Chapter 19

SCE&G
A SCANA COMPANY

VCS UFSAR Table of Contents

VCS UFSAR Formatting Legend

Color	Description
	Original Westinghouse AP1000 DCD Tier 2 & Tier 2*, Revision 19 content
	Departures from AP1000 DCD Tier 2 & Tier 2*, Revision 19 content
	Standard FSAR content
	Site-specific FSAR content
	Linked cross-references (chapters, appendices, sections, subsections, tables, figures, and references)

Section Title Page

LIST OF TABLES

LIST OF TABLES (CONTINUED)

LIST OF FIGURES

LIST OF FIGURES (CONTINUED)

Chapter 19 Probabilistic Risk Assessment

19.1 Introduction

Part 52 of the 10 Code of Federal Regulations requires that a probabilistic risk assessment (PRA) be submitted as a part of an application for design certification. The PRA provides an evaluation of the design, including plant, containment, and typical site analyses that consider both internal and external events.

The AP1000 design process includes a risk assessment of the design prior to being finalized to optimize the plant with respect to safety. Westinghouse accomplishes this by committing to the early application of probabilistic analysis techniques in the AP1000 design process. This work resulted in information used in the selection of design alternatives, with a goal that the overall level of safety of the completed design exceeds design objectives.

19.1.1 Background and Overview

The AP1000 PRA was developed to support the application for Design Certification of the AP1000 nuclear plant. The AP1000 design is based extensively on the AP600 standard nuclear plant that received Design Certification in December 1999. The AP600 PRA, which was reviewed by the US NRC in detail during the seven-year review of the AP600, is used as the starting point for the AP1000 PRA. Since the configuration of the AP1000 reactor and safety systems is the same as the AP600, the AP600 PRA is used as the basis of the AP1000 PRA with relevant changes implemented in the model to reflect the AP1000 design changes. AP1000 plant-specific T&H analyses are performed in order to determine the system success criteria. The core damage frequency and large release frequency are calculated for internal events. The external events and shutdown models are also assessed to derive plant insights and plant risk conclusions.

The purpose of the PRA is to provide inputs to the optimization of the AP1000 design and to verify that the US NRC PRA safety goals have been satisfied. As in the AP600, the PRA is being performed interactively with the design, analysis and operating procedures. The PRA results show that there are only minor impacts on the PRA results compared to AP600, and that the very low risk of the AP600 has been maintained in the AP1000; the AP1000 PRA meets the US NRC safety goals with significant margin. Insights from the analysis are provided discussing the effect on the PRA of differences between the AP600 and the AP1000 designs.

19.1.2 Objectives

The objectives of the AP1000 PRA are to:

- Provide an integrated view of the AP1000 behavior in response to transients and accidents, including severe accidents
- Satisfy the NRC regulatory requirements that a design-specific PRA be conducted as part of the application for design certification (10 CFR 52.47(a)(i)(v))
- Demonstrate that the design meets the proposed safety goals for core damage frequency and large fission product releases
- Construct a PRA Level 1 (core damage frequency), Level 2 (large release frequency), and Level 3 (offsite dose) model that is consistent with the AP1000 design configuration and operation requirements and the ALWR URD requirements on PRA methodology (Reference 19.1-1)

- Demonstrate the low vulnerability and insensitivity of the AP1000 design to human interaction
- Provide input to the design process (that is, provide a tool to investigate detailed design solutions and operational strategies to optimize AP1000 safety)
- Demonstrate compliance with the hydrogen control criteria set forth in 10 CFR 50.44
- Serve as a basis for an accident management program

19.1.3 Technical Scope

The technical tasks for the AP1000 PRA are defined in the following categories:

- Level 1 Analysis for Internal Events
- Level 2 Analysis for Internal Events
- Level 3 Analysis for Internal Events
- Sensitivity, Importance, and Uncertainty Analyses for Internal Events
- Shutdown Risk Assessment
- External Events Risk Assessment

The ALWR URD document serves as the base document to define the source of data.

The Level 1 analysis includes:

- Internal initiating events evaluation
- Event tree and success criteria analyses
- Plant systems analysis using fault tree models
- Common cause failure and human reliability analyses
- Data analysis
- Fault tree and event tree quantification to calculate the core damage frequency

The Level 2 analysis includes:

- An evaluation of severe accident phenomena and fission product source terms
- Modeling of the containment event tree and associated success criteria
- Analysis of hydrogen burning and mixing

The Level 3 analysis is an offsite dose evaluation.

The low power and shutdown analysis includes Level 1 shutdown assessment.

External events analyses include:

- Internal fire assessment
- Internal flooding assessment
- Seismic margin assessment
- High winds assessment
- External flooding assessment
- Transportation and nearby facility accident assessment

19.1.4 Project Methodology Overview

Guidelines have been developed for the major tasks. These guidelines provide homogeneity among similar tasks that are performed by different analysts (such as fault tree construction) and to

standardize the methodology for selected tasks (such as human reliability or common cause failure analysis).

The major activities performed during this study include:

- Initiating event and event tree analysis - Evaluations are performed to identify a comprehensive set of initiating events. This evaluation includes review of pressurized water reactor (PWR) operating experience, past PRAs, and consideration of AP1000-specific features. For each initiating event category, an event tree is constructed to model the accident sequences that may result.

- Success criteria - Extensive analyses are performed with MAAP4 (Reference 19.1-2), NOTRUMP, and other codes to determine the success criteria for system mitigation following initiating events.

- Analysis of individual systems - Qualitative analysis and fault tree construction are performed for safety-related and nonsafety-related front-line systems and supporting systems that contribute to prevention or mitigation of severe accident events. The analysis identifies the importance of each component for each system.

- Human reliability analysis - A detailed human reliability analysis is performed, with emphasis on the evaluation of the effect of single operator decisions on more than one system.

- Common cause failure analysis - An analysis is performed to identify and model the dependencies (common cause failures), both internal to individual systems and among systems, that use similar components exposed to similar environments.

- Severe accident analysis - Analyses are performed with the MAAP4 code to study the progression of severe accident sequences and to define the radionuclide source terms.

- Dose evaluation - The dose at the plant site boundary for the various fission product release categories are calculated.

- Hydrogen control analysis - Analyses to demonstrate the effectiveness of the hydrogen igniters are carried out using the MAAP4 code.

- Shutdown assessment - The frequency of core damage is assessed for low power and shutdown conditions.

- Fire and flood assessment - Internal fire and internal flood risk assessment evaluate potential vulnerabilities within the plant.

- Seismic margin assessment - Seismic margin methodology is used to identify potential seismic vulnerabilities and to assess the margin beyond the design-level safe shutdown earthquake.

- Assembly of results - The frequency of the dose at the site boundary exceeding a certain level is obtained by combining the results of the core damage analysis, severe accident analysis, and dose analysis.

19.1.5 Results

The AP1000 PRA is an integrated view of the AP1000 behavior in response to transients and accidents, including severe accidents.

The AP1000 core damage frequency for internal events from at-power conditions is extremely low. The core damage frequency calculated for internal events at shutdown conditions is also very low. The combined core damage frequency from internal events at power and at shutdown conditions meets the NRC and URD safety goals with substantial margin.

