consistent with regulatory guidance.

The PRA is being developed and continuously reviewed to reflect the latest plant design configuration. The PRA discipline is integrated into the on-going design process via the AREVA NP U.S. EPR project design directive and design change process. The design certification phase PRA will include an input freeze date, and any design changes made after the freeze date will be evaluated qualitatively for potential impact on the PRA.

The AREVA NP approach ensures technical adequacy of the PRA in that:

- The PRA model will represent the state of plant design at the time of design certification.
- The models will be developed consistent with industry good practice.
- The PRA models and assumptions will be reasonable, bounding, relevant to the PRA purpose, and supported through appropriate sensitivity studies.

PRA quality approach is demonstrated through the use of qualified personnel, use of procedures to control development of documentation, performance of independent review and checking of calculations and information used in the PRA, procedures for maintenance of documentation, and the corrective action process.

Additionally, a formal peer review of the U.S. EPR PRA will be performed later during the detailed design phase.

1.5 *Influence of PRA on the Plant Design*

During design development in the U.S. and Europe, the preliminary PRA results and insights have been used to influence design decisions. Several examples of how the PRA has influenced the design are provided below:

- Alignment of the safety chilled water system (SCWS) to provide cooling of the low head safety injection (LHSI) pumps for trains 1 and 4. This reduces the LHSI dependence on the component cooling water (CCW) and essential service water (ESW) systems.
- Improvement of the reliability of the safety injection system (SIS) automatic response at mid-loop conditions by adding diverse signals to auto-start medium head safety injection (MHSI) on low reactor coolant system (RCS) loop level or low suction pressure to the residual heat removal (RHR) pumps.
- Improved redundancy and reliability of the cooling system for the severe accident heat removal system (SAHRS) by providing two CCW/ESW divisions, each dedicated to the cooling of the associated SAHRS train. This eliminated the SAHRS dependence on divisions 1 and 4 of the CCW/ESW systems.

2.0 INTERNAL EVENTS PRA METHODOLOGY

2.1 *Level 1 Accident Sequence Evaluation and Success Criteria*

2.1.1 *Selected Initiating Events*

The objective of the accident sequence evaluation is to identify, group, and quantify U.S. EPR responses to different initiating events. These initiating events are the starting point for analyzing accident sequences and quantifying risk.

The development of initiating events is performed in the following stages:

- Identify a set of events that could cause a disturbance in the plant operating conditions and result in a plant trip.
- Group events that result in similar impacts and require the same system and operator responses to bring the plant to a safe condition.
- Quantify the expected frequency of occurrence for each initiator or initiator group.

To identify initiating events that could challenge U.S. EPR power operation, the following process is used:

- Numerous sources are reviewed to identify an initial list of potential initiating events, including NUREG/CR-5750 (Reference 5), the Advanced Light Water Reactor (ALWR) Utility Requirements Document (Reference 6), and U.S. EPR safety analysis information as it is developed. Table 2-1 contains an example list of initiating events selected for evaluation.
- U.S. EPR specific systems are evaluated using a failure modes and effects analysis (FMEA) approach to identify plant-specific system initiators and their impacts on plant operation.
- Pipe break initiators (e.g., loss of coolant accidents, steam generator tube ruptures, secondary piping breaks [feed and steam line breaks]) are evaluated from a plant-specific perspective and are included in the initiating event list.

- A systematic evaluation of potential loss of coolant accidents (LOCA) outside containment is conducted, and applicable events are evaluated as initiating events.

Internal initiating events selected for analysis are grouped into the following accident/event categories:

- Transient
- LOCA
- Steam Generator Tube Rupture (SGTR)
- Secondary System Line Break (steam line and feed line)
- Support System Failures (including loss of offsite power)
- LOCA Outside Containment
- Anticipated Transients Without Scram (ATWS)

Discussion of these accident/event categories is provided in the following sections.

2.1.1.1 *Transients*

Transient initiating events are combined into broad categories based on the availability of balance of plant systems credited in the accident sequence analysis (e.g., the main feedwater system, the condenser, the startup and shutdown system). The transient initiators are summarized below:

- General Transient (GTR)—This category includes events that result in automatic or manual reactor trip, but do not result in the direct unavailability of balance of plant equipment to provide secondary cooling after the plant trip. Typical events in this category include turbine trip, manual trip, loss of RCS flow, and rod drop. These events are modeled as a turbine trip.
- Loss of Condenser Heat Sink (LOC)—This category includes transient initiating events resulting in the unavailability of the main condenser as a heat sink.

Typical events in this category include inadvertent closure of the main steam isolation valves (MSIV) and loss of condenser vacuum.

- Loss of Main Feedwater (LMFW)—This category includes a complete loss of all main feedwater (MFW). Typical events in this category include loss of feedwater (FW) from various causes (e.g., low suction pressure or malfunction of all FW control valves).

2.1.1.2 *Loss of Coolant Accidents*

LOCA events inside containment are defined as RCS inventory losses with rates beyond the makeup capability of the charging system. LOCA events are grouped into three break size categories (i.e., small, medium, and large). The preliminary basis for break size division and corresponding differences in accident mitigation requirements are summarized below.

LOCA Size	Secondary Cooling	Inventory Control
Small Break	Required for 24-hour mission	One MHSI train with partial cooldown*
Medium Break	Only SG inventory required	One MHSI train with partial cooldown*
Large Break	Not required	One LHSI train

- The break size for a small break LOCA (SLOCA) initiating event is defined as a break large enough to exceed the normal chemical and volume control system (CVCS) charging flow, but not large enough that the flow through the break could provide for decay heat removal. Therefore, secondary cooling via the steam generators is required throughout the 24-hour mission time. RCS inventory control is provided by one of four MHSI trains in conjunction with successful partial cooldown (PCD). The preliminary lower bound break size is equivalent to approximately 0.6-inch diameter.

* Partial cooldown is described further in Section 2.1.2.2

- The break size for a medium break LOCA (MLOCA) initiating event is defined as a break large enough that FW supply is not required for accident mitigation. Thus, only the initial steam generator inventory is credited for secondary heat removal. RCS inventory control is provided by one of four MHSI trains in conjunction with successful partial cooldown. The preliminary lower bound break size is equivalent to approximately 3-inch diameter.
- The lower bound break size for a large break LOCA (LLOCA) initiating event is defined as a break large enough that the RCS depressurization through the break is fast enough to allow one of four LHSI pumps to successfully maintain core cooling. No secondary cooling is required. The preliminary lower bound break size is equivalent to approximately 6-inch diameter.
- The upper bound break size for an LLOCA would be a double-ended break of one of the four RCS loops, over 30 inches in diameter. Reactor vessel rupture events are not explicitly included in the model, but they will be addressed qualitatively.

In addition to pipe break LOCAs, the following loss of coolant events are also addressed:

- Reactor coolant pump (RCP) seal LOCA as an initiating event is not explicitly modeled because its frequency and impact are assumed to be bounded by the SLOCA frequency. However, the RCP seal LOCAs are modeled as a result of transients with loss of seal cooling (e.g., loss of CCW/ESW or loss of offsite power).
- Spurious operation of a pressurizer safety valve (PSV) is assumed to be included in the SLOCA frequency. Opening of a PSV requires operation of two solenoid pilot valves powered by two different electrical trains. The pressurizer safety valve is designed to fail closed on loss of power to either solenoid.

2.1.1.3 *Steam Generator Tube Ruptures*

An SGTR resulting in primary coolant leakage into the secondary side of the steam generator (SG) is similar to an SLOCA, except there are no containment indications of the event. If the secondary side is not isolated and pressure controlled, the SG can overfill, and RCS leakage can escape to the environment. The U.S. EPR SGTR mitigating strategies are designed to minimize the likelihood of a radioactive release through the main steam relief valve (MSRV) or the main steam safety valves (MSSV) of the affected SG. The MHSI pumps have a design shutoff pressure of approximately 1400 psig, which is below both the MSSV setpoint and the upper MSRV setpoint, which is set automatically on a high SG level.

2.1.1.4 *Secondary System Line Breaks*

The secondary line break analysis applies to those secondary line breaks that are large enough to initiate secondary side isolation and safety injection (SI) actuation. The initiating events considered are discussed below:

- Steam line breaks can occur upstream or downstream of the MSIVs. Steam line breaks inside containment (SLBI) (i.e., breaks occurring upstream of the MSIVs) cannot be isolated, and at least one SG will always blow down. These breaks are modeled as inside containment breaks. Breaks occurring downstream of the MSIVs can be isolated and are modeled as steam line breaks outside containment (SLBO). Spurious operation of an MSSV is also modeled.
- FW line breaks inside containment (FLBI) on the SG side of the containment isolation check valve are unisolable (i.e., at least one SG blows down). FLBI and SLBI are currently considered as a single initiator because the success criteria and required mitigating systems are similar. FW line breaks outside containment (FLBO) and other feed line breaks that do not directly result in loss of any SG inventory are treated as total loss of FW initiating events.
- Spurious operation of an MSRV train is not explicitly modeled as an initiating event because its impact and frequency are assumed to be bounded by

secondary system line breaks. The MSRV trains consist of a main steam relief control valve (MSRCV) (normally open) and an associated main steam relief isolation valve (MSRIV) (normally closed). A failed open MSRV train is unlikely because spurious operation of two solenoids is needed to open the MSRIV, and the solenoids fail closed upon loss of power. The MSRCVs in series with the MSRIVs can be closed to isolate a spuriously open MSRIV. Additionally, the main steam relief train (MSRT) receives a close signal on low SG pressure.

2.1.1.5 *Support System Initiators*

The following support system initiators are considered:

- Loss of Component Cooling Water/Emergency Service Water—The CCWS provides cooling to the RCPs, the CVCS pumps, and the SIS pumps. Therefore, loss of component cooling has the potential to cause a reactor trip and to degrade safety systems. Each CCWS train has its own dedicated ESW train to remove heat to the environment, and the CCWS initiating event analysis incorporates applicable ESW failure modes as appropriate. Partial losses of the CCWS are also considered as initiators, resulting in a loss of several CCW/ESW initiating events. Loss of an ultimate heat sink (UHS) is included in these events.
- Loss of Balance of Plant—The closed cooling water system removes the heat generated by components in the conventional part of the plant via the closed cooling water heat exchangers to the auxiliary cooling water system. Complete loss of the closed cooling water system will result in a turbine trip and reactor trip. The MFWS and the startup and shutdown system (SSS) are assumed to be unavailable because of loss of cooling.
- Loss of Offsite Power—The loss of offsite power (LOOP) event affects plant operations because it is assumed that the LOOP results in a complete unit trip and it also affects mitigation response by placing demands on the onsite power system.

- Loss of an Electrical Bus—Loss of single switchgear is conservatively included in the accident sequence model as an initiating event to bound electrical failures and to demonstrate that the risk from a loss of one safety train is relatively low.

2.1.1.6 *Loss of Coolant Accidents Outside Containment*

An interfacing system loss of coolant accident (ISLOCA) is a postulated loss of RCS inventory through system piping that extends outside of containment. For the U.S. EPR, an interfacing system is any fluid system that is directly connected to the RCS, and has the potential to be exposed to RCS pressure through the failure or misalignment of normally closed valves or through failure of heat exchanger tubes. The scope of the ISLOCA evaluation includes 0.6-inch diameter pipe and larger. This is because the approximate maximum RCS flow rate from a postulated 0.6-inch diameter (or smaller) break is not expected to exceed the makeup capacity of the CVCS. Several industry studies including NUREG/CR-5744 (Reference 7) and EPRI-NSAC-154 (Reference 8) have concluded that ISLOCA events within the capacity of the charging system are not significant contributors to the ISLOCA CDF.

The ISLOCA candidate systems and associated containment penetrations are reviewed based on the above criteria. ISLOCA preventive design features (i.e., in-series check valves, motor operated valves, pipe strength, control room alarms, and control room indications) are used to identify those RCS connections that are subject to further detailed evaluation. The initial systems chosen for detailed quantitative modeling include:

- Safety Injection System (LHSI\RHR, MHSI)
- CVCS (charging line, letdown line)
- CCWS (high pressure cooler, RCP thermal barrier cooling coils)

The frequency of core damage for postulated ISLOCA events is estimated as the product of two factors:

- The frequency of the ISLOCA event given the plant's preventive design features (initiating event frequency).
- The probability that the ISLOCA can be isolated, or otherwise terminated by RCS depressurization, prior to the occurrence of in-containment refueling water storage tank (IRWST) draining. Large diameter ISLOCA events (e.g., SIS discharge or suction pipe breaks) are typically assumed to result in core damage. Small diameter ISLOCA events (e.g., heat exchanger tube break) provide more time to recover via isolation or operator actions to depressurize.

2.1.1.7 *Anticipated Transients Without Scram*

Failure of reactor trip is considered in the accident sequence quantification for each initiating event requiring reactor trip. Reactor trip failure is assumed to result from three causes:

- Failure of the reactor trip signal
- Failure of the reactor trip devices
- Mechanical binding of the control rods

The primary functions required to mitigate an ATWS event are:

- Primary system overpressure protection
- Long term shutdown
- Adequate primary to secondary heat removal

Each of these functions is considered in the ATWS event tree modeling.

2.1.2 *Accident Sequences*

Initiating events trigger sequences of events that challenge plant control and safety systems whose failure could potentially lead to plant damage or large release. The

accident sequence analysis evaluates equipment and operator responses to initiating events. In the PRA model, the accident sequence analysis needs to adequately resolve the dependencies between causes of the initiating events and systems available to mitigate the consequences of these events. System responses and time required for operator actions are defined in the success criteria analysis.

Event Sequence Diagrams (ESD) are used to help document the plant response showing success paths to stable states and to document the hardware failures and human errors that could lead to core damage. In the PRA model, the ESDs are converted to Event Trees (ET) to quantify risk associated with an initiating event.

Accident sequences are binned to one of the following end states:

- Success—This is a controlled stable state with the reactor subcritical, stable water inventory, and adequate heat (power) removal.
- Core Damage—This end state is applied when success cannot be established and maintained as described above. Core damage is defined in Section 2.1.3.

The above definition of success requires that three fundamental safety functions be satisfied:

- Reactivity control to reduce heat generation
- Inventory control to remove heat from the fuel
- Heat removal to transfer heat to the environment

2.1.2.1 *Reactivity Control*

When key reactor parameters are outside their safety limits, the reactor trip system drops control rods to shut down power generation and to protect the reactor. The reactor trip system is highly reliable with numerous diverse and redundant input signals. Reactor trip system failure or an ATWS does not automatically result in core damage because other mitigating systems (e.g., boron injection) can be used to reach a stable

state. The ATWS event sequence analysis describes the mitigating systems and their success criteria.

2.1.2.2 *Inventory Control*

The inventory control function removes heat from the fuel rods to the reactor coolant. This function can be challenged in a number of ways, including a LOCA initiating event or because of system failures after the initiating event (e.g., RCP seal LOCA). The SIS is needed to provide inventory control and to remove heat from the fuel to the IRWST. An SI signal is generated on low pressurizer pressure. The inventory control function could also be challenged if the secondary heat removal function is lost. In this case, operators initiate primary feed and bleed by opening the PSV.

The following systems can provide inventory makeup to the reactor vessel: MHSI, LHSI, Accumulators, CVCS, and extra borating system (EBS). Further information on these systems is described in Section 2.3.

For certain initiating events and accident sequences, inventory control is dependent on the secondary cooling portion of the heat removal function described below. For example, MHSI pump injection during an SLOCA requires a PCD using the SG MSRV function. The PCD is automatically initiated by an SI actuation signal. If all MHSI trains fail, operators would initiate fast cooldown (FCD) to allow discharge of accumulators and LHSI injection.

2.1.2.3 *Heat Removal*

The heat removal function transfers the heat from the reactor coolant to the environment. Heat removal requirements depend on the initiating event and the accident sequence.

Secondary cooling with the SGs is sufficient for transients or events where RCS integrity is maintained (no LOCA condition). This can be satisfied with one MFW pump, or one SSS pump, or one emergency feedwater (EFW) pump supplying one SG with steam relief to the main condenser through the main steam bypass (MSB) or to

atmosphere through one MSRV. Further information on the MSRV/MSSV trains is provided in Section 2.3.

If secondary cooling is unsuccessful, the operators initiate primary feed and bleed cooling. Primary bleed is initiated through the PSVs or severe accident depressurization valves (SADV), and feed is provided by the CVCS or an SI train. The heat transferred to primary containment is removed by IRWST cooling. LHSI trains with heat exchangers or the SAHRS provide IRWST heat removal function.

2.1.3 *Success Criteria*

To satisfy success in the Level 1 PRA model, each accident sequence must maintain a safe stable state for 24 hours (i.e., a 24-hour mission time is used; specific sequences may require longer term heat removal). Sequences that do not meet the success criteria are binned to a core damage end state (CDES).

Core damage is defined as uncovery and heat up of the reactor core to the point that prolonged oxidation and severe fuel damage involving a large fraction of the core is anticipated.

Computer codes MAAP4 and S-RELAP5 are used to determine and justify Level 1 (core damage) success criteria for the at-power PRA. These computer codes are described further in Section 5.0.

For most transient and LOCA events, the success criteria for not achieving core damage is that the peak cladding temperature is less than 2200°F. This is consistent with the ASME PRA Standard (Reference 9). For ATWS events, RCS overpressure greater than 130% of design pressure is used as a determination of core damage. For LPSD; the time to core damage is conservatively derived based on the time to uncover the core.

2.2 *Data and Common Cause Failure Analysis*

2.2.1 *Sources of Initiating Event Data*

The U.S. EPR PRA uses the following sources for the development of initiating event frequencies:

- NUREG/CR-5750 (Reference 5) documents the initiating event experience for U.S. nuclear power plants. This source was used for the GTRs, secondary line breaks, and all LOCAs except ISLOCAs (which were calculated using fault tree analysis).
- NUREG/CR-6890 (Reference 10) reflects the LOOP data from 1986-2004 (including the 2003 major grid related events), and is a current source of operating experience for LOOP.
- Fault tree analysis is used to calculate the initiating event frequencies for the support system failure initiating events. This method is also used to calculate the initiating event frequencies for ISLOCAs.

Table 2-2 provides information on the sources of initiating events for the U.S. EPR.

2.2.2 *Sources of Component Failure Data*

The U.S. EPR PRA uses component failure data from a number of generic sources to characterize the failure probabilities of the U.S. EPR components. The component failure data sources include:

- "Generic Component Failure Database for Light Water and Liquid Sodium Reactor PRAs," EGG-SSRE-8875 (Reference 11). This report serves as a source for most of the basic event data for plant mechanical and electrical components.
- "Centralized Reliability and Events Database of Reliability Data for Nuclear Power Plant Components," ZEDB Analysis for 2002 (Reference 12). This data source includes all German nuclear plants, Dutch Unit Borssele, and Swiss Unit

Goesgen. This source is used to take advantage of the European operating experience with the components that are part of the basic U.S. EPR design.

- "European Industry Reliability Data Bank," EIReDA95 (Reference 13). This source is used for a limited number of the components (e.g., safety relief valves).

An example of the component failure data used in the U.S. EPR PRA is shown in Table 2-3.

2.2.3 *Common Cause Component Groups and CCF Parameters*

Modeling of common cause failures (CCF) is based on the methods presented in NUREG/CR-5485 (Reference 14). The following principles are used in modeling CCF:

- Intra-system CCF is modeled for identical, non-diverse, active components. Independence is assumed for components of diverse design or function.
- Inter-system CCF is generally not modeled based on a high level review and current state of knowledge for component design, maintenance, and testing. The exception to this approach is the modeling of IRWST sump strainers CCF to capture the common impact of potential debris blockage events.

The CCF values used in the U.S. EPR PRA are based on NUREG/CR-6819 (Reference 15).

2.2.4 *Comparison to Other Sources*

The sources of data were compared with widely accepted U.S. data sources such as the NUREG/CR-5500 (Reference 16) and NUREG-1715 (Reference 17) series of studies, and the Electric Power Research Institute (EPRI) ALWR Database (Reference 6). A sample of this comparison is shown in Table 2-4. This analysis shows that the U.S. EPR data is comparable to the widely accepted U.S. data sources.

Table 2-5 provides an example comparison of the CCF European data to the U.S. EPR PRA CCF data. The European data used the generic European Utility Requirements (EUR) Beta factors, which were converted to Multiple Greek Letter (MGL) CCF values

identical for all components, while the U.S. EPR PRA uses the component specific values available in NUREG/CR-6819 (Reference 15).

2.3 *PRA Systems Analysis*

2.3.1 *Description of U.S. EPR Systems in the PRA*

A brief description of the U.S. EPR major front line systems and support systems that are modeled in the PRA is provided below. Additional information on the U.S. EPR is provided in Reference 18. A description of the PRA modeling of the digital I&C system is provided in Section 2.3.2. It is noted that the following system descriptions are subject to change, and the final design information will be provided in the Design Certification Application (DCA).

2.3.1.1 *U.S. EPR Systems for Inventory Control*

Medium Head Safety Injection System

The MHSI system PRA-credited function is to provide RCS inventory makeup to ensure adequate core heat transfer for events that result in a loss of RCS inventory. The MHSI system consists of four 100% capacity, independent trains that are physically separated and protected within their respective safeguard buildings. The MHSI system takes suction from the IRWST. A schematic of the MHSI system is shown in Figure 2-1.

The MHSI pumps have a design shutoff pressure of approximately 1400 psig. For certain initiating events and accident sequences involving RCS pressure above MHSI shutoff pressure, MHSI is dependent on the secondary cooling portion of the heat removal function via the SGs and MSRVs for RCS depressurization. For example, an SG PCD is required for MHSI injection during an SLOCA. The PCD signal is automatically initiated by an SI signal.

Low Head Safety Injection/Residual Heat Removal System

The LHSI/RHR system PRA-credited function is to provide RCS inventory makeup to ensure adequate core heat transfer for events that result in low RCS level/inventory.

The PRA also credits LHSI/RHR to remove heat from IRWST during accidents and to support LPSD conditions. The LHSI system consists of four 100% capacity trains that are protected within their respective safeguard buildings. Under normal conditions, all four trains are separate and independent. For maintenance purposes, the capability exists to connect the discharge lines of train one to train two and of train three to train four. Divisional CCW/ESW trains remove heat from the LHSI/RHR system. The LHSI system takes suction from the IRWST. A schematic of LHSI/RHR is shown in Figure 2-1.

Accumulators

The PRA-credited function of the accumulators is to inject water into the RCS for loss of inventory events. There are four accumulators (one for each cold leg) that automatically inject their contents when RCS pressure is below approximately 600 psig. The accumulators are shown in Figure 2-1.

In-Containment Reactor Water Storage Tank

The PRA-credited function of the IRWST is to provide a source of borated water for MHSI and LHSI in the event of loss of RCS inventory and for containment heat removal and core melt cooling in the event of a severe accident. The IRWST is a single tank, integral to the containment structure. The IRWST is located at a low point in the containment, and water discharged from the RCS into containment will drain back into the IRWST. The IRWST eliminates the need to actively transfer MHSI/LHSI pump suction to the containment sump for long term recirculation. The IRWST is shown in Figure 2-1.

Extra Borating System

The EBS consists of two pumps with limited flow capacity. The PRA-credited EBS function is to provide emergency boration of the RCS during events that require negative reactivity insertion. The EBS pumps are located in the Fuel Building.

Chemical Volume Control System

The CVCS consists of two pumps with limited flow capacity. The PRA-credited function of the pumps is to provide high pressure injection for small leaks that are within the CVCS makeup capacity. The CVCS pumps are located in the Fuel Building.

RCP Stand-Still Seal System

In addition to the normal multi-stage RCP shaft seal, each RCP is equipped with a stand-still seal system (SSSS) to provide backup seal capability. The SSSS is deployed pneumatically when the associated RCP shaft stops rotating. This added seal protection reduces the likelihood of an RCP seal LOCA-type event during scenarios caused by simultaneous loss of seal support systems (i.e., loss of barrier cooling [provided by CCW] and seal injection [provided by CVCS]).

2.3.1.2 *U.S. EPR Systems for Secondary Heat Removal*

Main Feedwater System

The PRA-credited function for the MFWS is to provide SG inventory makeup for those events that require secondary heat removal via the SGs. The MFW is equipped with four electric motor-driven MFW pumps, which take suction from the FW tank. Each MFW pump is capable of handling approximately 33% of the full power load. Normally, three MFW pumps are operating to support full power plant operation. The MFWS is located in the Turbine Building.

Startup and Shutdown System

The PRA-credited function for the SSS is to provide SG inventory makeup for events that require secondary heat removal via the SGs, including support of the RCS PCD and FCD functions. The SSS consists of a single electric motor-driven pump, which takes suction from the FW tank. The SSS pump feeds the SGs via the low flow FW control valve or the low-low flow FW control valve depending on plant conditions. The SSS is located in the Turbine Building.

Emergency Feedwater System

The PRA-credited function for the EFW system is to provide SG inventory makeup for events that require secondary heat removal via the SGs, including the RCS PCD and FCD functions. Each SG has a dedicated EFW train for maintaining SG level. Each EFW train consists of an electric motor-driven pump with dedicated suction tank. The EFW pumps are interconnected via normally closed motor operated valves (MOV); therefore, any EFW train can be connected to any SG or suction tank. EFW discharges to the SGs independently of the MFW piping. The EFW trains are physically separated and protected within their respective safeguard buildings.

Main Steam System

The PRA-credited function for the main steam system (MSS) is to provide secondary heat removal by discharging steam to the main condenser, or to atmosphere, via the MSRV train or the MSSV. Each SG is connected to a common header to the main condenser via an MSIV and is equipped with one MSRV train and two MSSVs, which discharge to atmosphere. The MSRV trains are credited in the PRA to perform the RCS PCD and FCD functions to support the MHSI and LHSI functions. SG isolation is also modeled for SG tube rupture events and secondary side breaks.

Pressurizer Relief System

The PRA-credited functions for the RCS pressurizer relief system are to: protect the RCS from overpressure events; reduce RCS pressure in support of feed and bleed operations; and perform RCS depressurization during a severe accident to prevent RCS failure at high pressure. The U.S. EPR is equipped with three PSVs and two severe accident depressurization lines. The severe accident depressurization lines consist of two parallel trains, each line has two SADVs in series: a depressurization valve (globe valve) and an isolation valve (gate valve). The PSVs and SADVs are shown in Figure 2-2.

Severe Accident Heat Removal System

The PRA-credited functions for the SAHRS are to provide cooling of the IRWST water as a backup to LHSI/RHR during accident conditions and to provide heat removal/spray of the containment space to prevent containment overpressure. The SAHRS is a dedicated containment heat removal system that consists of two trains. The primary operating modes of the SAHRS include:

- Active recirculation cooling of the IRWST
- Active spray for environmental control of the containment atmosphere
- Passive cooling of molten core debris
- Active recirculation cooling of the molten core debris
- Active back-flush of IRWST strainers

The SAHRS heat exchangers transfer the residual heat from containment to the UHS via dedicated CCW and ESW trains. The SAHRS trains are associated with divisions 1 and 4 and are located in Safeguards Buildings 1 and 4. The general configuration of a single SAHRS train is provided in Figure 2-3.

2.3.1.3 *U.S. EPR Support Systems*

Alternating Current Electrical Distribution System

The PRA-credited function for the alternating current (AC) electrical distribution system is to provide AC electrical power to the frontline and support systems from both offsite and onsite power sources. This is accomplished through the distribution system consisting of switchgear buses, motor control centers, and uninterruptible power supplies (UPS). There are four independent AC electrical divisions that support the safety train divisions. Each division is located within a separate safeguards building.

Direct Current Electrical Distribution System

The PRA-credited function for the direct current (DC) electrical distribution system is to provide divisional DC electrical power to the frontline and support systems from the

associated division's DC battery. Each safety division is equipped with a dedicated, Class 1E battery with redundant battery chargers. The divisional batteries are designed for a discharge of two hours based on the necessary loading of the batteries. The U.S. EPR also includes a separate non-class 1E UPS system for severe accident management. This system consists of redundant batteries designed for twelve hours discharge.

Emergency Diesel Generators

The PRA-credited function for the emergency diesel generators (EDG) is for each EDG to independently provide onsite AC electrical power to its associated electrical division should the normal offsite power source become unavailable. There are four EDGs, each dedicated to an electrical division. The EDGs are located in two separate diesel buildings; these buildings are spatially separated on the plant site. The EDGs are also physically separated within the diesel buildings.

Station Blackout Diesel Generators

The PRA-credited function for each station blackout (SBO) diesel generator is to provide an independent and diverse power source to its associated electrical division. The standard U.S. EPR is designed with two SBO diesel generators to supply power to plant loads in the unlikely event of a LOOP with failure of all EDGs (SBO-type event). The SBO diesels are associated with train divisions 1 and 4 and are manually started and aligned to the respective bus from the main control room (MCR) or can be started locally. The SBO diesels are independent and diverse of the EDGs based on consideration of attributes (e.g., different capacity rating, different manufacturer, different controls, different location). The standard U.S. EPR design has two SBO diesels; however, other alternate AC sources may be considered on a site-specific basis.

Essential Service Water System and Ultimate Heat Sink

The PRA-credited function for the ESW system is to remove reactor heat and heat generated by equipment/components during normal operating conditions, transients,

and accidents. The ESWS supplies water to the CCWS heat exchangers and consists of four independent trains. The UHS design configuration for the U.S. EPR includes mechanical draft cooling towers; however, site-specific conditions may require alternative designs for the UHS.

Component Cooling Water System

The PRA-credited function for the CCW system is to remove reactor heat and heat generated by equipment/components by circulating water through the various heat loads and the CCW heat exchangers to transfer heat to the ESW system. The CCW system consists of four trains located within their associated safeguards building.

Safeguard Buildings Ventilation Systems

The PRA-credited function for the safeguards buildings ventilation system is to remove heat generated by operation of equipment and components. The safeguards buildings ventilation system is cooled via the SCWS.

Safety Chilled Water System

The PRA-credited function for the SCWS is to remove heat generated by equipment, components, and the safeguards buildings ventilation system. Two divisions of safety chilled water are cooled via the CCWS, and two divisions are air cooled. The SCWS trains are located in the safeguards buildings.

2.3.1.4 *U.S. EPR System Dependency Analysis*

Support system dependent failures are explicitly captured in the PRA model via the fault tree linking approach. Support system dependencies are identified and documented within the systems analysis for each mitigating system. In addition, a dependency matrix is generated and used as a tool to provide proper translation and modeling of dependent systems, and to help demonstrate the independence of the U.S. EPR train divisions. Table 2-6 is an example system dependency matrix for the U.S. EPR PRA.

2.3.2 *U.S. EPR Digital I&C PRA Model*

The protection system (PS) performs the functions that are needed to bring the plant to a controlled state following a design basis event. These functions include automatic initiation of reactor trip and actuation of engineered safety features (ESF). The PS uses the AREVA TELEPERM XS (TXS) safety-related I&C platform; which is a digital I&C technology that has been used in European reactor protection systems (RPS) and engineered safety features actuation systems (ESFAS) for over ten years.

The PS is modeled in detail in the PRA and is discussed in further detail in Section 2.3.2.1. The PS is modeled to the level of detail of the rack-mounted TXS modules; this level of detail also corresponds to the acquisition of failure data for the TXS components that are in world-wide service.

There are other I&C systems that are not modeled in detail in the PRA. This includes the operational plant control system known as the reactor control, surveillance and limitation (RCSL) system. The RCSL system implements automatic, manual, and monitoring functions needed to control and limit certain reactor core, RCS, and nuclear steam safety system (NSSS) parameters. The RCSL system restores normal operating conditions, via actions such as runback of power, to prevent challenging of the protection system. Experience with similar systems in Europe indicates that the RCSL system reduces reactor trips.

In addition to RCSL, there is also the safety automation system (SAS), which controls certain safety-related support systems, such as CCW and ventilation, and the process automation system (PAS), which controls non-safety-related systems. The PAS also contains some backup functions for reactor trip and actuation of ESF that are implemented using diverse hardware technology and diverse software. The SAS and PAS are modeled with conservative reliability until design details are available later in the detailed design process.

2.3.2.1 *Protection System General Description*

The PS has a fourfold redundant structure; each redundancy is allocated to a different electrical division and is located in a different safeguard building.

Each PS division is separated into two independent subsystems of functional diversity: subsystem A and subsystem B. There is no communication between the subsystems. Each protection function initiating a reactor trip is assigned to one specific PS subsystem. For initiating events that require reactor trip, there is a primary trip signal and a diverse backup trip signal. The parameters and sensors used to actuate the backup signal are different from the ones that actuate the primary signal.

The safety functions are distributed between the subsystems; if the main initiation signal is processed in subsystem A (or B), a second initiating signal is provided in subsystem B (or A). For ESF actuation, diverse functions (e.g., EFW and SIS actuation) are placed in different subsystems.

Figure 2-4 illustrates the functionally diverse architecture of a single division. Some of the key components of the system are shown in this simplified sketch. The processing of the PS safety functions are distributed among several specialized units—each unit consisting of a subrack with its own computer processor and supporting modules (e.g., input modules and output modules) and their interconnections. The acquisition and processing units (APU) acquire the sensor signals and perform their processing (e.g., as signal validation or threshold detection). Each APU of a subsystem is connected to the actuator logic unit (ALU) of the same subsystem in the four divisions (i.e., each ALU receives data from APUs in the four divisions). The number of APUs per subsystem varies depending on the number of processed signals. Dedicated fiber optic networks are used between the APUs and ALUs, so that a failure within one ALU or APU that might lead to a failure of the associated networks will not impact the redundant communications.

The ALUs perform voting and actuation management (discussed below for ESF actuation and reactor trip). There are two redundant ALUs per subsystem per division. The outputs from the two redundant ALUs are combined as follows:

- The reactor trip order is a de-energized-to-actuate order. To protect against spurious reactor trip, the reactor trip order is generated from the two ALUs connected in a functional AND logic configuration. The output from the two functionally diverse subsystems is combined in a functional OR logic configuration before being sent to diverse reactor trip devices. Further discussion of trip devices is provided in Section 2.3.2.2.
- ESF actuation orders are energized-to-actuate orders. ESF actuation orders are generated within a subsystem by the two redundant ALUs connected in a functional OR logic configuration. Actuators dedicated to each device are driven either by subsystem A or subsystem B, depending upon the function.