The AP1000 large release frequency of the dose at the site boundary exceeding 1 rem effective dose equivalent in 24 hours after core damage for internal events from at-power conditions is very low. Like the core damage frequency, the combined large release frequency from internal events at power and at shutdown conditions meets the NRC safety goals with substantial margin.

In the AP600 licensing process, an initial set of sensitivity analyses were made to assess the importance of non-safety related systems. Later on, this exercise grew into a full-fledged PRA model which was named the focused PRA. The focused PRA was performed to assess the importance of the nonsafety-related systems. The results of the focused PRA (Reference 19.1-3) demonstrated that the AP600 passive plant design was able to meet the NRC safety goals crediting only safety-related equipment, with no credit for any of the nonsafety-related systems. To resolve the regulatory treatment of nonsafety-related systems, Westinghouse and the NRC agreed to availability controls of selected nonsafety-related systems for the purposes of providing defense-in-depth as well as investment protection.

The AP1000 PRA demonstrates a very similar low risk profile for the AP1000 as for the AP600. Sensitivity studies performed for the AP1000 demonstrates that no nonsafety-related system is of high risk importance. The same nonsafety-related system availability controls adopted for the AP600 will be applied to the AP1000 for the purpose of providing defense-in-depth and investment protection and are discussed in Section 16.3.

There are no critical operator actions in the AP1000 PRA analyses. The core damage frequency remains relatively small even if all operator actions are assumed to fail. Only a small improvement in the core damage frequency can be realized by improving the reliability of the plant operators.

The AP1000 containment is capable of providing an effective barrier to the release of fission-products to the environment and includes effective hydrogen control measures. The AP1000 design meets the criteria in 10 CFR 50.44.

These results demonstrate that the AP1000 meets and exceeds the design goals specified in Subsection 19.1.2.

Insights regarding the AP1000, derived from or verified by this PRA, include:

- Passive safety-related systems eliminate the dependence of safety-related system operation on ac electric power and compressed air. This significantly reduces the core damage frequency resulting from a loss of offsite power or station blackout event.

- Reactor coolant pump seal loss-of-coolant accidents are eliminated because of the use of sealless reactor coolant pumps.

- Simplified passive safety-related systems reduce the need for, and importance of, operator action.

- The analysis shows that many of the events, which in the past were leading contributors to the risk of nuclear power plants, are not as significant for the AP1000. The contribution of interfacing systems loss-of-coolant accidents, which are typically the highest risk severe accident sequences, is made insignificant by the design of the AP1000.

- The ability to flood the reactor cavity is an important contributor to maintaining a low release frequency for AP1000. This feature and the design of the reactor insulation that provides for cooling of the reactor vessel keep a damaged core inside the reactor vessel. This reduces the potential for ex-vessel severe accident events.

- The AP1000 design provides a passive means of maintaining the containment integrity by removing decay heat from the containment with water on the containment shell or through air cooling. This cooling ability reduces the potential of containment failure due to overpressurization after severe accident.

- The AP1000 containment design enhances the deposition of aerosols before they are released to the environment and reduces the potential environmental effects of a severe accident that has failed the containment.

19.1.6 Plant Definition

19.1.6.1 General Description

See Chapter 1.

19.1.6.2 AP1000 Design Improvement as a Result of Probabilistic Risk Assessment Studies

Design improvements were incorporated in the AP600 design based on the results of the AP600 PRA and other design analyses and are discussed in Reference 19.1-3. These improvements have been retained in the AP1000 design. Additional design changes have been incorporated in the AP1000 as a result of the AP1000 PRA. The most significant design changes prompted by the AP1000 PRA are:

- Two recirculation lines, each containing a motor-operated valve and a squib valve or a check valve and a squib valve in series, are used to provide recirculation flow from containment sump to the core through direct vessel injection line. Diversity is provided in the actuation by using diverse squib valves. The motor-operated valve is designed so that it remains open in case of failure.

- Three parallel supply lines allow water flow from PCCWST to the containment shell. Diversity is provided in the actuation by using motor-operated valves for one path.

19.1.7 References

19.1-1. Advanced Light Water Reactor Requirements Document, Volume III, Appendix A to Chapter 1, "PRA Key Assumptions and Groundrules," Revisions 5 and 6, December 1993.

19.1-2. EPRI MAAP 4.0 Users Manual.

19.1-3. AP600 PRA.

19.2 Internal Initiating Events

The design certification of the AP1000 included consideration by the NRC of the topic referred to in this section.

19.3 Modeling of Special Initiators

The design certification of the AP1000 included consideration by the NRC of the topic referred to in this section.

19.4 Event Tree Models

The design certification of the AP1000 included consideration by the NRC of the topic referred to in this section.

19.5 Support Systems

The design certification of the AP1000 included consideration by the NRC of the topic referred to in this section.

19.6 Success Criteria Analysis

The design certification of the AP1000 included consideration by the NRC of the topic referred to in this section.

19.7 Fault Tree Guidelines

The design certification of the AP1000 included consideration by the NRC of the topic referred to in this section.

19.8 Passive Core Cooling System - Passive Residual Heat Removal

See Subsection 6.3.1.1.1.

19.9 Passive Core Cooling System - Core Makeup Tanks

See Subsections 5.4.13 and 6.3.2.2.1.

19.10 Passive Core Cooling System - Accumulator

See Subsection 6.3.2.2.2.

19.11 Passive Core Cooling System - Automatic Depressurization System

See Subsections 5.4.6 and 6.3.2.2.8.5.

19.12 Passive Core Cooling System - In-containment Refueling Water Storage Tank

See Subsection 6.3.2.2.3.

19.13 Passive Containment Cooling

See Subsection 6.2.2.

19.14 Main and Startup Feedwater System

See Subsection 10.4.9.

19.15 Chemical and Volume Control System

19.15.1 System Description

See Subsection 9.3.6.2.

19.15.2 System Operation

See Subsection 9.3.6.4.

19.15.3 Performance during Accident Conditions

See Subsection 9.3.6.4.5.

19.15.4 Initiating Event Review

The design certification of the AP1000 included consideration by the NRC of the topic referred to in this section.

19.15.5 System Logic Models

19.15.5.1 Assumptions and Boundary Conditions

The following assumptions are used for the chemical and volume control system PRA model:

a. - i. The design certification of the AP1000 included consideration by the NRC of the topic referred to in this section.

j. Either one of the two makeup pumps is sufficient to deliver borated water to the reactor coolant system. To simplify the PRA model, it is assumed that one makeup pump is always the operating pump and the other makeup pump is always the standby pump.

k. - q. The design certification of the AP1000 included consideration by the NRC of the topic referred to in this section.

19.15.5.2 Fault Tree Models

The design certification of the AP1000 included consideration by the NRC of the topic referred to in this section.

19.15.5.3 Human Interactions

The design certification of the AP1000 included consideration by the NRC of the topic referred to in this section.

19.15.5.4 Common Cause Failures

The design certification of the AP1000 included consideration by the NRC of the topic referred to in this section.

TABLES 19.15-1 THROUGH 19.15-9 NOT USED.
FIGURE 19.15-1 NOT USED.