2.3.2.2 *Reactor Trip Devices*

There are three diverse sets of trip devices that can independently trip the control rods. The control rods are supplied from two independent power sources; either can maintain control rod function. There are four normally-closed reactor trip breakers. The trip breakers interrupt the power supply in case of a reactor trip order from the PS. For this function, two trip breakers are connected in series in each power supply. Two are located in division 2 (connected in series) and are tripped by divisions 1 and 2 of the PS respectively. The other two are located in division 3 (connected in series) and are tripped by divisions 3 and 4 of the PS. Therefore, the coincidence logic of the breakers for reactor trip is one-out-of-two-twice logic. Figure 2-5 shows the arrangement of the reactor trip breakers.

Contactors that also function to interrupt the power supply to the control rods are diverse from the trip breakers, and located in different divisions (divisions 1 and 4) than the breakers. The normally-energized contactors are opened by orders from the PS. There are 23 sets of 4 contactors; each set supplies power to four rod cluster control

assemblies (RCCA) (except for one set that supplies power solely to the central RCCA). Each set of 4 contactors is connected in a 2-of-4 circuit; each contactor within a set is actuated by one PS division. Figure 2-5 shows the arrangement of the contactors.

There is an additional trip method that is not shown in Figure 2-5. Specifically, the control rod drive mechanism (CRDM) power supplies contain fast-acting transistors that release power to the control rod grippers independent of the breakers and contactors. These are non-safety related devices, but are designed to trip the control rods faster than the mechanical trip devices. Because the CRDM power is de-energized before the breakers and contactors open, wear on the breakers and contactors is minimized. The transistors will trip the reactor even if there is CCF of all of the breakers and all of the contactors.

2.3.2.3 *Diversity Concept*

CCF between the diversity groups (subsystems A/B) is unlikely because the subsystems are functionally diverse (application programs and parameter/sensor inputs are different), and the subsystems are independent. Thus, no information is shared between diversity groups via network connections. The outputs of the PS are connected to diverse reactor trip devices. The ESF functions are also divided between the diverse subsystems to obtain maximum functional diversity.

In addition to the functional diversity provided by the A/B subsystems within the PS and the diversity of the reactor trip devices, there is additional defense in depth provided in the I&C architecture. This includes the trip reduction features of the RCSL system, which provides control, surveillance, and limitation functions to reduce reactor trips and PS challenges, including automatic power reduction that is not credited in the PRA. In addition, backup trip and actuation functions are performed by the non-safety related I&C system (i.e., the PAS), which includes functions to satisfy the requirements of 10 CFR 50.62 (Reference 19) and additional diversity to satisfy the guidance in Branch Technical Position (BTP) HICB 19 (Reference 20). The PAS is implemented on the TELEPERM XP (TXP) platform, which provides additional hardware and software

diversity from the TXS platform. These backup trips and actuations will be considered for inclusion in the PRA when a detailed design is available.

2.3.2.4 *Component Failure Rate Data*

The failure rate data for the TXS components comes from operating history. The TXS system is a proven design with over ten years of operating history in RPS and ESFAS systems in various European plants. The main computer processor module currently has over 50 million hours of operating experience.

The data are collected at the rack-mounted module level of detail. The failure rates for the TXS components are obtained from field data and are calculated using the chi-squared distribution with a 95% confidence interval. Due to the conservative statistical treatment inherent in the chi-squared distribution, the calculated failure rates used in the PRA are conservative relative to the observed experience. The field data for the TXS components is updated on a periodic basis.

2.3.2.5 *Treatment of Fault-Tolerant Design*

The TXS hardware and software used by the PS has extensive self-testing features and fault tolerant design. The fault tolerant design of the system allows a failed unit or input to be recognized as faulted by the downstream components, which can modify their voting logic to compensate for the faulted input. For example, as faulted inputs are recognized, the coincidence can be programmed to transition from 2-of-4 to 2-of-3; then to 1-of-2, if three inputs are faulted to the safe state. These features improve the reliability of the system, and minimize the need for periodic surveillance testing.

The PRA model assumes that some percentage of the failure modes will be test-revealed rather than self-revealing. The manufacturer's data for the TXS modules also includes estimated percentages of failure modes that are self-monitored (SM) and non-self-monitored (NSM). The PRA model also breaks out these failure modes, where appropriate, using separate basic events for SM and NSM. This allows the different mathematical models built into the RiskSpectrum® PRA software to be used for

calculating the basic event unavailability. The SM failure modes are self-revealing and are modeled with the repair time unavailability model. The NSM failure modes are test-revealed and are modeled with the test interval unavailability model. The NSM failure modes, although they are typically the smaller percentage, are usually more important because they have a long mean-time-to-repair (MTTR) and represent less favorable coincidence logic than the SM failure modes.

2.3.2.6 *Software Common Cause Failure*

The software for the PS is robust, and the software development process for the TXS platform is of high quality. The software development tools and TXS operating system are mature and have been in operation for over ten years in the European RPS and ESFAS. The application software uses only qualified software modules from a quality-controlled functional block library. The software development process and architecture are described in detail in the TELEPERM XS topical report (Reference 21).

The TXS computer processors use a deterministic operating system. This is a favored software design method for embedded systems and increases the predictability of the software. The most important features of the TXS software design include a strictly cyclic processing of application software. The asynchronous operating system (meaning no real-time clock that redundant processors synchronize to) reduces CCF potential and enhances reliability. Another important feature is that only static memory allocation is used (i.e., each variable in the application program has a permanent dedicated place in memory); therefore, memory conflicts caused by dynamic memory allocation are not possible. There are also no process-driven interrupts. Other important features are bus systems with a constant load, no long-term data storage, and no use of external data storage media.

The potential for software CCFs is minimized by the high-quality software design tools, the deterministic operating system, built-in monitoring and testing, and built-in functional diversity.

In the PRA model, software failure is treated as a CCF mechanism for the computer processors. A CCF grouping is applied to the computer processors that have the same application software and inputs. A common cause group of processors is conservatively assumed to fail all of the functions that are carried by those processors.

A conservative beta-factor is applied to each CCF group. The beta factor is applied to the experience-based failure rates of the computer processors. Because the failure data for the processors are based on actual field data, they include both hardware and software causes. Software is considered a source of failure for the processors, and the processor failure rate coupled with the CCF factors adequately captures the potential software CCF contribution.

2.3.2.7 *Hardware Common Cause Failure*

CCF groups are also assigned to hardware components of the PS. CCF grouping is applied to the reactor trip devices (breakers and contactors) and to the sensor inputs to the PS. CCFs are modeled with the MGL method.

Another potential CCF included in the PS model is stuck control rods. The basis for the control rod CCF used in the U.S. EPR PRA is the CCF probability derived in Volume 11 of NUREG/CR-5500 (Reference 22). As documented in this NUREG, a control rod failure probability was calculated based upon a single control rod failure in PWR history (plus a second rod failure was assumed for uncertainty), then a CCF probability was conservatively calculated for 50% or more of the rods fail to insert (4.1E-8/demand). The calculated value is conservative because it is based on one actual failure, and the demand data is from a limited time period (1990 to 1998 for unplanned trips, 1984 to 1989 for cyclic tests). The preliminary PRA also assumes that 50% of the control rods inserted is a success. This is based on preliminary analysis for the U.S. EPR as well as several NRC sources (NUREG/CR-5500 [Reference 16], SECY-83-293 [Reference 23], NUREG-1000 [Reference 24]) that have historically defined successful scram as insertion of about 20% of the control rods, evenly spaced.

2.3.2.8 *Protection System Top Events Modeled in the PRA*

For the ESF functions, each actuated ESF device or train is treated as a separate top event and modeled explicitly. This allows the PS fault trees to be linked with the frontline system fault trees. This fault tree quantification resolves the dependencies, properly models, and correctly implements the divisional redundancy and A/B subsystem functional diversity. Important ESF functions include: EFW actuation, initiation of an SIS, closure of MSIV, opening of the MSRT, and containment isolation.

For reactor trip, initiating event-specific fault trees are not developed for each initiator because of the low probability associated with ATWS, and the extensive redundancy and diversity built into the U.S. EPR reactor trip design. Instead, representative reactor trips are modeled with a typical set of challenged parameters. This assumption is based on the PS being designed so that each postulated initiating event will challenge at least two different measured parameters for reactor trip, and that the two parameters are implemented in separate subsystems A and B. This is conservative because often there will be additional trips that will occur if the trips that are credited in the safety analysis were to fail.

One representative reactor trip top event that is modeled is a turbine trip initiating event. This is a typical reactor trip with plant parameters of high RCS pressure and high SG pressure. A second representative reactor trip top event is an LMFW initiating event. The LMFW event was chosen because the preliminary design for LMFW uses low SG level as the primary trip and Departure from Nucleate Boiling Ratio (DNBR) as the backup trip. The DNBR trip uses a larger number of plant parameter inputs than most (including neutron flux, RCP speed, RCS pressure, RCS temperature) and is considered to be conservative relative to the reliability of simpler trip functions.

2.4 *Human Reliability Analysis*

2.4.1 *Human Reliability Analysis for Pre-Accident Operator Actions*

Pre-accident operator actions are quantified using the Accident Sequence Evaluation Program (ASEP) method documented in NUREG/CR-4772 (Reference 25) as

implemented by the EPRI Human Reliability Analysis Calculator® (EPRI HRA Calculator). The EPRI HRA Calculator software is described in more detail in Section 5.0. The ASEP method is a slightly modified version of the Technique for Human Errors Rate Prediction (THERP) method, which provides a more conservative but significantly faster evaluation of the human error probabilities (HEP) associated with routine test and maintenance activities. These pre-accident operator actions, if not performed correctly, could impact performance of the mitigating system after an accident. They are systematically identified by evaluating each mitigating train credited in the PRA. In the design certification PRA, some assumptions are made on test practices based on engineering judgment and experience with current plants.

The ASEP methodology evaluation is illustrated in Figure 2-6. As shown in this figure, pre-accident HEPs are considered negligible if the component, usually a valve manipulated during a test or maintenance, has a status indication in the control room. Also, a medium dependency (see Section 2.4.3 for treatment of human dependency) is assumed between post-maintenance test and independent verification. Two pre-accident HEP values used in the U.S. EPR PRA are shaded in Figure 2-6. These actions correspond to the HEPs with (ASEP Case VIII) and without (ASEP Case III) an effective post-maintenance test (e.g., a pump flow test). A check of equipment status during each shift is not credited. Calibration errors are not considered in the design certification phase of the PRA.

2.4.2 *Human Reliability Analysis for Post-Accident Operator Actions*

2.4.2.1 *Design Philosophy for Operator Actions*

The design philosophy of the U.S. EPR regarding operator actions is that systems and controls are designed so that operator action is not required to mitigate design basis accidents (DBA) or anticipated operational occurrences within 30 minutes if performed from the MCR or within 60 minutes if performed outside the MCR. The operator actions credited in the PRA are generally well-established actions that would be taken in response to beyond DBA event sequences where multiple failures of safety-related equipment are postulated. This includes, for example, initiating feed and bleed for

accidents involving complete loss of secondary-side cooling, or starting the SBO diesel generators upon loss of AC power, and failure of all EDGs.

2.4.2.2 *Post-Accident HRA Methodology*

The post-accident operator actions were quantified using the method of Standardized Plant Analysis Risk – Human Reliability Analysis (SPAR-H) (Reference 26) as implemented by the EPRI HRA Calculator. SPAR-H is a simple and conservative Human Reliability Analysis (HRA) method for estimating the HEPs associated with operator decisions and actions in response to initiating events. SPAR-H is an appropriate HRA method for the current stage of the U.S. EPR design because emergency operating guidelines and procedures are not yet available. The SPAR-H method bases its HEP estimates primarily on time available for the diagnosis and action, coupled with high-level performance shaping factors (PSF).

The SPAR-H methodology evaluates the HEP error contributions from diagnosis failure and action failure. These are adjusted by PSF applied for available time, stress, complexity, experience and training, procedures, ergonomics, fitness for duty, and work processes. In the design certification phase PRA, the evaluated PSFs are limited to available time, stress, complexity, and experience and training.

2.4.2.3 *Performance Shaping Factors*

Performance Shaping Factors for Time

The PSFs for available time are based upon a timeline, such as the one shown in Figure 2-7. The first four time parameters shown in the figure are specified based on the accident sequence and the operator action:

- The total time window (T_{sw}) is measured from accident initiation until core damage is unavoidable, estimated from thermal-hydraulic analysis.
- The time delay until the first cue (T_{delay}) is generally estimated from knowledge of the accident sequence, the available instrumentation, and thermal-hydraulic analysis.

- The median time needed for diagnosis ($T_{½}$) is based on engineering judgment, estimating a reasonable time for cognition based on the complexity of the cues and the clarity of the criteria that is expected in the emergency operating procedures (EOP) related to the action. Taken together, the delay time for the cue (T_{delay}) and the median response time for diagnosis ($T_{½}$) represent the total time needed for an operator to make a confident decision on a course of action.
- The time needed for action (T_M) is estimated based on the complexity of the action, and whether or not it can be performed from the MCR. Generally five minutes is estimated for simple MCR actions and 15 minutes for actions that require leaving the MCR. However, these action times are adjusted if they involve several or complex steps.

PSFs for time are determined based on a comparison of the time needed and time available for both diagnosis and action. Assigned multiplication factors are shown below.

Inadequate time, probability of failure	=	1.0
Barely adequate time, PSF	=	10x
Nominal time, PSF	=	1x
Extra time, PSF	=	0.1x
Expansive time, PSF	=	0.01x

Other Performance Shaping Factors

The PSF for stress is assigned as extreme (5x), high (2x), or nominal (1x). The PSF for stress is assigned based on engineering judgment and knowledge of the applicable accident sequence. For example, extreme or high stress is assigned for accident sequences that are especially severe (e.g., a LOCA with failure of SI) or where the proposed operator action is drastic (e.g., feed and bleed).

The PSF for complexity is assigned as high (5x), moderate (2x), nominal (1x), or obvious (0.1x, applicable to diagnosis only, not action). This is also assigned based on engineering judgment. For example, accident sequences where cues might be ambiguous (e.g., an SLOCA that does not depressurize) are assigned high complexity. In other cases (e.g., SGTR), the cues may be compelling, and accordingly, obvious diagnosis is assigned.

For the experience and training PSF, the specific qualifications of the operator are not known at this time, and the base PSF is nominal or insufficient information. However, certain operator actions, such as initiation of feed and bleed or performing an RCS cooldown, are assigned a PSF of high experience/training (0.5x) because these are actions that will receive extensive attention in operator training and will be practiced many times on the simulator.

The PSFs for procedures, ergonomics, fitness for duty, and work processes are assigned to nominal (1x) or insufficient information (1x) until detailed design information is developed.

2.4.3 *Treatment of Dependencies Between Human Actions*

The dependencies between human actions are evaluated using the SPAR-H dependency rating system. The SPAR-H rating system uses the following factors to assess the dependency level between two actions:

- Whether the crew performing the operator action is the same crew that made the previous human error.
- Whether the operator action is close in time to the previous human error. SPAR-H defines close in time as from within seconds to a few minutes.
- Whether the operator action takes place in the same location as the previous human error. This may be the same control, display, or equipment, or be in close proximity.

- Whether additional cues were available following the previous human error. These cues can be additional parameter displays, alarms, or procedures steps.

The combinations of these factors and how they affect dependency level is illustrated in Figure 2-8. The HEP for the dependent action is assigned based on the assessed level of dependence as shown in Table 2-7.

There could also be assigned zero dependence. This would be the case where the operator has no knowledge of the previous task, or there is no expectation that knowledge of the previous task would influence the current task. This is assumed to be the case between pre-accident human actions and post-accident human actions.

2.5 *Approach to Level 1 Uncertainty and Sensitivity Analyses*

2.5.1 *Uncertainty Analysis*

The uncertainty analysis is performed by standard Monte-Carlo simulation executed within RiskSpectrum using the input distributions for the initiating events, failures rates, CCF, and human errors. Both point estimate values and the mean values are reported for the CDF/LRF. The phenomenological uncertainties and model uncertainties are addressed in a sensitivity analysis.

2.5.2 *Sensitivity Analysis*

The sensitivity analysis is performed to address phenomenological uncertainties (e.g., uncertainties in the success criteria) and the PRA model uncertainties (due to various assumptions made in the PRA model). Factors selected for sensitivity analysis are based on their importance in the PRA model. Possible examples of sensitivity analyses are listed below:

- HEPs to address possible uncertainties in the inputs used in the HEP evaluation (timing, procedures, dependencies).
- Assumptions in the common cause grouping.
- Assumptions used in modeling of RCP seal LOCAs.

- Assumptions used in modeling of recovery of the offsite power.

2.6 *Level 2 PRA*

2.6.1 *Overview of Level 2 Methodology*

The Level 2 PRA calculates the probability, composition, magnitude, and timing of fission product releases from the plant. The Level 2 PRA is performed using a combination of deterministic and probabilistic analyses consisting of the following:

- Integration of the Level 1 and Level 2 analyses through the definition of CDESs
- Level 2 systems analysis
- Accident progression analysis to support development of the Containment Event Tree (CET) and determination of branch probabilities
- Development of release category (RC) bins to characterize fission product migration into the environment using CET techniques
- Determination of the source terms for key nuclides for each RC
- Uncertainty and sensitivity evaluations

The scope of the U.S. EPR Level 2 PRA includes evaluation of all plant operating states (POS). Spent fuel pool (SFP) releases are also evaluated.