19.16 Containment Hydrogen Control System

See Subsection 6.2.4.

19.17 Normal Residual Heat Removal System

See Subsection 5.4.7.

19.18 Component Cooling Water System

See Subsection 9.2.2.

19.19 Service Water System

See Subsection 9.2.1.

19.20 Central Chilled Water System

See Subsection 9.2.7.

19.21 ac Power System

See Subsection 8.3.1.

19.22 Class 1E dc & UPS System

See Subsection 8.3.2.1.1.

19.23 Non-Class 1E dc & UPS System

See Subsection 8.3.2.1.2.

19.24 Containment Isolation

See Subsection 6.2.3.

19.25 Compressed and Instrument Air System

See Subsection 9.3.1.

19.26 Protection and Safety Monitoring System

See Subsection 7.1.2.

19.27 Diverse Actuation System

See Subsection 7.7.1.11.

19.28 Plant Control System

See Subsection 7.1.3.

19.29 Common Cause Analysis

The design certification of the AP1000 included consideration by the NRC of the topic referred to in this section.

19.30 Human Reliability Analysis

The design certification of the AP1000 included consideration by the NRC of the topic referred to in this section.

19.31 Other Event Tree Node Probabilities

The design certification of the AP1000 included consideration by the NRC of the topic referred to in this section.

19.32 Data Analysis and Master Data Bank

The design certification of the AP1000 included consideration by the NRC of the topic referred to in this section.

19.33 Fault Tree and Core Damage Quantification

The design certification of the AP1000 included consideration by the NRC of the topic referred to in this section.

19.34 Severe Accident Phenomena Treatment

19.34.1 Introduction

This section describes how the AP1000 containment addresses challenges from severe accident phenomena, and how the challenges are evaluated in the probabilistic risk assessment (PRA). In the PRA, the Modular Accident Analysis Program (MAAP) version 4.04 code (Reference 19.34-8) is used to evaluate severe accident scenarios. Severe accident phenomenological uncertainties are treated with Risk-Oriented Accident Analysis Methodology (ROAAM) (Reference 19.34-2) phenomenological evaluations, with AP1000-specific decomposition event tree phenomenological evaluations, or with assumptions that certain low-frequency severe accident phenomena fail the containment. The objective of these studies is to show, with a high degree of confidence, that the AP1000 containment will accommodate the effects of severe accidents in a range of scenarios for at least the first 24 hours after the onset of core damage. Such evaluations demonstrate the robustness of the containment design.

19.34.2 Treatment of Physical Processes

The following eight issues are identified in Reference 19.34-1 as being representative of the phenomenological issues pertaining to severe accident conditions:

1. Loss-of-coolant accident (LOCA)
2. Fuel-coolant interaction (steam explosion)
3. Hydrogen combustion and detonation
4. Melt attack on concrete structure or containment pressure boundary
5. High-pressure melt ejection
6. Core-concrete interaction (CCI)
7. Containment pressurization from decay heat
8. Elevated temperature (equipment survivability)

The challenge to the containment integrity from a LOCA blowdown is covered in the containment design basis and is not specifically addressed here. Treatment of physical processes affecting the remaining challenges is discussed in this chapter.

19.34.2.1 In-Vessel Retention of Molten Core Debris

In-vessel retention (IVR) of core debris by external reactor vessel cooling is a severe accident mitigation attribute of the AP1000 design; it is discussed in detail in Section 19.39. With the reactor vessel intact and debris retained in the lower head, phenomena such as molten core-concrete interaction and ex-vessel steam explosion, which occur as a result of core debris relocation to the reactor cavity, are prevented.

The AP1000 reactor vessel insulation and containment geometry promote in-vessel retention. Engineered design features of the AP1000 containment flood the containment reactor cavity region during accidents, and thereby, submerge the reactor vessel in water.

Chapter 39 of the AP1000 PRA presents an AP1000-specific evaluation to determine the likelihood that sufficient heat can be removed from the outside surface of the submerged reactor pressure vessel lower head to prevent reactor vessel failure and relocation of debris to containment. The methodology used to quantify the margin to vessel failure in Reference 19.34-2 for the AP600 was adapted to the AP1000. For the AP1000 the methodology assumes that:

- The RCS is depressurized.
- The reactor vessel is submerged above the 98-ft elevation in the containment.
- The reflective insulation promotes the two-phase natural circulation in the reactor vessel cooling annulus.
- The reactor vessel external surface is bare metal.

The containment event tree includes a node to ascertain that the reactor coolant system (RCS) is depressurized and a node to determine if adequate water is available in the cavity to achieve two-phase natural circulation. Success at both of these nodes is required to demonstrate that the conditions and assumptions of the IVR analysis are met. The AP1000 design specifies that the reactor vessel insulation is designed appropriately and that the outer surface of the reactor vessel promotes wetability.

Accounting for the uncertainties in thermal-hydraulic parameters, the heat fluxes to the vessel wall and reactor vessel internals from the debris pool are calculated. The results show large margin to failure for the reactor vessel if it is externally cooled by water.

19.34.2.2 Fuel-Coolant Interaction (Steam Explosions)

A steam explosion may occur as a result of molten metal or oxide core debris mixing with water and interacting thermally. Steam explosions are postulated to occur inside the reactor vessel when debris relocates from the core region into the lower plenum and in the reactor cavity if the vessel fails and debris is ejected from it into water in the reactor cavity.

19.34.2.2.1 In-Vessel Fuel-Coolant Interaction

In-vessel steam explosions were studied extensively in the AP600 analyses. A ROAAM analysis of the AP600 reactor vessel lower head integrity under in-vessel steam explosion loading is presented in Reference 19.34-3. Typically, in-vessel steam explosion analyses focus on the α-mode containment failure, which is induced by the reactor vessel upper head failure. The ROAAM analysis focused on failure of the lower head since that steam explosion vessel failure mode would impair the in-vessel retention capability of the reactor vessel. The ROAAM analysis concludes that lower-head vessel failure from in-vessel steam explosion is physically unreasonable with very large margin to failure.

Based on the in-vessel core relocation scenario for the AP1000, the in-vessel steam explosion ROAAM analysis presented for the AP600 can be extended to the AP1000. The mass flow rate, superheat and composition of debris in the relocation from the upper core region to the lower head is expected to be essentially the same as the AP600. The geometry of the lower head of the AP1000 is the same as the AP600. Therefore, it is reasonable to extend the results of the AP600 in-vessel steam explosion ROAAM analysis to the AP1000.

The results of the in-vessel steam explosion ROAAM can also be extended to containment failure induced by in-vessel steam explosions (α-mode containment failure). The likelihood for vessel failure and subsequent containment failure due to in-vessel steam explosion is so small as to be negligible.

This conclusion is in agreement with the conclusions of the U.S. Nuclear Regulatory Commission (NRC)-sponsored Steam Explosion Review Group (Reference 19.34-4).

19.34.2.2.2 Ex-Vessel Fuel-Coolant Interaction

The first level of defense for ex-vessel steam explosion is the in-vessel retention of the molten core debris. If molten debris does not relocate from the vessel to the containment, there are no conditions for ex-vessel steam explosion. In the event that the reactor cavity is not flooded and the vessel fails, the PRA containment event tree assumes that the containment fails in the early time frame.