2.6.2 *Definition of Core Damage End States*

The CDES are used to group (or bin) accident sequences involving core damage, as identified in the Level 1 analysis.

The purpose of the CDES bins is to organize the numerous sequences from Level 1 into categories, each of which transfers to a single CET. Each CDES is characterized by a set of attributes that uniquely defines this set of Level 1 core damage sequences, which allow this set of sequences to be quantified as a group in the Level 2 CET. Because the Level 1 and Level 2 models are directly linked within RiskSpectrum, the inputs to the

CET preserve the Level 1 accident sequence information (Level 1 event tree top event status) to account for dependent top events.

2.6.3 *Level 2 Systems Analysis*

The severe accident mitigation systems evaluated in Level 2 are listed below.

- Severe Accident Depressurization Valves
- Combustible Gas Control System, including passive autocatalytic recombiners and gas mixing system
- Core Melt Stabilization System
- Containment Isolation System
- Severe Accident Heat Removal System
- RCS Injection Systems, recovery of SIS system for prevention of vessel failure

Extensions to the Level 1 systems analysis are performed as needed. For example, the Level 2 analysis requires that the SAHRS model be expanded beyond the containment cooling mode credited in the Level 1 analysis to include:

- Passive cooling of molten core debris
- Active spray for environmental control of the containment atmosphere
- Active recirculation cooling of the molten core debris and containment atmosphere

2.6.4 *Analysis of Severe Accident Phenomena and Progression*

Phenomenological Evaluations (PE) are performed to provide a comprehensive approach to supporting CET quantification. The PEs address those severe accident phenomena judged to be significant in determining the eventual outcome of a severe accident. Each PE evaluates the current state of knowledge concerning the phenomenon in question and considers inputs from available sources, including experiments, industry studies, and plant-specific accident progression analyses.

Typically, the outputs from the PEs are probability distributions describing the uncertainty in parameters of importance in the CET quantification process (e.g., the mass of hydrogen generated in-vessel or the probability of containment failure as a function of internal pressure). Plant-specific evaluation of the severe accident progression is performed using MAAP 4.07, which is described in Section 5.0.

2.6.5 *Containment Event Tree Quantification*

2.6.5.1 *Definition of Top Events*

The CET is constructed in time frames (typically three or four) to aid in describing the time dependent events within the tree. The top events in the CET address the phenomenological events, the systems, and the human actions credited to mitigate the severe accident. For the design certification PRA, the manual actions are selected from preliminary severe accident management guidance.

The CET is sufficiently detailed so that phenomenological-related dependencies can be properly represented. This approach also allows an appropriate level of detail to be achieved in identifying sequences, in quantifying their frequencies, and in assessing source terms.

Criteria are developed for the selection of the CET top events. Typically for a top event to be selected, it must represent an event that could occur in the time frame under consideration because this could significantly affect the fission product release characteristics or affect other top events.

2.6.5.2 *Description of Release Categories*

Each endpoint of the CET represents a unique accident sequence progression. There are thousands of possible accident progressions. To manage the results of the Level 2 PRA, the CET endpoints are grouped into representative RC bins.

Each RC contains a number of possible accident sequences whose fission product release characteristics (source terms) are similar enough that they can be reasonably

characterized by a single representative accident sequence. The source term of the accidents within the RC is then characterized by the source term of the representative sequence. The definition of RC considers the key sequence progression characteristics that influence the release spectrum.

2.6.6 *Source Term Evaluation*

Source term analysis is performed to quantify the composition, magnitude, and timing of the fission product releases. Sensitivity cases are performed to investigate the importance of key phenomena on the source term.

Accident progression calculations using MAAP 4.07 have been performed to develop the fission product source term. The CET sequences that contribute to each RC are examined, and one representative sequence is analyzed with MAAP, considering both the frequency of the contributor and how representative it is of the RC.

Fission product behavior models assume that the fission products are present as 12 representative groups. Group 1 fission products are noble gases. All other groups are modeled as aerosols (particulates).

2.6.7 *Approach to Level 2 Uncertainty and Sensitivity Analysis*

Uncertainty analyses are performed to identify important contributors in the data distributions for inputs to the CET, such as system/component failure rates and human actions. Sensitivity analyses are performed to address phenomenological uncertainties and model assumptions on the Level 2 results.

2.7 *Level 3 PRA*

A Level 3 PRA is performed to support the U.S. EPR design certification. The primary purpose of the Level 3 PRA is to perform quantification of dose and consequence results as needed for design certification, and to support Severe Accident Mitigation Design Alternatives (SAMDA) analysis and development of the Environmental Report.

For design certification, the Level 3 PRA uses realistic site data for evaluation of consequences.

The scope of the Level 3 PRA is determined by the RCs, which are the end product of the Level 2 PRA as discussed in Section 2.6. The Level 3 PRA model is developed and executed using the MACCS2 code (Reference 27) supplied by Sandia National Laboratories (SNL), and the RiskIntegrator spreadsheet. The MACCS2 code is an accident consequence code that estimates the potential offsite effect of postulated accident releases. MACCS2 performs atmospheric dispersion and deposition calculations to estimate the radiological doses, health effects, and economic consequences that could result from postulated accidental releases of radioactive material into the atmosphere. RiskIntegrator, an Excel spreadsheet program with a Visual Basic interface, performs simple calculations, organizes, and combines the results of the Level 1, Level 2, and Level 3 PRAs. The MACCS2 and RiskIntegrator codes are described further in Section 5.0 of this report.

The output of MACCS2 provides an estimate of Level 3 parameters such as expected number of early fatalities, early and latent cancers, population doses, and whole-body dose. The output of MACCS2, combined with the results of the Level 1 and 2 PRA, is used to provide an estimation of risk, considering both the frequency of a sequence and the consequence. In addition to the base case, sensitivity cases are performed to evaluate uncertainty and sensitivity of some input parameters and model assumptions.

Table 2-1—Example Table of Initiating Events Selection for at Power

NUREG/CR-5750 Initiating Events	US EPR Initiating Events
Loss-of-Coolant Accident (LOCA)	
Large Pipe Break LOCA	LLOCA
Medium Pipe Break LOCA	MLOCA
Small Pipe Break LOCA	SLOCA
Very Small LOCA/Leak	Not modeled. Assumed that normal charging will maintain inventory.
Stuck Open: Pressurizer PORV	Not applicable
Stuck Open: 1 Safety/Relief Valve	Design makes this highly unlikely. Included in SLOCA.
Stuck Open: 2 Safety/Relief Valves	Not Modeled
Reactor Coolant Pump Seal LOCA	RCP seal LOCAs are evaluated within event trees.
Steam Generator Tube Rupture	SGTR
Loss of Offsite Power	LOOP
Total Loss of Condenser Heat Sink	
Inadvertent Closure of All MSIVs	Included in Loss of Main Condenser (LOC)
Loss of Condenser Vacuum	Included in Loss of Main Condenser (LOC)
Turbine Bypass Unavailable	Included in Loss of Main Condenser (LOC)
Total Loss of Feedwater Flow	LOMFW
General Transients (combined)	Turbine Trip (TT)
High Energy Line Steam Breaks/Leaks (combined)	
Steam Line Break/Leak Outside Containment	SLBO
Steam Line Break/Leak Inside Containment	SLBI
Feedwater Line Break/Leak	Included in SLBI
Loss of Safety-Related Bus	
Loss of Vital Medium Voltage AC Bus	N1BDA
Loss of Vital Low Voltage AC Bus	Included in N1BDA
Loss of Vital DC Bus	To be modeled. DC design not finalized at this time.
Loss of Safety-Related Cooling Water	
Total Loss of Service Water	Numerous Loss of Service Water/Component Cooling Water Initiators
Partial Loss of Service Water	Numerous Loss of Service Water/Component Cooling Water Initiators
Loss of Instrument or Control Air	Not modeled. No significant air-operated components
Fire	Evaluated
Flood	Evaluated

Table 2-2—Example U.S. EPR Initiating Event List

Initiating Event	EPR Freq.	Basis	NUREG 5750 Freq.
General Transients			
TT – Turbine Trip (includes RT – Reactor Trip)	1.2	NUREG/CR 5750	1.2
LOC – Loss of Main Condenser (includes MSIV closure etc.)	1.20E-01	NUREG/CR 5750	1.20E-01
LOMFW – Total Loss of Main Feedwater	8.50E-02	NUREG/CR 5750	8.50E-02
Loss of Coolant Accidents (LOCA)			
SLOCA – Small LOCA (0.6 to 3-inch diameter)	5.00E-04	NUREG/CR 5750	5.00E-04
MLOCA – Medium LOCA (3 to 6-inch diameter)	4.00E-05	NUREG/CR 5750	4.00E-05
LLOCA – Large LOCA (>6-inch diameter)	5.00E-06	NUREG/CR 5750	5.00E-06
SGTR – Steam Generator Tube Rupture	7.00E-03	NUREG/CR 5750	7.00E-03
ISL-CCW RCPTB – CCWS RCP Thermal Barrier Tube Break	1.00E-09	FT Analysis	NA
ISL-CVCS HPTB – Tube Rupture High Pressure Letdown Cooler	2.20E-09	FT Analysis	NA
ISL-CVCS INJ – High Pressure CVCS Pipe Rupture Outside Containment	6.10E-12	FT Analysis	NA
ISL-CVCS REDS - Spurious Opening of Reducing Station	2.20E-09	FT Analysis	NA
ISL-SIS-LHSI -CL8 Break in LHSI Cold Leg Injection Check Valves with LHSI Line Break in Respective Safeguards Bldg	6.00E-10	FT Analysis	NA
ISL-SIS-LHSI-HL1 Failure of Hot Leg 1st MOV with Pressurization of LHSI line Through 1" Line and Subsequent Pie Break	2.40E-11	FT Analysis	NA
ISL-SIS-MHSI-CL-6 Break in MHSI Cold Leg Injection Check Valves with MHSI Line Break in Respective Safeguards Bldg	6.00E-10	FT Analysis	NA
ISL-SIS-MHSI-HL-1 Failure of Hot Leg 1st Isolation MOV with Pressurization of MHSI line Through 1" Line and Subsequent Pipe Break	1.20E-13	FT Analysis	NA
ISL-SIS RHR-HL10 – Failure of Suction Line Isolation MOVs and Subsequent RHR Line Break in Respective Safeguards Bldg	4.40E-10	FT Analysis	NA
ISL-SIS RHR-CL-1 – 1 Break in Common Cold Leg Injection Line Check Valve with Pressurization of RHR Line Through 1" Line and Subsequent RHR Line Break	2.20E-12	FT Analysis	NA
Secondary Side Breaks			
SLBO – Steam Break Downstream of MSIV	1.00E-02	NUREG/CR 5750	1.00E-02
SLBI – Steam Break Inside Containment	1.00E-03	NUREG/CR 5750	1.00E-03
MSSV – Spurious Opening of Steam Safety Valve	1.00E-03	NUREG/CR 5750	1.00E-03
Support System Failures			
LOOP – Loss of Offsite Power	3.59E-02	NUREG/CR-6890	4.60E-02
LOCCW-CH1L – CCWS Leak in Common Header 1	1.00E-02	FT Analysis	8.9E-3 Part. Loss of SW
LOCCW1 – Loss CCWS Train 1 and Failure of Switchover	1.00E-03	FT Analysis	"
LOCCW12 – Loss of CCWS Train 1 and Train 2	1.40E-03	FT Analysis	"
LOCC14-CH1 – Loss of CCWS Trains 1 and 4 and Failure of Switchover to CH 1	2.10E-05	FT Analysis	"
LOCCW14-CH12 – Loss of CCWS Trains 1 and 4 and Failure of Switchover to CH 1 & 2	5.70E-07	FT Analysis	"
LOCCW1L – Leak in CCWS Train 1 and Failure to Isolate	1.30E-04	FT Analysis	"
LOCCW-ALL – CCWS Total Loss of 4 Divisions	2.30E-05	FT Analysis	9.7E-4 Tot. Loss of SW
LBOP – Loss of Closed Loop Cooling Water or Aux Cooling Water	2.50E-02	FT Analysis	NA
N1BDA – Loss of Divisional Emergency AC (Switchgear N1BDA)	3.49E-02	FT Analysis	1.9E-2 Vital Med. Volt. AC Bus

Table 2-3—Example U.S. EPR PRA Component Failure Database

System	Component Type	Failure Mode Description	Unavailability	Failure Rate [/hr]	Mission Time [hr]
Emergency diesel engine	Diesel Generator	Failure to Run	5.60E-02	2.40E-03	24
Component cooling water system safety related	Pump - Motor Driven	Failure to Run	4.80E-05	2.00E-06	24
Service cooling water pump system	Pump - Motor Driven	Failure to Run	1.10E-04	4.60E-06	24
Containment heat removal system	Pump - Motor Driven	Failure to Run	2.42E-04	1.01E-05	24
Medium head safety injection system	Pump - Motor Driven	Failure to Run	1.22E-02	5.10E-04	24
Emergency feedwater pump system	Pump - Motor Driven	Failure to Run	1.22E-02	5.10E-04	24
All	Valve - Motor Operated	Failure to close	3.50E-03		
All	Valve - Motor Operated	Spurious operation	8.40E-06	3.50E-07	24
Component cooling water system process related	Valve - Safety	Premature opening	7.20E-05	3.00E-06	24

Table 2-4—Example Table of Failure Data Comparison

Group ID	Comp Type	Data Source	Failure Mode Description	Failure Rate [per demand or per hr]
DG-FTR (Emergency Diesel Engine)	Diesel Generator	U.S. EPR PRA	**Emergency Diesel Generator - Fails to run**	**2.40E-03**
		NUREG 5500 Data	Diesel Generator - Fails to run after the 1st hour - No recovery	9.43E-04
		ALWR EPRI Data	Diesel Generator - Fails to run	2.40E-03
DG-FTS (Emergency Diesel Engine)	Diesel Generator	U.S. EPR PRA	**Emergency Diesel Generator - Fails to start**	**4.50E-03**
		NUREG 5500 Data	Diesel Generator - Fails to start and load - No recovery	1.52E-02
		ALWR EPRI Data	Diesel Generator - Fails to start and load	1.40E-02
MDP-FTR A (Medium Head Safety Injection System) (Startup and Shutdown System) (Emergency Feedwater System)	Pump - Motor Driven	U.S. EPR PRA	**Motor-driven Pump - Fails to run**	**5.10E-04**
		ALWR EPRI Data	Motor-driven pump (Emerg. Feed) - Fails to run	1.50E-04
			Motor-driven pump (all other types) - Fails to run	2.50E-05
MDP-FTS A (Medium Head Safety Injection System) (Startup and Shutdown System) (Emergency Feedwater System)	Pump - Motor Driven	U.S. EPR PRA	**Motor-driven Pump - Fails to start**	**1.28E-03**
		NUREG 1715 Data	Motor-driven pump - Fails to start	1.37E-03
		ALWR EPRI Data	Motor-driven pump (Safety Inj.) - Fails to start on demand	1.00E-03
			Motor-driven pump (Emerg. Feed) - Fails to start on demand	3.00E-03
			Motor-driven pump (all other types) - Fails to start on demand	2.00E-03
VLV-MOV-FTC (All Systems)	Valve - Motor Operated	U.S. EPR PRA	**Motor-operated Valve - Fails to Close**	**3.50E-03**
		NUREG 1715 Data	Motor-operated valve - Fails to Close	4.67E-04
		ALWR EPRI Data	Motor-operated valve - Fails to Close	4.00E-03

Table 2-5—Example Common Cause Failure Data Comparison

Parameter	European Data	U.S. EPR (NUREG/CR-6819 2003 Update)			
	Generic (4 Components)	Generic	EFW Pump Start	LHSI Pump Run	EDG Start
Beta	0.1	0.0317	0.0374	0.00933	0.0177
Gamma	0.4	0.335	0.679	0.743	0.415
Delta	0.25	0.349	0.347	0.333	0.211
Conditional Four Train Failure Probability	0.010	0.004	0.009	0.002	0.002

Table 2-6—Example U.S. EPR System Dependency Matrix

System/Train Failure	Impacts								
	OCW	SCW	CVCS	RCP	MHSI	LHSI	SAC	EFW	Electrical
CCWS Common Header 1	1 of 2	20	1 of 2	Cooling to 2 pumps					
CCWS Common Header 2	1 of 2	30	1 of 2	Cooling to 2 pumps					
CCWS10					10	10 (Hx)			
CCWS20					20	20			
CCWS30					30	30			
CCWS40					40	40 (Hx)			
Operational Chilled Water (OCW)							50, 80		
Safety Chilled Water 10 (SCW)						10 (Pmp)	10 (61)	10	
Safety Chilled Water 20 (SCW)							20 (62)	20	
Safety Chilled Water 30 (SCW)							30 (63)	30	
Safety Chilled Water 40 (SCW)						40 (Pmp)	40 (64)	40	
SAC10 (SAB1 Ventilation)									10P
SAC20 (SAB2 Ventilation)									20P
SAC30 (SAB3 Ventilation)									30P
SAC40 (SAB4 Ventilation)									40P
SAC50 (Maintenance Train)									(10, 20)P
SAC80 (Maintenance Train)									(30, 40)P