An analysis of the structural response of the reactor cavity was performed for the AP600 (Reference 19.34-5, Appendix B). As in the in-vessel steam explosion analysis, the results of this AP600 ex-vessel steam explosion analysis are extended to the AP1000. The vessel failure modes for AP600 and AP1000 are the same. The initial debris mass, superheat and composition are assumed to be the same as the AP600. The reactor cavity geometry and water depth prior to vessel failure are the same as AP600. Therefore, the results of the AP600 ex-vessel steam explosion analysis are considered to be appropriate for the AP1000.

19.34.2.3 Hydrogen Combustion and Detonation

A decomposition event tree analysis discussed in Section 19.41 evaluates the potential for hydrogen combustion threatening the containment integrity during a severe accident sequence in the AP1000. The analysis examines diffusion flame burning and local detonation occurring during in-vessel hydrogen generation prior to hydrogen mixing in the containment and global deflagration and detonation, which may occur later when the hydrogen is mixed throughout the containment. Only in-vessel hydrogen generation is considered, since vessel failure and ex-vessel debris relocation is assumed to fail containment.

The AP1000 provides defense-in-depth to address hydrogen diffusion flames that may challenge containment integrity. The first level of defense is the stage four automatic depressurization system (ADS Stage 4) lines from the RCS, which prevent significant hydrogen releases to the in-containment refueling water storage tank (IRWST) and Passive Core Cooling System (PXS) compartments. ADS Stage 4 vents from the RCS hot legs to the loop compartments, which are shielded from the containment shell and have a constant source of oxygen from the natural circulation in the containment. Hydrogen can burn as a diffusion flame in the loop compartments without threatening the containment integrity. If ADS Stage 4 fails, the AP1000 has provided design considerations in IRWST vents to mitigate diffusion flames near the containment walls. Vents from the passive injection system compartments and chemical volume and control system compartment are located away from the containment shell and penetrations in order to mitigate the threat from hydrogen diffusion flames.

Containment failure from a directly initiated detonation wave is not considered to be a credible event for the AP1000 containment. There are no ignition sources of sufficient energy to directly initiate a detonation in the AP1000 containment. Deflagration to detonation transition (DDT) is considered to be the only likely mechanism to produce a detonation in the AP1000 containment.

The likelihood of DDT in the AP1000 containment is evaluated locally in confined compartments during in-vessel hydrogen generation and globally after in-vessel generation is concluded and hydrogen is mixed in the containment. For a DDT to occur, the combination of the gas mixture sensitivity to detonation and the geometric configuration potential for flame acceleration must be conducive to DDT. Since the hydrogen concentration necessary to form a detonable mixture depends on the size of the enclosure, concentration requirements for DDT in different regions of the AP1000 containment are extrapolated from the FLAME facility data (Reference 19.34-6) using scaling arguments based on the detonation cell width. The geometric requirement is evaluated considering aspects such as the degree of confinement and the extent and type of obstacles present in the

postulated flame propagation path. In all cases, DDT is assumed to result in containment failure in the containment event tree analysis.

Global hydrogen deflagration and the potential for containment failure are modeled on the containment event tree. Adiabatic, isochoric, complete combustion (AICC) is assumed, and peak pressure probability distributions are developed for the accident scenarios. The probability of containment failure due to hydrogen deflagration is evaluated from the containment failure probability distribution combined with the peak pressure probability distribution.

19.34.2.4 High-Pressure Melt Ejection

The AP1000 incorporates design features that prevent high-pressure core melt. These features include the passive residual heat removal (PRHR) system and the ADS. These design features provide primary system heat removal and depressurization to prevent high pressure core damage conditions. The consequences from postulated high pressure melt ejection (HPME) are mitigated by the containment layout which provides a torturous pathway to the upper compartment, and no direct pathway for the impingement of debris on the containment shell.

In high-pressure core damage sequences the potential exists for creep-rupture-induced failures of the RCS piping at the hot-leg nozzles, the surge line, the steam generator tubes and, given debris relocation to the lower plenum, in the reactor vessel lower head. Failure of the hot-leg nozzle or surge line prior to failures of other components results in the rapid depressurization of the RCS. Failure of the steam generator tubes results in a containment bypass and a large release of fission products to the environment. Failure of the lower head of the reactor vessel results in the potential for HPME.

Hot-leg nozzle failure is expected prior to steam generator tube failure, but because of large uncertainties, hot-leg nozzle creep rupture failure is not credited with preventing steam generator tube failure. In the PRA, steam generator tube failure is assumed for high-pressure sequences in the containment event tree analysis unless operator action to depressurize the RCS with the ADS is successful.

19.34.2.5 Core Debris Coolability

In accident sequences where the reactor pressure vessel failure is not prevented, core debris may be discharged into the reactor cavity. The likely vessel failure modes produce a low pressure melt ejection (LPME) to the containment. The AP1000 cavity design provides area for the core debris to spread. Condensate from the passive containment cooling system (PCS) returns to the reactor cavity, thereby providing a long-term supply of water to cool the core debris.

At vessel failure it is very likely that the cavity will be filled with water from the RCS, core makeup tanks (CMTs), and accumulators to at least the 83-ft elevation. There are significant uncertainties associated with debris spreading into a water-filled cavity. Debris-spreading is mainly a function of the highly uncertain vessel failure mode. A large-scale lower-head failure releasing debris at a high rate would enhance spreading, while a localized failure mode would release debris at a slow rate, which would most likely cause the debris to pile up under the reactor vessel and minimize spreading.

Given the uncertainties in the debris-spreading and in non-condensable gas generation and combustion, the containment event tree analysis does not credit containment integrity in the event of failure of the lower head of the vessel and relocation of the core.

A limited set of deterministic analyses of debris spreading and core-concrete interaction in the AP1000 cavity is presented in Appendix 19B. The analyses show that basemat melt-through is not predicted to occur within 24 hours of the accident initiation. Basemat melt through is predicted to

occur before pressurization of the containment by non-condensable gases challenges the containment integrity.

19.34.2.6 Containment Pressurization from Decay Heat

The AP1000 containment is cooled via the PCS (see Section 19.40). Evaporative water cooling of the containment shell provides long term containment cooling and limits the containment pressure to less than the design pressure for all severe accident events except hydrogen combustion (which is addressed separately). Containment water is provided to the top of the containment via redundant, diverse system of valves and lines, including a line that can be connected to an outside water source, such as a fire truck.

In the unlikely event that water cannot be supplied to the top of the containment shell for an extended period of time, air-only cooling by air flowing through the PCS annulus provides significant cooling to the containment. Under the right environmental conditions, the containment is expected to reach an equilibrium pressure that will not challenge containment integrity. However, under nominal-to-conservative environmental conditions, containment integrity by air-cooling alone cannot be assured. In this case, containment failure is predicted to occur more than 24 hours after accident initiation.

A significant amount of time is available for operator action to vent the containment under the severe accident management guidance (SAMG). Containment venting mitigates uncontrolled releases of fission products from a failed containment. The AP1000 can be vented on an ad-hoc basis under the SAMG from a number of containment penetrations. Containment venting also reduces the partial pressure of non-condensable gases in the containment, and thus creates a new containment underpressure failure mode that may occur if containment is cooled after venting.

19.34.2.7 Elevated Temperatures (Equipment Survivability)

Reference 19.34-7 states that equipment identified as being useful to mitigate the consequences of severe accidents must be designed to provide reasonable assurance that it will continue to operate in a severe accident environment for the length of time needed to accomplish its function. Also, 10 CFR 50.44 requires safety equipment to continue performing its function after being exposed to a containment environment created as a consequence of generating a quantity of hydrogen equivalent to that from 100-percent cladding oxidation. As the AP1000 design uses thermal igniters to burn hydrogen in a controlled manner, it is necessary to demonstrate that the safety equipment can continue to perform its function in the high-temperature environment created by the hydrogen burning.

The functions of the equipment in containment for which credit is taken in the AP1000 PRA were reviewed to determine if the equipment is required to operate in a severe accident environment and beyond design basis limits. The equipment and the basis for operation are the same as the AP600. Therefore, the results of the AP600 are extended to the AP1000 for equipment survivability.

19.34.2.8 Summary

The potential for and the consequences of severe accident phenomena are evaluated. The preventive and mitigative features of the AP1000 addressing the severe accident phenomena are discussed. This information is applied to the containment event trees and used in the quantification of the large release frequency.

19.34.3 Analysis Method

The design certification of the AP1000 included consideration by the NRC of the topic referred to in this section.

19.34.4 Severe Accident Analyses

The design certification of the AP1000 included consideration by the NRC of the topic referred to in this section.

19.34.5 Insights and Conclusions

The analyses of the severe accident phenomena for the AP1000 PRA highlight the following insights and conclusions:

- The design of the AP1000 reactor vessel, vessel insulation, and reactor cavity; and the ability to flood the cavity after a severe accident reduce the potential challenges to the containment integrity by maintaining the vessel integrity.
- Should a failure of the reactor vessel occur, the design of the reactor cavity enhances the ability to cool any core debris that exits the vessel.
- Lower head vessel failure due to in-vessel steam explosions is physically unreasonable.
- The ADS and PRHR system are design features that can be used to prevent high-pressure core melt in a severe accident.
- A directly-initiated hydrogen detonation in the AP1000 containment is not a credible event.
- The equipment needed to mitigate the consequences of a severe accident is designed to provide reasonable assurance that it will continue to operate during an accident.

19.34.6 References

19.34-1. Letter from D. A. Ward, Advisory Committee on Reactor Safeguards, to K. A. Carr, Chairman, Nuclear Regulatory Commission, “Proposed Criteria to Accommodate Severe Accidents in Containment Design,” dated May 17, 1991.

19.34-2. Theofanous, T. G., et al., “In-Vessel Coolability and Retention of a Core Melt,” DOE/ID-10460, July 1995.

19.34-3. Theofanous, T. G., et al., “Lower Head Integrity Under In-Vessel Steam Explosion Loads,” DOE/ID-10541, July 1996.

19.34-4. NUREG-1116, *A Review of the Current Understanding of the Potential for Containment Failure From In-Vessel Steam Explosions*, 1985.

19.34-5. GW-GL-022, AP600 Probabilistic Risk Assessment, August 1998.

19.34-6. Sherman, M. P., Tieszen, S. R., and Benedick, W. B., *FLAME Facility - The Effects of Obstacles and Transverse Venting on Flame Acceleration and Transition to Detonation for Hydrogen-Air Mixtures at Large Scale*, NUREG/CR-5275, April 1989.

19.34-7. Attachment to letter from D. M. Crutchfield, Office of Nuclear Reactor Regulation, to E. E. Kintner, Advanced Light Water Reactor Steering Committee, “Major Technical and Policy Issues Concerning the Evolutionary and Passive Plant Designs,” dated February 27, 1992.

19.34-8. “EPRI MAAP 4.0 Users Manual.”

TABLES 19.34-1 THROUGH 19.34-26 NOT USED.
FIGURES 19.34-1 THROUGH 19.34-391 NOT USED.

19.35 Containment Event Tree Analysis

The design certification of the AP1000 included consideration by the NRC of the topic referred to in this section.

19.36 Reactor Coolant System Depressurization

19.36.1 Introduction

Depressurization of the reactor coolant system is required for the external water cooling of the reactor vessel that will prevent vessel failure and core debris relocation to the containment (Reference 19.36-1). If the reactor coolant system (RCS) is at high pressure during core damage, containment failure may be postulated by several severe accident phenomena including induced failure of the steam generator tubes, high-pressure melt ejection, and direct containment heating.

19.36.2 Definition of High Pressure

High pressure is defined to support the assumptions of the PRA model. Induced steam generator tube rupture, high-pressure melt ejection, and reactor vessel failure into the flooded cavity will not occur if there is successful reactor coolant system depressurization.

Vessel failure can occur at elevated pressures with melted core debris in the vessel. This could cause the ejection of core debris from the vessel, followed by entrainment of debris in the high-velocity steam and water blowdown that would follow. Direct containment heating (DCH) and shifting of the reactor vessel are postulated containment failure mechanisms related to high pressure ejection of molten core debris.

Vessel failure and ex-vessel severe accident phenomena are prevented in the AP1000 by external cooling of the reactor vessel when the cavity is flooded. Flooding of the cavity occurs when the in-containment refueling water storage tank (IRWST) water fills the cavity. This can happen because of depressurization and subsequent in-containment refueling water storage tank water injection or when the cavity flood lines on the in-containment refueling water storage tank are opened. This cooling confirms the core debris will remain in the vessel. Heat transfer from the molten debris in the vessel through the lower head will thin the vessel wall and reduce the capability of the vessel to withstand higher pressures. It is conservatively assumed in this analysis that molten core debris in the vessel could cause failure at pressures greater than 150 psig.

If there is no molten core debris in the vessel, the vessel and the rest of the reactor coolant system, including the stream generator tubes, are expected to remain intact at pressures up to 3200 psig. This is consistent with the design of the reactor coolant system primary side.

19.36.3 References

19.36-1. Theofanous, T. G., et al., "In-Vessel Coolability and Retention of a Core Melt," DOE/ID-10460, July 1995.

19.37 Containment Isolation

Containment isolation is required before significant fission-product release after core uncovery. If the containment is not isolated, then the core damage results in a fission-product release to the environment. Containment isolation following an accident is achieved automatically by the protection and safety monitoring system or by the operator as instructed by an Emergency Response Guideline.

19.38 Reactor Vessel Reflooding

Reflooding of the in-vessel core debris will occur following an accident if the reactor coolant system is sufficiently depressurized and if the in-containment refueling water storage tank water can enter the reactor vessel, either through one or both in-containment refueling water storage tank gravity injection lines or through a break in the reactor coolant system.

Successful reflooding of the reactor vessel following an accident that resulted in core damage provides additional cooling to core debris and the vessel wall. It may also have the undesirable effect of leading to the production of hydrogen if water reacts with unoxidized zirconium and molten core debris.