- 10, 20, 30, 40 (50, 80) identifies train divisions
- 61, 62, 63, 64 identifies safeguards buildings ventilation system d
- “Hx” indicates heat exchangers cooling
- “Pmp” indicates pump cooling
- “P” indicates partial dependency

Table 2-7—SPAR-H Dependency Formula

Level of Dependence	Conditional Probability Equation (N = HEP)	Approximate Value for Small N
Zero dependence (ZD)	N	**N**
Low Dependence (LD)	$\frac{1+19N}{20}$	**0.05**
Medium dependence (MD)	$\frac{1+6N}{7}$	**0.14**
High Dependence (HD)	$\frac{1+N}{2}$	**0.5**
Complete Dependence (CD)	1.0	**1.0**

Figure 2-1—Safety Injection Systems

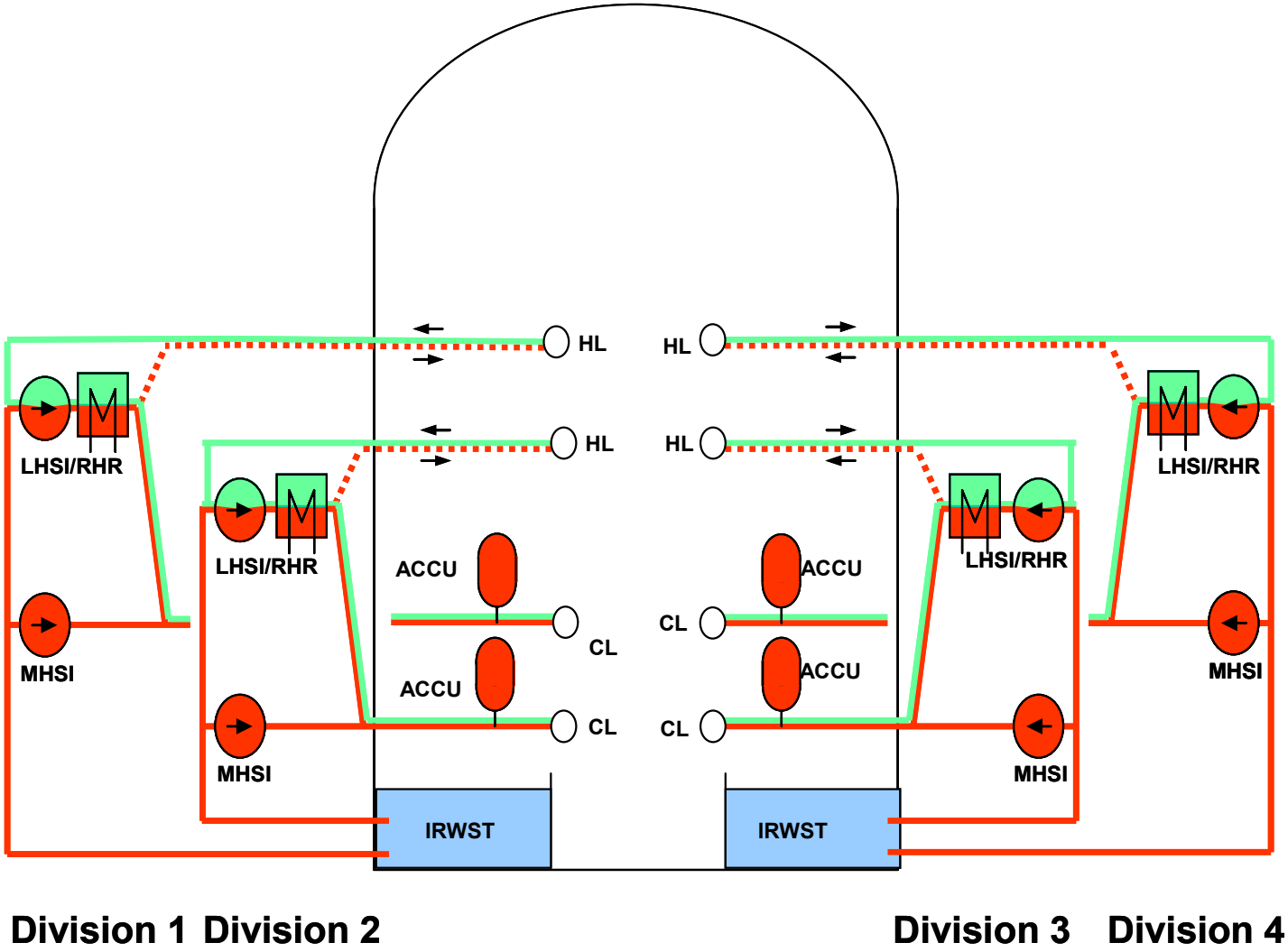


Figure 2-2—RCS Safety and Severe Accident Depressurization Valves

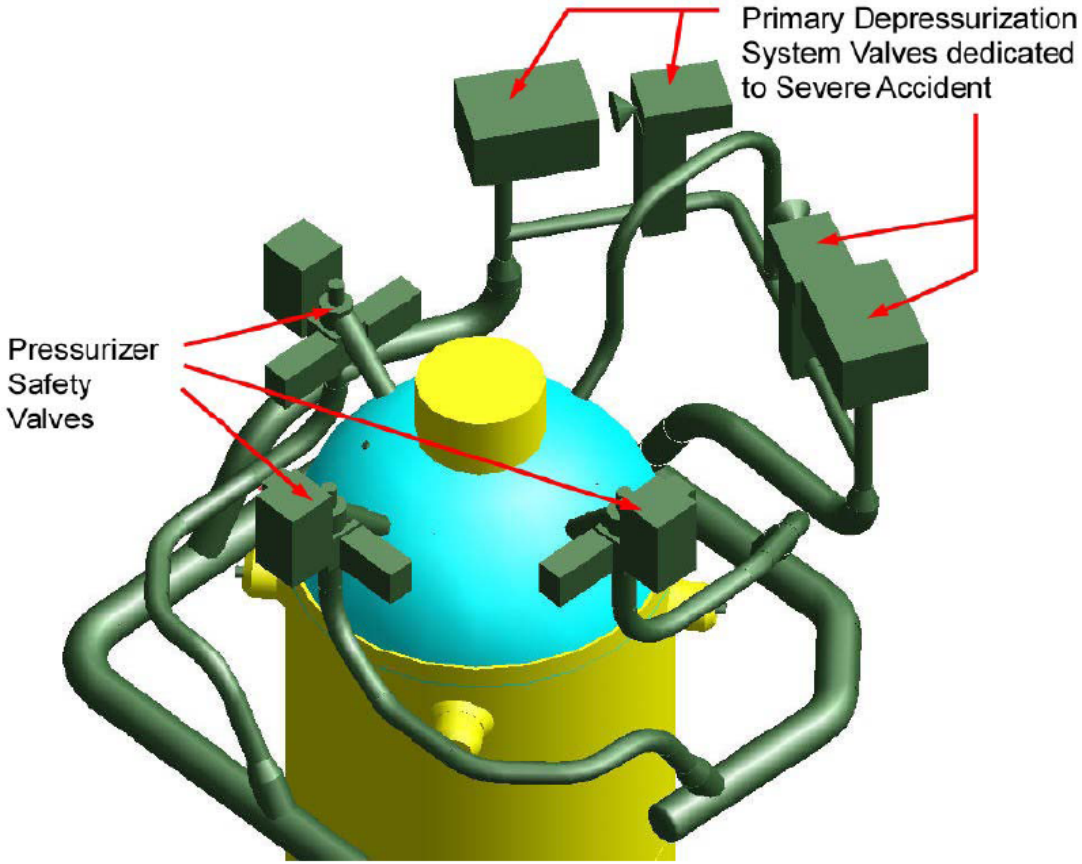


Figure 2-3—Severe Accident Heat Removal System

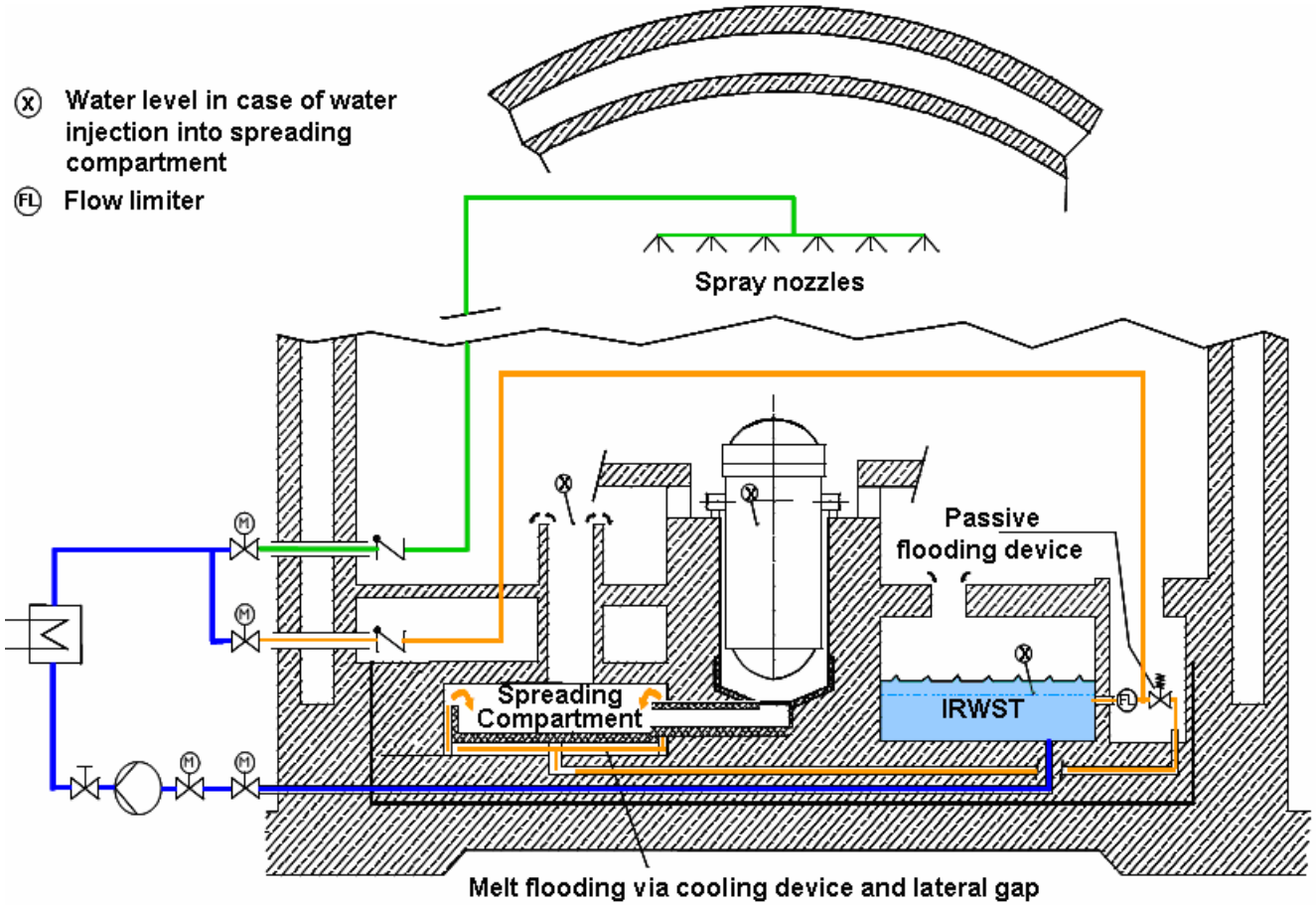


Figure 2-4—Diverse Architecture of a Single Division

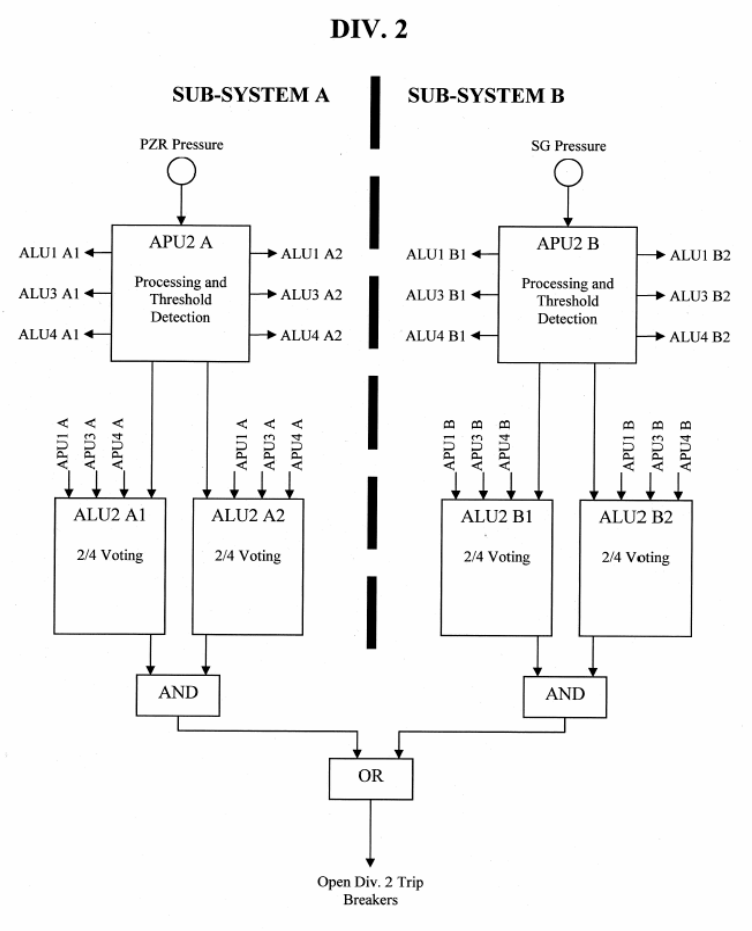


Figure 2-5—Arrangement of the Reactor Trip Breakers

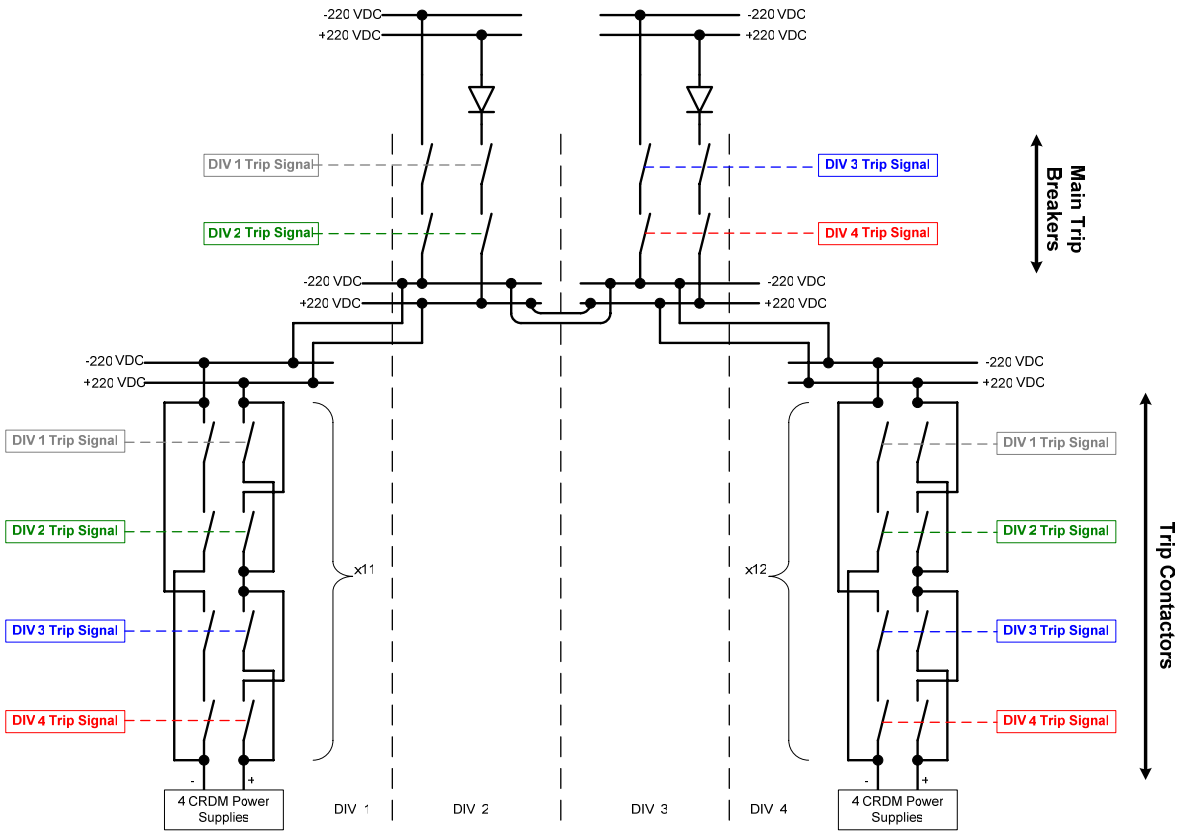
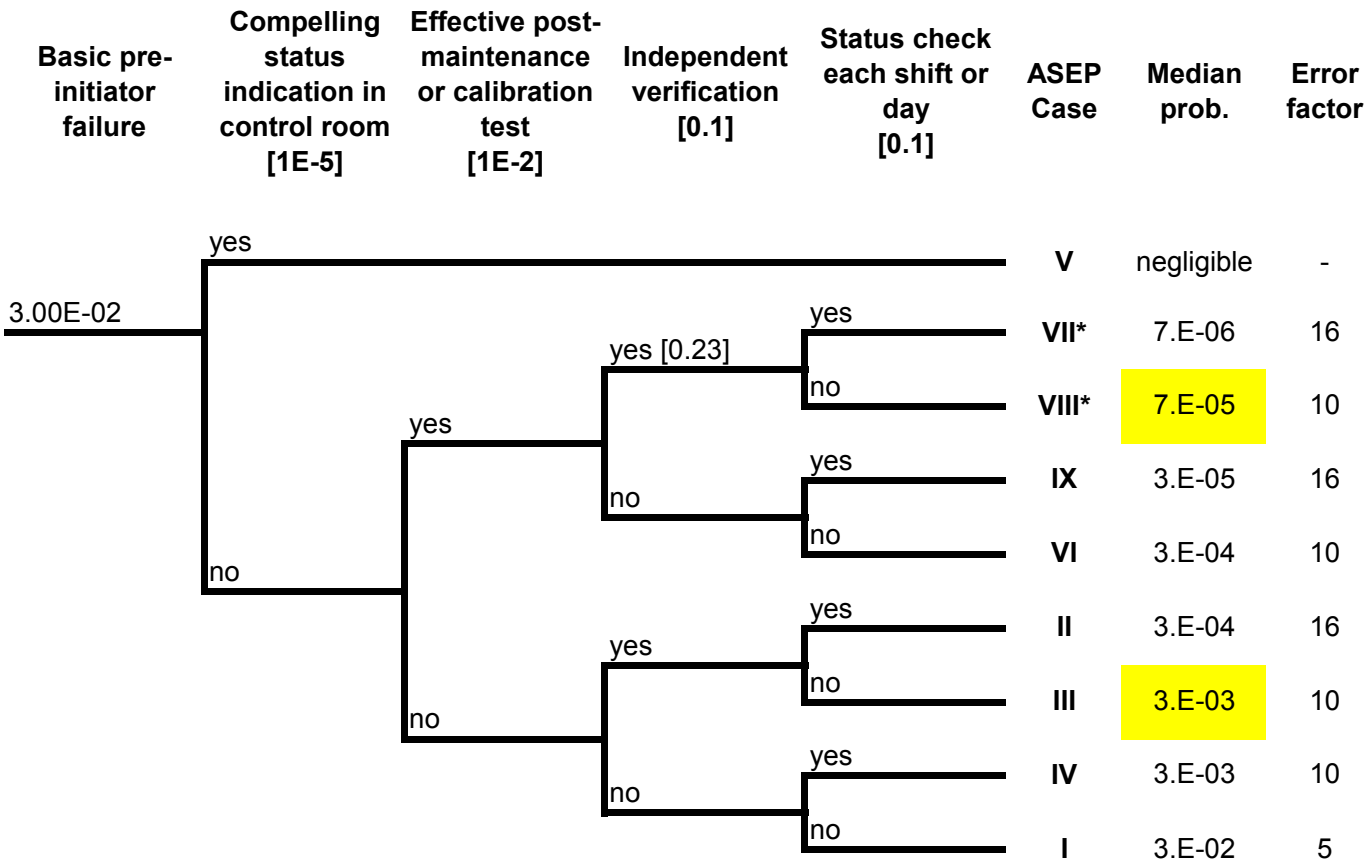
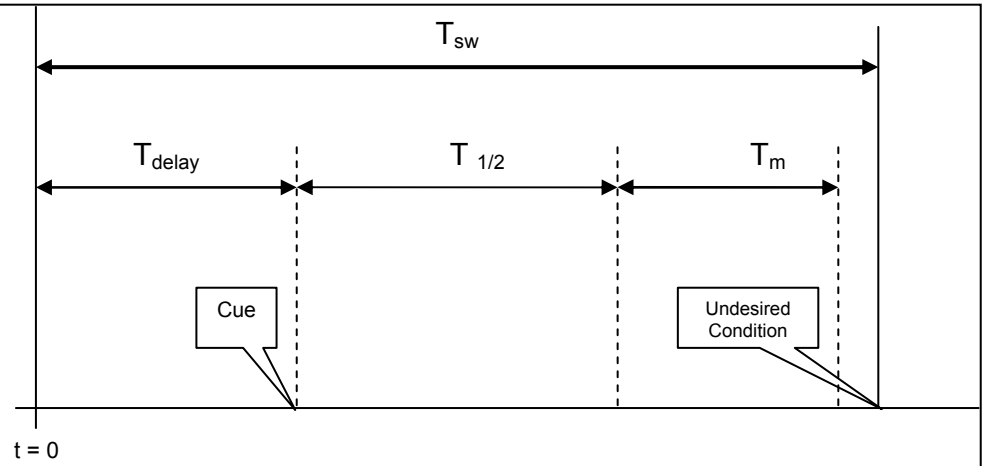


Figure 2-6—Pre-Accident HEP Evaluation



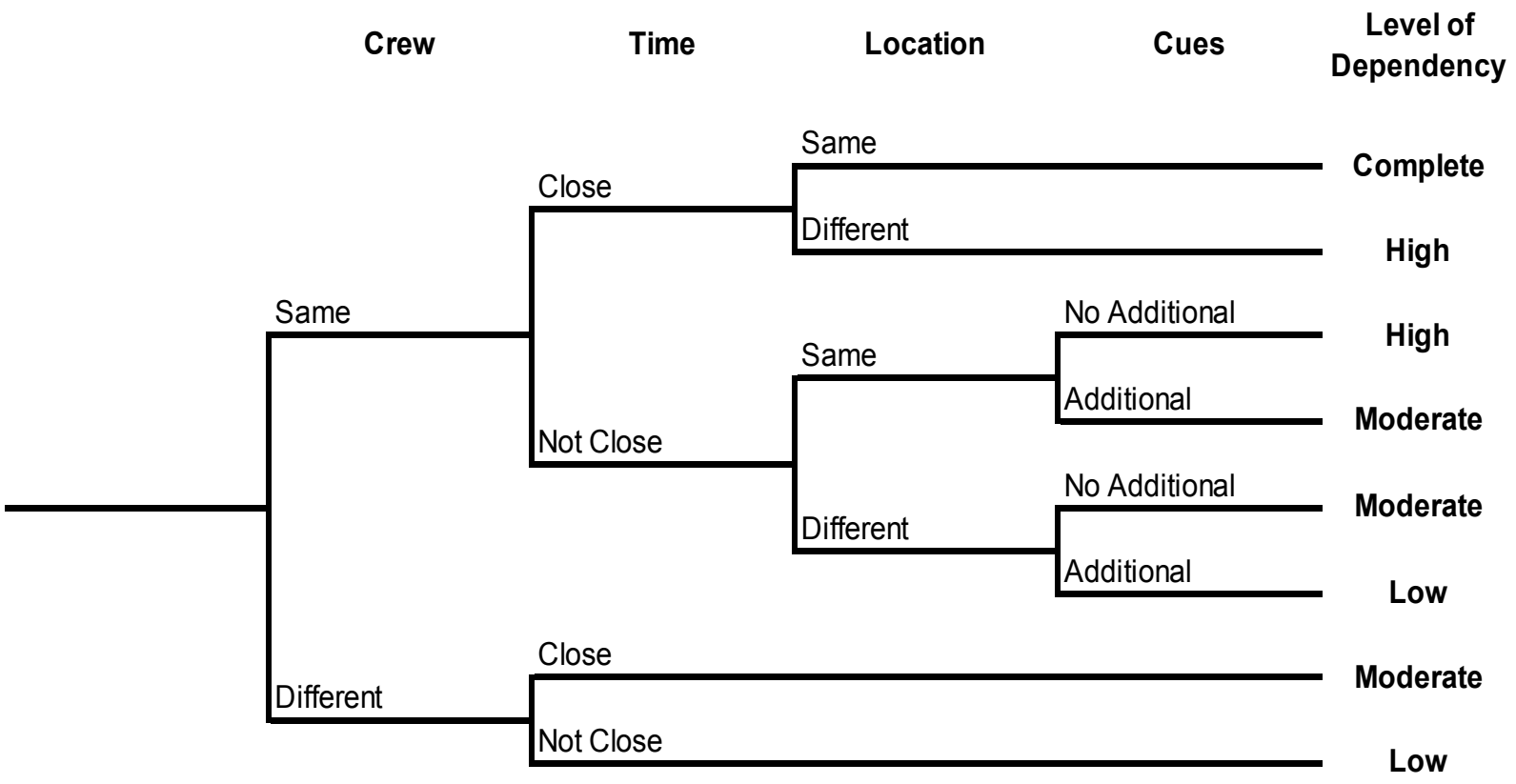
Reference: NUREG/CR-4772, Accident Sequence Evaluation Program Human Reliability Analysis Procedure; A.D. Swain; February 1987 (ASEP).

Figure 2-7—Post-Accident Time Window



T_{SW} = Total time from event start until irreversible damage
T_{delay} = Delay time from start of event until cue is reached
$T_{½}$ = Median time needed for diagnosis
T_M = Time needed for action (manipulation)
$T_{diagnosis}$ = T_{SW} -T_{delay}– T_M = Time available for cognitive response
T_{action} = T_{SW} -T_{delay}– $T_{1/2}$ = Time available for action

Figure 2-8—SPAR-H Dependency Rating System



3.0 INTERNAL FLOODING, INTERNAL FIRES, AND EXTERNAL EVENTS METHODOLOGY

3.1 *U.S. EPR Spatial Arrangements*

The U.S. EPR is designed so structural design and physical arrangements of the buildings provide protection from both external and internal hazards. A general layout of the major U.S. EPR buildings is shown on Figure 3-1. It is noted that the design features and/or parameters are subject to change, and the final design information will be provided in the DCA. The buildings that contain SSCs credited in the PRA analysis are the: Reactor Building, four Safeguard Buildings, two EDG Buildings, ESW Building (not shown on Figure 3-1), Fuel Building, and Turbine Building. Offsite power is routed from the transformer area (not shown on Figure 3-1) to each safeguards building.

The design philosophy of the U.S. EPR is for each train/division of safety systems to be located in a different safeguard building and physically separated from the other trains. This separation includes all support systems for the specific train: power supplies; controls; cooling systems; and heating, ventilation, and air conditioning (HVAC). The Reactor Building contains multiple safety trains. In addition to the Reactor Building, control cables for different trains are routed through the MCR and cable distribution area located within Safeguard Buildings 2 and 3. Location of safety divisions is illustrated in Figure 3-2.

As part of the U.S. EPR PRA hazard evaluation, a spatial database is being developed containing information about locations of the SSCs credited in the PRA model. An example from this database is shown in Table 3-1 for Safeguard Building 1.

3.2 *Internal Flooding Analysis*

Based on the spatial separation between safety trains in the U.S. EPR, a bounding internal flooding analysis method is used in the design certification PRA. This analysis will be updated, as necessary, during the detailed design phase when more detailed information is available on the flooding sources, pipe routings, and specific component

locations. The aim of this bounding analysis is to show that the CDF/LRF, as a result of a more detailed internal flood evaluation, will not change the conclusion that the overall CDF/LRF meets the U.S. EPR design objective.

For each building containing SSCs credited in the PRA analysis, the approach to the internal flooding evaluation consists of the following steps:

1. Calculate flooding frequency based on the flooding sources and piping segments. If design information is not available, use conservative estimates of flooding frequency from available industry references.

2. Analyze possible flooding scenarios for each location and, based on the PRA model, select the worst scenario.

3. Apply the total building flooding frequency to the worst scenario, and calculate corresponding CDF/LRF.

For the design certification phase PRA, and based on the above approach, sufficient information is available to calculate the frequency of internal flooding for each safeguard building. This calculated frequency is based on the total number of pipe sections for each system. Both operating systems and stand-by systems (including the fire water system) are considered in the frequency. Conservative estimates of flooding frequency are used for the other locations.

3.3 *Internal Fire Analysis*

Given the design of spatial separation and fire barrier design between safety trains in the U.S. EPR, a bounding internal fire analysis method is used in the design certification PRA. This analysis will be updated as necessary during the detailed design phase when more detailed information is available on the combustible loadings, cable routings, and specific component locations. The aim of this bounding analysis is to show that the CDF/LRF, as a result of a more detailed internal fire evaluation, will not change the conclusion that the overall CDF/LRF meets the U.S. EPR design objective.

For each building/fire area containing SSCs credited in the PRA analysis, a bounding approach to the internal fire evaluation consists of the following steps:

1. Estimate fire frequency based on the available industry experience (e.g., NUREG/CR-6850 [Reference 28]). Use conservative fire frequency estimates for locations where no available industry data applies.