19.39 In-Vessel Retention of Molten Core Debris

19.39.1 Introduction

In-vessel retention of molten core debris through water cooling of the external surface of the reactor vessel is a severe accident management feature of the AP1000. During postulated severe accidents, the accident management strategy to flood the reactor cavity with in-containment refueling water storage tank water and submerge the reactor vessel is credited with preventing vessel failure in the AP1000 probabilistic risk assessment. The water cools the external surface of the vessel and prevents molten debris in the lower head from failing the vessel wall and relocating into containment. Retaining the debris in the reactor vessel protects containment integrity by eliminating the occurrence of ex-vessel severe accident phenomena, such as ex-vessel steam explosion and core-concrete interaction, which have large uncertainties with respect to containment integrity.

The AP1000 provides for in-vessel retention with features that promote external cooling of the reactor vessel:

- The reliable multi-stage reactor coolant system depressurization system results in low stresses on the vessel wall after the pressure is reduced.
- The vessel lower head has no vessel penetrations to provide a failure mode for the vessel other than creep failure of the wall itself.
- The floodable reactor cavity can submerge the vessel above the coolant loop elevation with water intentionally drained from the in-containment refueling water storage tank.
- The reactor vessel insulation provides an engineered pathway for water-cooling the vessel and for venting steam from the reactor cavity.

19.39.2 Background on the Application of In-Vessel Retention to the Passive Plant

The Risk-Oriented Accident Analysis Methodology (ROAAM) analysis of the in-vessel retention phenomena (References 19.39-1 and 19.39-2) provided the basis for the application of the in-vessel retention accident management strategy to the AP600 passive plant and quantification of vessel failure in the AP600 PRA (Reference 19.39-3). The ROAAM included an analysis of the in-vessel melt progression and evaluation of the structural and thermal challenges to the vessel during the relocation to the lower head, including in-vessel steam explosion. Testing and evaluation of the uncertainties associated with the thermal loads produced by the in-vessel circulating molten debris pool, and heat removal limitations due to boiling crisis on the exterior vessel surface were performed in the ACOPO (Reference 19.39-4) and ULPU programs (References 19.39-1 and 19.39-5). The ROAAM concluded that the limiting challenge to the vessel integrity is the thermal loading produced during the steady-state heat transfer to the lower head wall after complete debris relocation to the lower plenum. The in-vessel retention ROAAM analyses and testing showed that the water in the AP600 cavity will remove the heat produced by the molten debris bed in the lower head with significant margin while the structural integrity of the lower head was maintained.

Based on the ROAAM results, vessel failure in the AP600 was considered to be physically unreasonable, and a probability of zero was applied to vessel failure in the AP600 PRA (Reference 19.39-3) if the following conditions of the ROAAM analysis were met:

- The reactor coolant system was depressurized.
- The reactor vessel was submerged sufficiently to wet the heated surface.

- Reactor vessel reflective insulation and containment water recirculation flow paths allowed sufficient ingress of water and venting of steam from the cavity.

- The treatment of the lower head outside surface (painting, coatings, etc.) did not interfere with water cooling of the vessel.

19.39.3 Application of In-Vessel Retention to the AP1000 Passive Plant

To establish a strong basis for crediting in-vessel retention in the AP1000, the following steps are taken:

- Establish design measures to increase the capability of the water to remove heat from the external surface of the reactor vessel (increase critical heat flux).

- Demonstrate that the thermal failure remains the limiting failure over the structural failure for the AP1000.

- Demonstrate that the AP1000 in-vessel melt progression does not change from the AP600 melt progression in such as way as to challenge the vessel integrity during relocation.

- Demonstrate that the heat load correlation, as applied from the ACOPO program (Reference 19.39-4), scales appropriately to the AP1000.

- Quantify the thermal loads using probability distributions developed specifically for the AP1000.

These items are discussed in the following sections.

19.39.4 Reactor Vessel Failure Criteria

The conclusions of the structural analyses performed for the AP600 in Reference 19.39-1 can be extrapolated to the AP1000. Thus, for the AP1000, success of in-vessel retention can be based solely on the thermal success criterion.

19.39.5 In-Vessel Melt Progression and Relocation

The AP1000 core and lower internals geometry has been changed from the AP600 geometry as a result of the higher power output. The core is made up of 157 fuel assemblies with a 14-foot active fuel length. To accommodate the larger reactor core, the thick stainless steel reflector has been replaced by a 7/8″ thick core stainless steel shroud. The thick bottom plate of the shroud is mounted flush on the support plate. There are no former plates in the annulus between the shroud and the core barrel. The core barrel is 2″ thick and hangs from the upper head flange. Cooling holes through the core shroud provide cooling flow to the shroud from the core flow.

The phenomena associated with melting the core and the relocation of the molten debris to the lower plenum play an important role in the composition and configuration of the debris pool (Reference 19.39-2). In turn, the characteristics of the debris pool significantly impact the heat loading to the lower head wall and the challenge to lower head integrity (Reference 19.39-1). Therefore, understanding the melting and relocation scenarios plays an important role in the assessment of in-vessel retention of molten core debris in the lower plenum.

The important conclusions from the analysis of the lower plenum debris pool formation are:

- The lower plenum debris bed is cooled with water during the entire relocation process prior to contact with the support plate. Transient debris configurations are not predicted to threaten vessel integrity.

- The lower plenum oxide debris subsumes the lower core support plate before dry out in the lower plenum occurs. If the relocated debris is assumed to be instantaneously quenched in the lower plenum water, the oxide debris contacts the lower support plate before the debris can return to a superheated condition. Therefore, the lower core support plate, core shroud and a sizeable fraction of the core barrel are subsumed in the debris bed. The focusing effect is mitigated.

- The lower plenum debris bed is predicted to form a metal layer over oxide pool configuration.

- The potential for debris interaction creating a bottom metal pool of uranium dissolved in zirconium is expected to be small.

- The earliest time to achieve the fully molten, circulating debris bed in the lower plenum is 2.7 hours after event initiation.

19.39.6 Application of Heat Transfer Correlations to the AP1000

19.39.6.1 Debris Pool to Vessel Wall Heat Transfer

The heat transfer from the oxide pool containing the decay heat producing fission products to the lower head of the reactor vessel is described using correlations that were developed in the Department of Energy (DOE) program for the AP600 in-vessel retention assessment.

The correlations developed in the ACOPO experiments and used in the AP600 in-vessel retention ROAAM for heat transfer from the debris pool to the lower head wall are applicable for use in the AP1000 in-vessel retention analysis.

19.39.6.2 Vessel Wall to External Cooling Water Heat Transfer

The heat transfer from the vessel wall to the cooling water is limited by the transition to film boiling at the external surface of the vessel wall. The maximum heat flux that can be removed prior to the transition to film boiling is the critical heat flux. If the heat flux from the debris pool to the wall is less than the critical heat flux, the vessel maintains sufficient strength to carry the load on the vessel. At heat fluxes above the critical heat flux, the external wall temperature increases significantly, the strength of the wall is lost, and the vessel fails.

Testing has been performed with ULPU-2000 Configuration IV (Reference 19.39-4) which demonstrates the feasibility of increasing the critical heat flux for AP1000. The heat removal capability is enhanced by constructing a hemispherical baffle outside the lower head to channel the cooling water flow and by assuring the flooding level in the containment outside the reactor vessel is sufficient for two phase natural circulation (Reference 19.39-4).

The AP1000 employs a reactor vessel insulation design that provides water inlet, steam venting and a baffle around the lower head to enhance the heat removal and increase the critical heat flux on the reactor vessel external surface. The insulation is vented from the annulus between the insulation and vessel to the vessel nozzle gallery at the 98 ft elevation.

19.39.7 Quantification of Heat Load on the Reactor Vessel Wall

With the baffle installed in the AP1000 and the cavity adequately flooded, significant margin-to-failure for in-vessel retention via external reactor vessel cooling is achieved.

Based on the results of the ROAAM testing and analysis and the UPLU-2000 Configuration IV testing, vessel failure is concluded to be physically unreasonable in the AP1000 PRA provided the following conditions are met:

- The reactor coolant system is depressurized.
- The vessel is submerged adequately to promote natural circulation of water through the baffle surrounding the lower head.
- Reactor vessel reflective insulation remains structurally sound under the pressure loads produced by the boiling external to the reactor vessel, allows water inlet at the bottom and venting of steam at the top, and provides the proper baffling to increase the critical heat flux on the external surface of the vessel lower head.
- The reactor vessel external surface conditions do not preclude the wetting phenomena identified as the cooling mechanism in the ULPU testing.

19.39.8 Reactor Coolant System Depressurization

Reactor coolant system depressurization is discussed in Section 19.36.

19.39.9 Reactor Cavity Flooding

Reactor cavity flooding is accomplished through either operator action or through the progression of the accident. The operator floods the cavity by opening a motor-operated valve and a squib valve in the recirculation lines between the in-containment refueling water storage tank and the containment recirculation sump, as shown in Figure 19.39-15. The operator action is prescribed by entering the AFR-C.1 Function Restoration Guideline (Reference 19.39-6) when the core-exit thermocouples reach 1200°F. The water floods the containment by flowing out of the recirculation screens, filling the containment floodable region of the containment, shown in Figure 19.39-15, to at least the 107′ 2″ elevation, shown in Figure 19.39-16.

To achieve the high critical heat flux for the AP1000 lower head, water level in containment must be sufficient for two phase natural circulation flow. The vents from the AP1000 reactor vessel insulation exit to the vessel nozzle gallery at the 98 ft elevation. It is conservatively assumed that the water level in the containment has to reach the 98 ft elevation within seventy minutes after the core exit temperature exceeds 1200°F, for successful vessel cooling.

The AP600 procedures instructed the operator to flood the reactor cavity at the end of AFR-C.1 Function Restoration Guideline before entering the severe accident management guidelines. The AP1000 requires the cavity to be flooded to a higher level and more quickly than the AP600. For the AP1000, the operator action to initiate cavity flooding has been moved to the entry of the AFR-C.1 Function Restoration Guideline to meet the time requirement for cavity flooding success.

19.39.10 Reactor Vessel Insulation Design Concept

With respect to in-vessel retention severe accident management, the goal of the reactor vessel insulation is to ensure that there will always be an adequate water layer next to the reactor vessel to promote heat transfer from the reactor vessel. The insulation will define an optimized flow path next

to the lower head to enhance the critical heat flux. The cooling of the vessel in a severe accident is accomplished by providing:

- A means of allowing water free access to the region between the reactor vessel and insulation.
- A frame that maintains the structural integrity of the insulation surrounding the lower head which provides the baffle for the water flow next to the vessel.
- A means to vent steam generated by the water cooling the vessel wall from the insulation surrounding the reactor vessel.
- A support frame to prevent the insulation panels above the vessel lower head from breaking free and blocking water from cooling the reactor vessel exterior surface.

19.39.10.1 Description of Reactor Vessel Insulation and Venting

Subsection 5.3.5 provides a description of the reactor vessel insulation and the functional requirements for the insulation.

19.39.10.2 Design Analysis of the Insulation and Support Frame

The insulation forms an engineered pathway to enhance the cooling of the external surface of the reactor vessel during in-vessel retention. Structural support to maintain this pathway is provided.

19.39.10.3 Reactor Vessel External Surface Treatment

Based on the reactor vessel system design specification, the surface is not coated and remains as bare metal.

19.39.11 Reactor Vessel Failure

Based on the analysis of in-vessel retention, an intact reactor vessel remains intact if the reactor coolant system is depressurized and the reactor vessel is adequately submerged.

19.39.12 Summary

In-vessel retention of molten core debris via external reactor vessel cooling can be accomplished in the AP1000.

- The reactor vessel insulation must provide a structurally sound baffle around the lower head and lower cylinder of the vessel to channel the flow between the vessel and insulation. An insulation design that provides the proper water inlet, steam venting and flow baffling is specified for the AP1000.
- The reactor cavity must be flooded to an elevation of at least 98 ft prior to the onset of the steady–state heat flux to the vessel wall from the debris to produce the driving head required to enhance the critical heat flux on the vessel surface. The operator action to flood the cavity has been moved to the first step of the emergency operating procedures to provide adequate flooding.

19.39.13 References

19.39-1. Theofanous, T.G., et al., “In-Vessel Coolability and Retention of a Core Melt,” DOE/ID-10460, July 1995.

19.39-2. Theofanous, T.G., et al., “Lower Head Integrity Under In-Vessel Steam Explosion Loads,” DOE/ID-10541, June 1996.

19.39-3. AP600 PRA Report, GW-GL-022, August 1998.

19.39-4. Theofanous, T.G., and S. Angeli, “Natural Convection for In-Vessel Retention at Prototypic Rayleigh Numbers,” Nuclear Engineering and Design, 200, 1-9 (2000).

19.39-5. Angelini, S., et al., “The Mechanism and Prediction of Critical Heat Flux in Inverted Geometries,” Nuclear Engineering and Design, 200, 83-94 (2000).

19.39-6. AP600 Emergency Response Guidelines.

TABLES 19.39-1 THROUGH 19.39-3 NOT USED.

FIGURES 19.39-1 THROUGH 19.39-15 NOT USED.