2. Assume that each fire ignition will grow to a fully developed fire (do not consider the possibility that the fire will self-extinguish).

3. Analyze possible fire scenarios for the location and, based on the PRA model, select the worst scenario.

4. Only credit automatic fire suppression (if not affected by the specific fire).

5. Only credit human recovery actions for control room fire scenarios. These actions are implemented from the remote shutdown station that is physically separated and electrically independent of the control room.

6. Apply the total building/fire area frequency to the worst scenario: credit auto suppression, if applicable; operator action, if applicable (only for the control room); and calculate the corresponding CDF/LRF.

3.4 *Seismic Methodology*

The PRA-based seismic margins approach is discussed in SECY 93-087 (Reference 29). A PRA-based seismic margins assessment is being performed so that potential vulnerabilities are identified and corrected, and so that the seismic risk will be low. The internal events PRA, including power operation and shutdown, provides the starting point for the seismic PRA-based model. This model also provides the primary basis for establishing the seismic equipment list (SEL), which identifies equipment and structures for seismic fragility analysis. Because this assessment is being conducted early in the plant design, fragility assumptions are documented to support seismic design development in the detailed design phase. Guidance on seismic margins methods is

provided in ANSI-ANS-58.21, Section 3.7 and Appendix B (Reference 30) and is considered in this assessment. The key elements of implementing the PRA-based seismic margins methodology for the U.S. EPR are summarized below:

- Seismic Hazard Input
- Seismic Fragility Evaluation
- Systems/Accident Sequence Analysis
- High Confidence Low Probability Failure (HCLPF) Sequence Assessment

3.4.1 *Seismic Hazard Input*

The U.S. EPR seismic design safe shutdown earthquake (SSE) is based on the EUR ground motion spectral shape anchored to 0.30g peak ground acceleration (PGA), which applies to both horizontal and vertical motions. The PRA-based seismic margins assessment addresses the plant's seismic capacity margin up to 1.67 times the SSE. This margin will be demonstrated as an HCLPF—high confidence (95%) of low probability (5%) of failure. The PRA-based seismic margin assessment does not require a probabilistic seismic hazard analysis and its resulting hazard curves. However, as described in Section 3.4.2, seismic hazard inputs and assumptions are essential to the fragility evaluation.

3.4.2 *Seismic Fragility Evaluation*

At the design certification stage, design details, anchorage, qualification, and analyses are still in development. Thus, "reasonable achievable" fragilities are being established using U.S. EPR design criteria, the EPRI ALWR Utility Requirements Document (Reference 6), and experience from other seismic PRAs.

The fragility evaluation will provide estimates of the conditional probability of failure of SSCs in the seismic PRA model, assuming the seismic event has occurred. The ground motion capacity of a component and its uncertainties are estimated where capacity is defined as the PGA value (or the average spectral acceleration) above which the seismic response at the component's location in a structure exceeds the

component's resistance capacity, resulting in its postulated failure. The resulting fragilities will be described with the median capacity, logarithmic standard deviations for randomness and uncertainty, and HCLPF.

The U.S. EPR design ground response spectrum is an input to the fragility evaluation, and the conservatism between this design motion and the median ground response spectrum must be estimated. The NUREG/CR-0098 (Reference 31) response spectrum is assumed to provide a median response spectrum as is traditionally done in other margins studies. Recent studies by EPRI (References 32 and 33) of 28 sites indicate that the use of NUREG/CR-0098 response spectrum is conservative.

For the U.S. EPR design certification, AREVA NP will use the design and qualification criteria to estimate the factors arising from these conservatisms. There are substantial additional margins in the actual designs, and an estimate of these margins is made to develop the fragilities. For example, actual stress in a component may be much less than the allowable or the equipment is tested to an enveloping spectrum while the actual floor response spectrum at that equipment location may be significantly lower. Generic sources for estimating these design margins are EPRI TR-103959 (Reference 34) and the EPRI ALWR Utility Requirements Document (Reference 6).

3.4.3 *Systems/Accident Sequence Analysis*

A seismic margins PRA model is developed from the internal events PRA model to include the important accident sequences and to provide a basis for establishing the SEL. This model also contains random failures and human errors from the internal events PRA. The seismic margins PRA model is used to analyze combinations of component seismic failure and to identify vulnerabilities in the design, so they can be addressed during detailed design.

Seismic initiating events are determined from review of the internal events PRA and fragility information. Preliminary seismic initiating events include SLOCA and LOOP. Structures and other passive components not typically included in the internal events PRA are also considered. Systems analysis fault trees from the internal events PRA

are assessed for incorporating the seismic fragilities and any unique impacts (e.g., assume no recovery of offsite power). The seismic fragility inputs are included in the fault trees as basic events to obtain seismic failures in the analysis of cutsets for core damage. The internal events PRA fault tree models are used so that random non-seismic equipment failure probabilities can be included in the analysis. Human actions in the PRA model are also reviewed and evaluated relative to potential seismic impact on the human reliability.

3.4.4 *HCLPF Sequence Assessment*

Risk is addressed by showing that there is adequate margin in the plant seismic design to 1.67 times the SSE (i.e., a review level earthquake anchored at 0.5g PGA). The “min-max” method of evaluating accident sequence cutsets is used to assess the HCLPF capacity of the plant.

The min-max method assesses the accident sequence HCLPF by taking the lowest HCLPF value for components analyzed under OR-gate logic and the highest HCLPF value for components analyzed under AND-gate logic. Random component failures and human actions are also considered in the evaluation.

The product of this evaluation is identification of the limiting structure/component HCLPF in the assessment of core damage cutsets. The HCLPF results and PRA insights from this evaluation are assessed to identify seismic vulnerabilities relative to the review level earthquake and their potential resolution.

3.5 *Other External Events*

For the U.S. EPR, both the structural design and physical arrangement of the buildings provide significant protection from external hazards. The Reactor Building, Safeguards Buildings 2 and 3, and the Fuel Building are structurally protected against aircraft hazard and other external hazards (e.g., postulated explosion pressure waves). Safeguards Buildings 1 and 4, MS and FW valve compartments, and diesel buildings are not structurally protected against aircraft hazard; however, they are located so only

one safety division would be impacted by a postulated aircraft hazard. These safety-related buildings and structures of the U.S. EPR are also designed to withstand the effects of seismic events and tornado events.

Based on the above plant design considerations, the risk from external hazards is judged to be low, and a screening evaluation of external hazard risks (e.g., high winds, tornado, explosion, random aircraft hazard) is not included within the scope of the design certification PRA. Proper characterization of external hazards is site-specific. Therefore, screening of applicable external hazards will be completed as part of the site-specific assessment.

Table 3-1—Example U.S. EPR Spatial Database

Building	System US	System	Component ID	Basic Event Desc	Component Type	U.S. EPR Room Elev	U.S. EPR Rooms	U.S. EPR Room Description	PRA Flood Area	PRA Fire Area
SAB1	CCWS	KAA	30KAA10AA033A	CCWS, Train 1 Solenoid Pilot Valve KAA10AA033A	SOV	0' - 0"	31UJH10004	CCWS / EFWS Valve Room / Penetration Area Div. 1	SAB1-0-06	1UCOS3
	CCWS	KAA	30KAA10BB001	CCWS, Train 1 Surge Tank KAA10BB001	Tank	+68' - 10 3/4"	31UJK29025	CCWS Surge Pool Div. 1	SAB1+69-05	
	RHR	JNA	30JNA10AA003P ASM	RHR, Train 1 RCS Suction MOV JNA10AA003, PAC A Priority Module (Type AV42) (Self-Monitored)	PAC A Priority Module (Type AV42)	+26' - 6 3/4"	31UJK18024	I&C Cabinets Div. 1	SAB1+27-06	1UCOS5
	RHR	JNA	30JNA10AA101	RHR, LHSI Train 1 HTX Bypass MOV JNA10AA101	MOV	-16' - 4 3/4"	31UJH05004	SIS Valve Room / Penetration Area Div. 1	SAB1-16-11	1UCOS3
	SAHR	JMQ	30JMQ10AC001	SAHR, Train 1 HTX 10, JMQ10AC001	Heat Exchanger	-16' - 1"	31UJH05012	SAHR Heat Exchanger Div. 1	SAB1-16-10	1UCOS3
	SAHR	JMQ	30JMQ10AP001	SAHR, Train 1 Motor Driven Pump JMQ10AP001	Pump	-31' - 6"	31UJH01008	SAHR Pump Div. 1	SAB1-31-05	1UCOS3
	SAHR	JMQ	30JMQ11AA001	SAHR, Train 1 Spray Line MOV JMQ11AA001	MOV	-16' - 4 3/4"	31UJH05007	SAHR Valve Room / Penetration Area Div. 1	SAB1-16-10	1UCOS3
	SCWS	QKA	30QKA10AH112	SCWS, Train 1 Chiller Unit QKA10AH112	Chiller	+39' - 4 1/2"	31UJK22028	Secured Chilled Water System Div. 1	SAB1+39-04	1UCOS12
	SCWS	QKA	30QKA10AP107	SCWS, Train 1 Motor Driven Safety Chiller Pump QKA10AP107	Pump	+39' - 4 1/2"	31UJK22028	Secured Chilled Water System Div. 1	SAB1+39-04	1UCOS12

Figure 3-1—Example of U.S. EPR Arrangement of Buildings

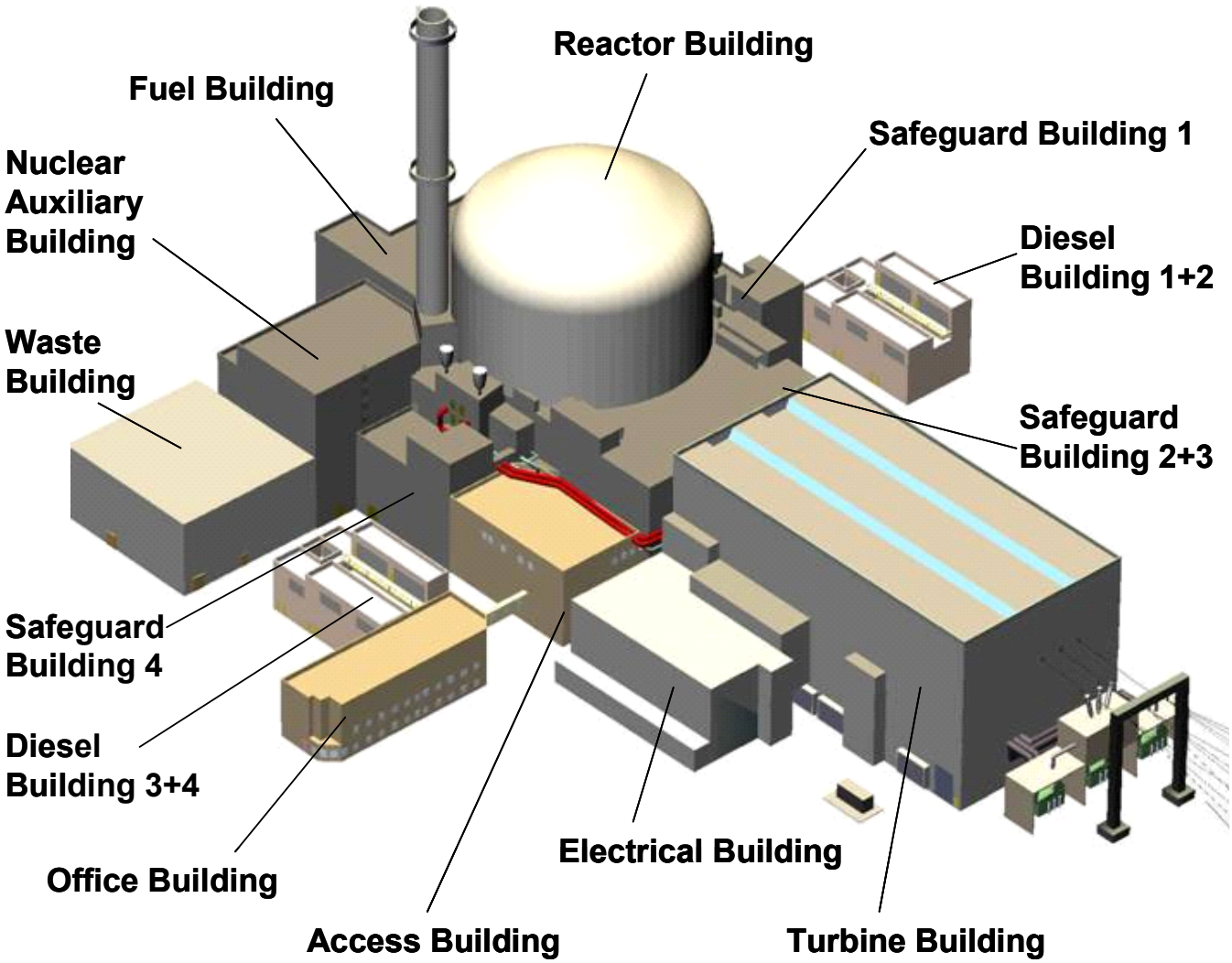
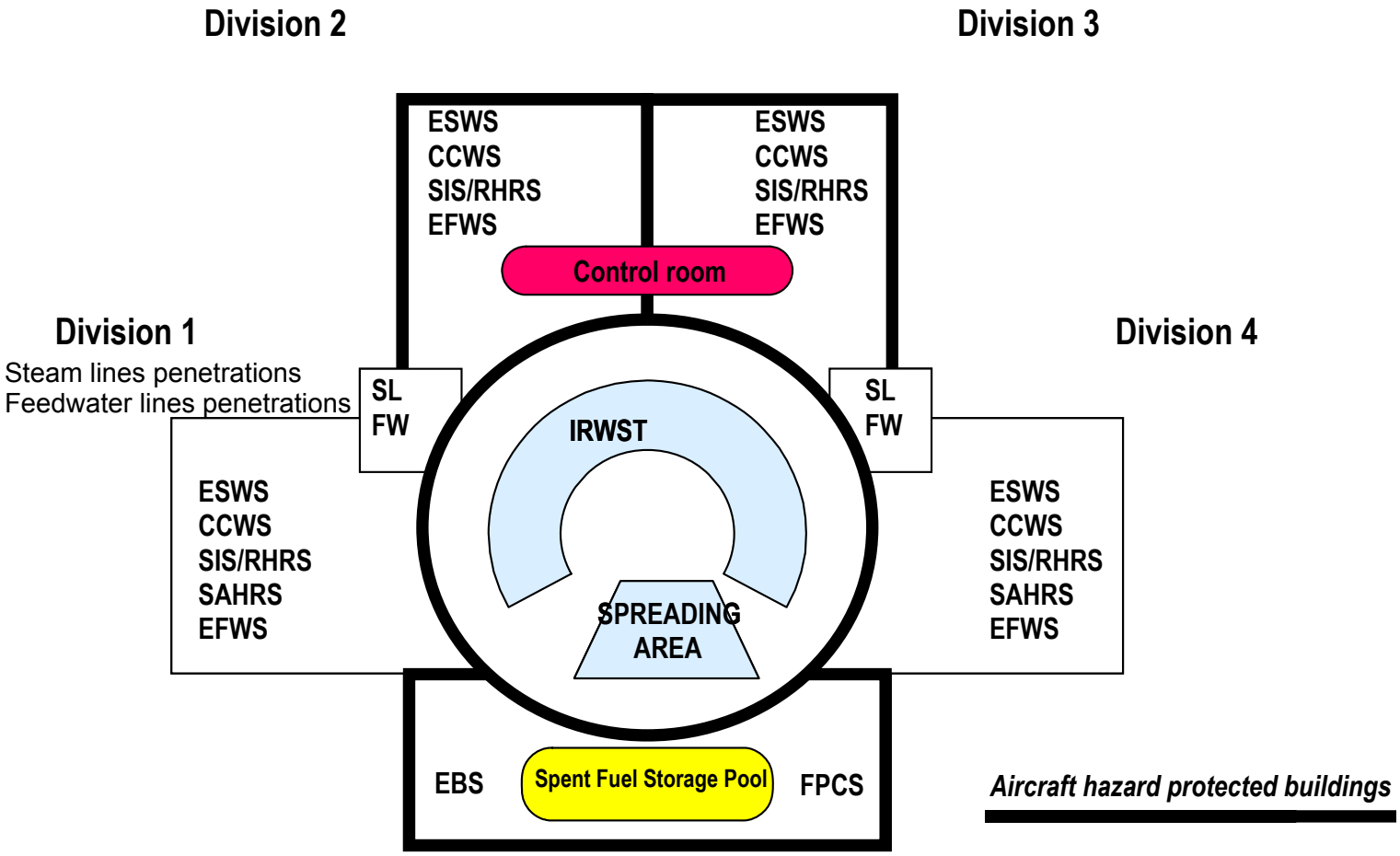


Figure 3-2—Safety Systems Spatial Allocation



4.0 LOW POWER SHUTDOWN ANALYSIS

4.1 *Scope of the Low Power Shutdown Analysis*

The LPSD analysis is an extension of the at-power PRA to include the POS associated with taking the reactor to hot standby, cold shutdown, mid-loop operation, refueling, and startup. The overall LPSD PRA methodology is the same as the at-power PRA. Unique initiating events, success criteria, and accident response are developed for each POS. An overview of the methodology focusing on the differences to the at-power methods is provided below.

Limited analyses of fire, flood, and seismic initiators are being performed so that these hazards are considered in the LPSD PRA. Fire and flood events are evaluated with bounding analyses so that no unique risk issues associated with the low power operation exist. Unique equipment and structures associated with the LPSD PRA are added to the SEL to consider their seismic design margins.

4.2 *Plant Operating States*

The process of identifying a reasonable set of POS includes consideration of changes in the RCS conditions, impacts on initiating events, safety functions, unavailability of safety trains, success criteria, and evaluation of transition states versus steady-states. The POS selection is based on the following key characteristics:

- RCS level (pressurizer, mid-loop, cavity pool flooded)
- Reactor pressure vessel (RPV) integrity (head on, head off)
- Number of RHR trains operating/available (including their support systems)

Other characteristics (e.g., temperatures, pressures, number of available SGs, number of RCPs running, RPV and pressurizer venting) are evaluated and accounted for in the modeling of each POS.

Table 4-1 provides a summary of the preliminary POS developed for the U.S. EPR and compares them to the operating modes as defined in typical Technical Specifications. POS A and B are analyzed in the at-power PRA model, and the remaining POS are analyzed in the LPSD PRA model. Loss of SFP cooling is also analyzed.

4.3 *Selected Initiating Events for LPSD*

The following provides a summary of the preliminary initiating events specific for the LPSD:

- Loss of RHR: Loss of decay heat removal during various LPSD states could occur because of a loss of RHR/LHSI trains or their supporting systems (e.g., loss of CCW/ESW cooling). Because only one train of heat removal is required to prevent heatup and two, three or four RHR trains are normally available/running during various POS, multiple trains would have to fail to cause an initiating event.
- Loss of Inventory due to Level Drop: Draining the RCS too low and causing cavitation of all heat removal pumps is considered an important event during mid-loop operation and is included as an initiating event. However, automatic isolation features included in the U.S. EPR design reduce the likelihood and improve mitigation of this event.
- Loss of Inventory due to RHR LOCA outside containment: This event is a postulated leak in the RHR system outside containment and subsequent failure to isolate the break. Automatic isolation features included in the U.S. EPR design reduce the likelihood and improve mitigation of this event.

Human-induced events during shutdown are not explicitly modeled. These events are considered to be less likely in the U.S. EPR design when considering the automatic protection features. Human-induced-type events will be evaluated when the plant-specific shutdown procedures are available.

4.4 *Success Criteria for LPSD*

The success criteria are based on actions and systems required to prevent the RCS from boiling and subsequent core uncovery. Some system response and timing requirements are similar to at-power requirements, and some are more relaxed given lower temperatures and pressures during LPSD states. The following are examples:

- SG Relief during SBO: During shutdown, only one SG volume is required to cope with a loss of all cooling for two hours versus the four SGs required during power operation.
- MHSI: During shutdown, partial cooldown is not required for any loss of inventory because RCS pressure is low and secondary side MSRV set points are low enough so that RCS pressure does not exceed MHSI shutoff head.
- RCP Seals: During shutdown, after an RCP pump is tripped, the RCP seal cooling is no longer required.

4.5 *Systems Analysis for LPSD*

The system fault trees developed for the at-power PRA are modified for different success criteria and used in the LPSD PRA. The following summarizes preliminary system fault tree model changes:

- RHR/LHSI trains are modeled as operating in the RHR mode rather than being in standby injection mode (LHSI).
- RHR protective trip is added for the LPSD operation. Low loop level will trip the operating RHR pumps to protect the pumps and allow them to be restarted after level recovery.
- SIS actuation is changed to low delta-Psat in POS Ca and to low loop level in other LPSD POS.
- SFP cooling and makeup systems are modeled to evaluate loss of the SFP cooling as an initiating event and recovery with backup trains.

4.6 *Human Reliability for LPSD*

There are many specific operator actions evaluated in the LPSD PRA. The same methodology used for the at-power PRA model is used for LPSD.

Table 4-1—Example U.S. EPR Plant Operating States

POS	POS Description	Applicable Tech Spec Mode
A	Full Power to Hot Shutdown (T > 550˚F)	Mode 1 – Power Operation Mode 2 – Startup
B	SG Heat Removal (T > 248˚F)	Mode 3 – Hot Standby
Ca	RHR Heat Removal with Level in Pressurizer (T ~ 248 to 131˚F)	Mode 4 – Hot Shutdown Mode 5 – Cold Shutdown
Cb	RHR Heat Removal at Mid-loop with RPV Head On (T ~ 131˚F)	Mode 5 – Cold Shutdown
D	RHR Heat Removal at Mid-loop with RPV Head Off (T ~ 131˚F)	Mode 6 – Refueling
E	Reactor Cavity Flooded (T ~ 131˚F)	Mode 6 – Refueling
F	Core off loaded to spent fuel pool (SFP Cooling modeled)	NA

5.0 COMPUTER CODES

5.1 *PRA Level 1 and 2 Codes*

5.1.1.1 *RiskSpectrum Professional*

The U.S. EPR design certification PRA model is developed and quantified using the RiskSpectrum Professional software code. RiskSpectrum is a product of Relcon AB of Sweden. This software code uses the linked fault tree methodology. Analysis cases are created for fault tree analysis, event tree sequence analysis, and consequence analysis. To accomplish this, base models are modified using house events, exchange events, and boundary condition sets. Multiple minimum cutsets (MCS) results can be merged; an MCS editor allows for further refinement of the results. Several event trees can be linked, including Level 1 event trees with Level 2 containment event trees. A comprehensive set of importance factors can be generated along with uncertainty and time-dependent results.

Basic event reliability parameters can be presented as a probability, failure rate, or frequency and can incorporate MTTR, test interval, time to first test, and mission time within these models. Parameters can be provided as point estimate values or be represented as various distributions, including normal, lognormal, beta, and gamma. CCF modeling is automated using common cause groups and can use either the MGL method or Alpha Factor method.

RiskSpectrum is designed to execute on a personal computer (PC). Test output supplied from Relcon AB is used to validate correct installation and operation of the code.

RiskSpectrum currently has more than 1000 users in 362 organizations in 41 countries. About 40% of the world's nuclear power plants PRAs use RiskSpectrum Professional.

5.1.1.2 *Modular Accident Analysis Program*

MAAP4 is an integrated system code that combines, in one package, models for heat transfer, fluid flow, fission product release and transport, plant system operation and performance, and operator actions. Physical models exist for processes that are important during transients that lead to and go beyond fuel damage. The models are coupled at every time step.

MAAP4 provides an accident analysis tool to study all phases of severe accident studies, including accident management. MAAP4 includes models for accident phenomena that can occur within the primary system, the containment, or auxiliary-type buildings. For a specified reactor and containment system, MAAP4 calculates the progression of the postulated accident sequence (including the deposition of the fission products) from a set of initiating events to either a safe, stable state or to an impaired containment condition (by over-pressure or over-temperature), and the possible release of fission products to the environment.

MAAP version 4.07 is the U.S. EPR version of MAAP4, which contains specific models for U.S. EPR design features. The U.S. EPR has specific containment regions devoted to debris stabilization and long term cooling should a severe accident lead to melting of the reactor core and RPV failure. The modifications performed to the MAAP4 code address the ways that these specific elements of the containment can be represented in the MAAP4 framework. The AREVA NP Severe Accident Evaluation Topical Report (Reference 35) provides further information on MAAP 4.07.

Use of MAAP in the PRA:

Level 1: MAAP is used to perform deterministic thermal-hydraulic analysis to support the development of system success criteria and operator action times.

Level 2: MAAP is used to perform deterministic severe accident analysis—the simulation of the course and progression of a severe accident sequence—and is a key input to a level 2 PRA in three areas:

- To assist in developing the containment event tree and understanding the most likely event progression for the important sequences within a damage state bin.
- To assist in quantifying the containment event tree by aiding in understanding the important phenomena and resulting loads on containment resulting from the severe accident.
- To characterize the source term—the composition, magnitude, and timing of releases to the environment associated with each of the RC bins.

MAAP Benchmarking:

Level 1: A specific benchmarking effort is performed for application of MAAP in the Level 1 PRA. For selected events, use of MAAP is justified by qualitative arguments and comparison to parallel calculations conducted with the S-RELAP5 code. This benchmarking allows deriving suitable Level 1 acceptance criteria when using the MAAP plant model.

Level 2: A description of the MAAP benchmarking performed to support the U.S. EPR severe accident evaluation is described in Reference 35.

5.1.1.3 *S-RELAP5 Accident Analysis Code*

AREVA NP developed the S-RELAP5 safety analysis code to perform LOCA and non-LOCA PWR safety analyses. S-RELAP5 has been approved by the NRC.

S-RELAP5 uses a two-fluid, nonequilibrium, nonhomogeneous, thermal-hydraulic model for transient simulation of the reactor coolant system. The basic S-RELAP5 models include: hydrodynamic, heat transfer, heat conduction, fuel, reactor kinetics, control system, and trip system models. The hydrodynamics includes generic component models (e.g., pumps, valves, accumulators), and some special process models (choked flow and countercurrent flow limitation). The system mathematical models are solved by fast numerical schemes to permit cost-effective computations.

The S-RELAP5 U.S. EPR input model contains detailed nodalization of the primary system including the reactor vessel, cold and hot legs, pressurizer, pressurizer relief valves, primary side of the SGs (4 loops), and the ECCS. For the secondary side, the S-RELAP5 model includes SGs, EFW, MSRVs, MSSVs, and the common header of the steam lines.

S-RELAP5 is used in the PRA to:

- Determine the success criteria for events where the MAAP code is not appropriate such as ATWS events where kinetics feedback effects are needed.
- Benchmark/validate event-specific MAAP calculations and acceptance criteria.

SRELAP5 analyses use realistic input parameters and system assumptions consistent with the PRA approach.

5.1.1.4 *EPRI Human Reliability Analysis Calculator*

The U.S. EPR PRA uses the EPRI HRA Calculator. The EPRI HRA Calculator is a software tool designed to facilitate a standardized approach to HRA. The EPRI HRA Calculator is designed to step PRA analysts through the HRA tasks needed to develop and document Human Failure Events (HFE), and to quantify HEPs. The EPRI HRA Calculator operates on a basic event basis and is based on EPRI's Systematic Human Action Reliability Procedure (SHARP) and SHARP1 methods. The current version of the calculator applies EPRI's Cause-Based Decision Tree Method (CBDTM), the Human Cognitive Reliability/Operator Reactor Experiments (HCR/ORE), the ASEP, the SPAR-H, and the THERP.

For the U.S. EPR design certification PRA model, AREVA NP primarily uses the ASEP method for development of pre-accident HEPs and the SPAR-H method for development of post accident HEPs. The EPRI HRA Calculator incorporates the SPAR-H worksheet, which is a major component of the SPAR-H method, and the SPAR-H dependency rating system. Validation of proper installation and execution of the code is performed.

The EPRI HRA Calculator development is directed by the EPRI HRA/PRA tools Users Group. Membership currently includes 19 utilities comprising more than 60 nuclear power plants in the U.S. and one international member (CANDU Owners Group).

5.2 *PRA Level 3 Codes*

5.2.1 *MACCS2 Code Description*

MACCS2 (Version 1.31.1) (Reference 27) is used for the Level 3 PRA. MACCS2, supplied by SNL, is an atmospheric dispersion/consequence code that estimates the potential offsite effect of postulated accident releases of radioactive material.

MACCS2 requires five input files: MET, SITE, ATMOS, EARLY, and CHRONC. The MET file contains meteorological data, specifically hourly data for one year that includes wind velocity (speed and direction), stability class, and rainfall.

Both the MET file and the SITE file require establishing a specific spatial grid (e.g., increasing concentric circles at 1, 2, 3, 4, 5, 10, 20, 30, 40, 50 miles). These circles are divided into 16 equal sectors, starting with north (N), and working clockwise: NNE, NE, ENE, E, ESE, SE, SSE, S, SSW, SW, WSW, W, WNW, NW, and NNW. These sectors are used to identify the wind direction in the MET file. The sector/circle spatial grid will be used to divide the area around the plant into bins for population data, land usage, watershed index, and regions used in the SITE file.

The other three input files (i.e., ATMOS, EARLY, and CHRONC) represent the functional modules of MACCS2. These modules are overlaid by the phases that MACCS2 uses (i.e., emergency, intermediate, and long-term). ATMOS is used to perform all the calculations that pertain to atmospheric transport, dispersion, and deposition.

ATMOS is also responsible for tracking radioisotope decay during these processes. One plume is modeled for the U.S. EPR Level 3 analysis as provided by the Level 2 MAAP and RC output. The output from ATMOS is used for both EARLY and CHRONC.

EARLY performs all the calculations pertaining to the emergency phase (typically, one week), which begins when the first plume of the release arrives. Mitigative actions during the emergency phase include evacuation, sheltering, and dose-dependent relocation. EARLY considers exposure pathways, such as cloudshine, groundshine, and resuspension inhalation. Parameters for the EARLY file included cloudshine shielding factor and groundshine shielding factor. The parameters of the evacuation model are specified in the EARLY file.

CHRONC performs all the calculations pertaining to the intermediate and long-term phases. The intermediate phase begins as the emergency phase ends. Exposure pathways considered are groundshine and resuspension inhalation. Doses from food and water ingestion are not considered. The dose model used is simple: if the dose threshold is exceeded, the population is relocated to uncontaminated areas for the duration of the intermediate phase; otherwise, the population is subjected to dose for the entire phase. The long-term phase begins at the end of the intermediate phase. Exposure pathways for the long-term phase include: groundshine, resuspension inhalation, and food and water ingestion.

5.2.2 *RiskIntegrator*

RiskIntegrator is an Excel spreadsheet application that aids the processing of Level 3 PRA output. RiskIntegrator facilitates the linkage between the Level 1 and 2 PRA results, and the Level 3 PRA results. Consequently, when a change is made in the Level 1 or 2 PRA results, the output of the Level 3 PRA can be regenerated by RiskIntegrator without re-executing MACCS2.

RiskIntegrator is an Excel spreadsheet program with a Visual Basic interface. The RiskIntegrator spreadsheet requires the following files:

- Conditional Probability Matrix (CPM) (from Level 1 PRA results)
- Release Category Matrix (RCM) (from Level 2 PRA results)
- Initiating Event Look-up Table

- MACCS2 output file

The CPM contains two dimensions: initiating events and plant damage states. The two dimensions of the RCM are RC and plant damage states. The initiating event look-up table contains an initiating event code, flag for internal versus external events, textual description, and a group designation. The look-up table is used to display PRA results by initiating event groups. The MACCS2 output file is used directly as created by MACCS2.

The Visual Basic interface and Excel perform relatively simple matrix multiplications. A selected set of hand calculations is performed and compared to the output of RiskIntegrator to validate proper execution.

6.0 SUMMARY AND CONCLUSIONS

The U.S. EPR design certification PRA is being developed in parallel with U.S. design activities. Probabilistic evaluation of the U.S. EPR design features has benefited as a result of international cooperation between the U.S. and European divisions of AREVA. This cooperation is ongoing and includes sharing of PRA experience and technology through technical review meetings and collaborative work assignments.

In the design certification phase, the PRA is being developed and is continuously reviewed and updated to reflect the latest plant design configuration. The PRA discipline is integrated into the on-going design process via the AREVA NP U.S. EPR project design directive and design change process. Therefore, as the design is developed, the PRA remains current, and is continuously used to communicate any risk insights for design decision-making. The design certification PRA will use an input design freeze date, and any design changes made after the freeze date will be evaluated qualitatively for potential impact on the PRA.

This PRA Methods Report provides an overview of the scope, objectives, basic approach, methodology, and computer codes to be employed in the design certification PRA.

The information presented demonstrates that the design certification PRA, when completed, will provide a comprehensive and complete assessment of the U.S. EPR design and will meet the objectives for design certification, which include:

- Meet regulatory requirements for U.S. design certification.
- Demonstrate the robustness of the U.S. EPR design, and that the design satisfies the AREVA NP design objectives and NRC probabilistic safety objectives with margin.
- Provide a useful tool to support design decision making to enhance plant safety, and support developments of risk-informed programs.

7.0 REFERENCES

1. "Early Site Permits; Standard Design Certification; and Combined Licenses for Nuclear Power Plants," 10 CFR Part 52.

2. "Evolutionary Light Water Reactor (LWR) Certification Issues and Their Relationship to Current Regulatory Requirements," SECY 90-016, January 12, 1990.

3. "An Approach for Determining the Technical Adequacy of Probabilistic Risk Assessment Results for Risk-Informed Activities," Regulatory Guide 1.200, February 2004.

4. "An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis," Regulatory Guide 1.174, Revision 1, November 2002.

5. J.P. Poloski, et al., "Rates of Initiating Events at U.S. Nuclear Power Plants: 1987-1995," NUREG/CR-5750, February 1999.

6. "EPRI Advanced Light Water Reactor Utility Requirements Document," ALWR-URD, December 1995.

7. D. L Kelly, J. L Auflick, and L. N Haney, "Assessment of ISLOCA Risk Methodology and Application to a Westinghouse Four-Loop Ice Condenser Plant," NUREG/CR-5744, May 1992.

8. E. T Burns, et al., "ISLOCA Evaluation Guidelines," EPRI-NSAC-154, September 1991.

9. "Standard for Probabilistic Risk Assessment for Nuclear Power Plant Applications," Addenda to ASME RAS-2002, ASME-RA-Sb-2005, December 2005.

10. S. A Eide, C. D. Gentillon, T. E Wierman and D. M. Rasmuson, “Reevaluation of Station Blackout Risk at Nuclear Power Plants,” NUREG/CR-6890, December 2005.

11. S. A. Eide, S. V. Chmilewski and T. D. Swantz, “Generic Component Failure Database for Light Water and Liquid Sodium Reactor PRAs,” EGG-SSRE-8875, EG&G Idaho, 1990.

12. “Centralized Reliability and Events Database (ZEDB) – Reliability Data for Nuclear Power Plant Components: Analysis for 2002, VGB Power Tech Service Gmbh.”

13. “European Industry Reliability Data Bank,” EIReDA, EIReDA95, Volume 2, 1977/1993.

14. A. Mosleh, D. M. Rasmuson, and F. M. Marshall, “Guidelines on Modeling Common-Cause Failures in Probabilistic Risk Assessment,” NUREG/CR-5485, November 1998.

15. T. E. Wierman, D. M. Rasmuson and N. B. Stockton, “Common Cause Failure Event Insights,” NUREG/CR-6819, May 2003.

16. “Reliability Studies,” NUREG/CR-5500, 2004 Updates, October-November 2005.

17. “Component Performance Studies,” NUREG-1715, 1999.

18. Letter, Ronnie L. Garner (AREVA NP) to Document Control Desk, "EPR Design Description," NRC:05:02, August 12, 2005.

19. “Requirements for Reduction of Risk from Anticipated Transients Without SCRAM (ATWS) Events for Light-Water-Cooled Nuclear Power Plants,” 10 CFR 50.62.

20. "Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer-Bases Instrumentation and Control Systems," NRC Branch Technical Position-HICB-19, Revision 4, June 1997.

21. Letter, James F. Mallay (Siemens) to Document Control Desk, "Publication of EMF-2110 (NP)(A) Revision 1, TELEPERM XS: A Digital Reactor Protection System," ML003732631, dated July 12, 2002.

22. T. E. Wierman, S. T. Beck, M. B. Colley, S A. Eide, C. D. Gentillon and W. E. Kohn, "Reliability Study: Babcock & Wilcox Reactor Protection System, 1994–1998," NUREG/CR-5500, Volume 11, 1984-1998, INEEL, November 2001.

23. "Amendments to 10 CFR 50 Related to Anticipated Transients Without Scram (ATWS) Events," SECY-83-293, NRC, July 19, 1983.

24. "Generic Implications of ATWS Events at the Salem Nuclear Power Plant," NUREG-1000, Volumes 1 and 2, August 1983.

25. Swain A., "Accident Sequence Evaluation Program Human Reliability Analysis Procedure," NUREG/CR-4772, SAND86-1996, February 1987.

26. D. Gertmen, H. Blackman, J. Marble, J. Byers and C. Smith, "The SPAR-H Human Reliability Analysis Method," NUREG/CR-6883, INL/EXT O5-00509, Idaho National Laboratory, August 2005.

27. Chanin and Young 1998: D. Chanin, and M. L. Young, "Code Manual for MACCS2," NUREG/CR-6613 Vol. 1, SAND97-0594, prepared for U.S. NRC and U.S. DOE, May 1998.

28. "EPRI/NRC-RES Fire PRA Methodology for Nuclear Power Facilities," EPRI 1011989, NUREG/CR-6850, September 2005.

29. "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light Water Reactor (ALWR) Designs," SECY-93-087, April 2, 1993.

30. “External Events in PRA Methodology Standard,” ANSI-ANS-58.21-2003.

31. N. M Newmark and W. J. Hall “Development of Criteria for Seismic Review of Selected Nuclear Power Plants,” NUREG/CR-0098, May 1978.

32. “Assessment of a Performance Based Approach for Determining the SSE Ground Motion for New Plant Sites, V.2, Seismic Hazards Results at 28 Sites,” EPRI Product ID #1012045, Final Report, May 2005.

33. “Assessment of a Performance Based Approach for Determining the SSE Ground Motion for New Plant Sites, V.1, Performance Based Seismic Design Spectra,” EPRI Product Code #1012044, Final Report, June 2006.

34. “Methodology for Developing Seismic Fragilities,” EPRI-TR-103959, Research Project RP2722-23, Final Report, Prepared for EPRI, Palo Alto, CA, June 1994.

35. Letter, Ronnie L. Garner (AREVA NP) to Document Control Desk, "Request for Review and Approval of ANP-10268P Revision 0, U.S. EPR Severe Accident Evaluation Topical report," NRC 06:049, October 31, 2006.