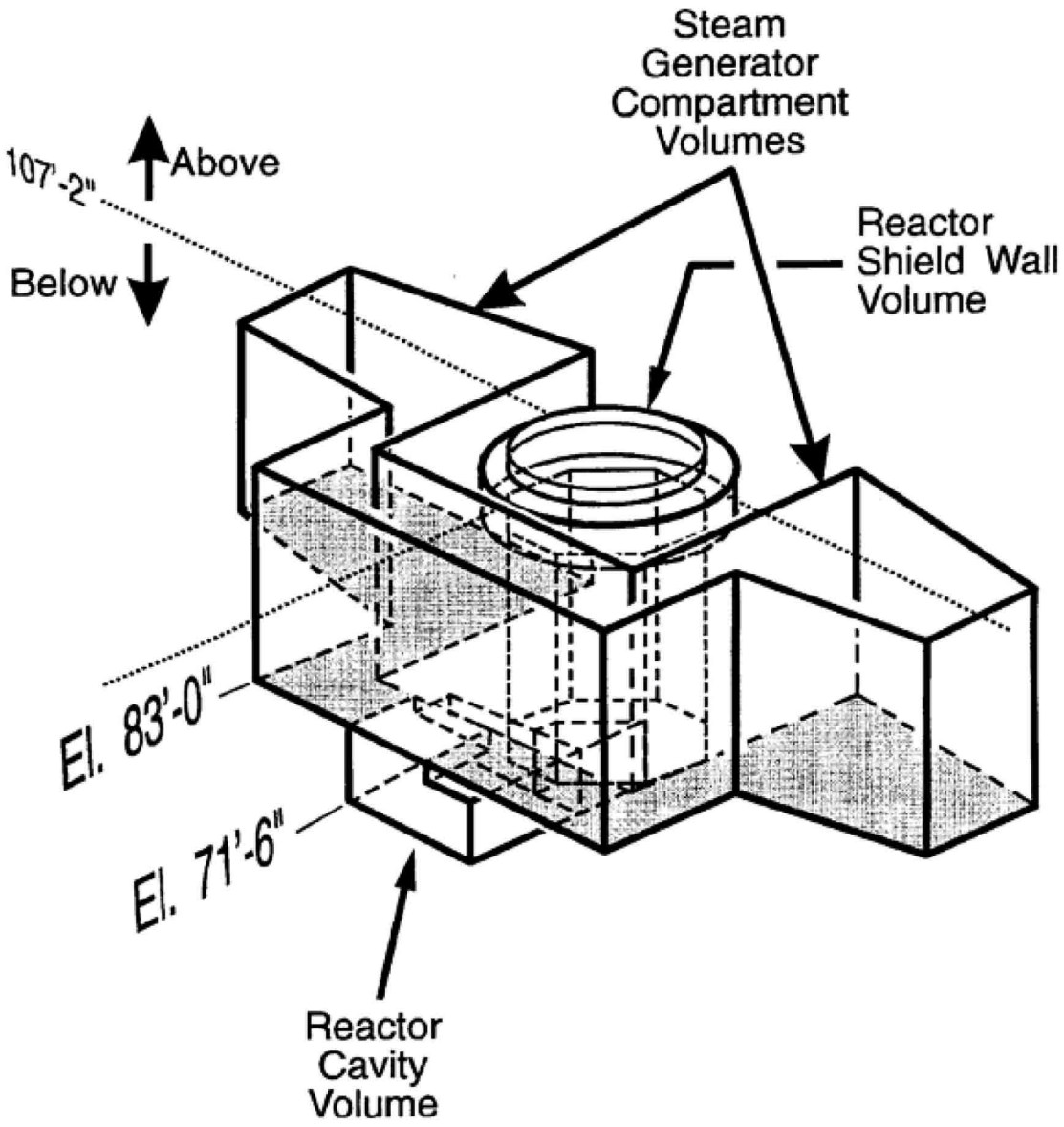

Figure 19.39-16 Containment Floodable Region

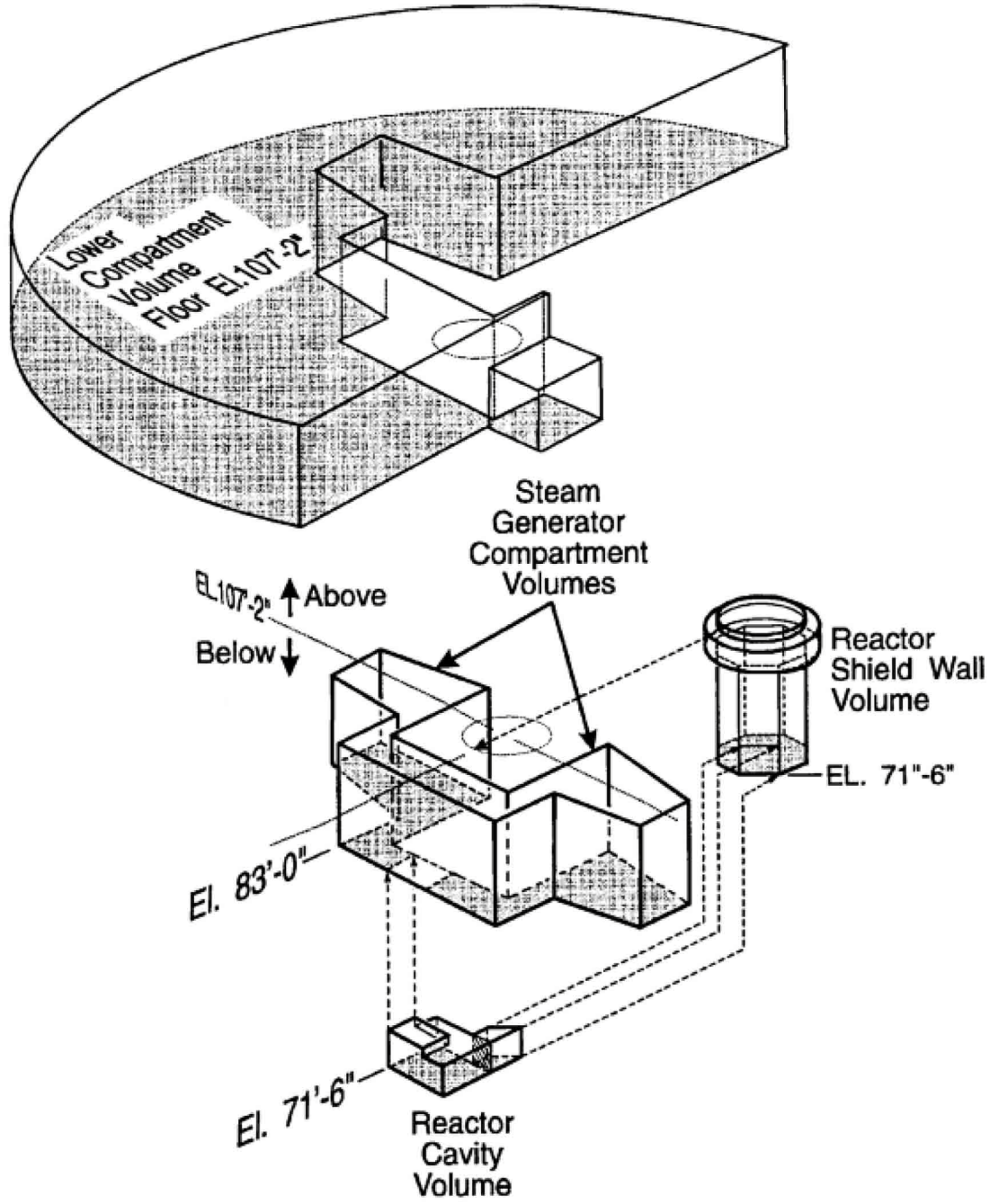

Figure 19.39-17 Containment Floodable Region – Expanded View

FIGURES 19.39-18 AND 19.39-19 NOT USED.

19.40 Passive Containment Cooling

The Nuclear Regulatory Commission (NRC) containment performance goal for advanced containment systems is to provide a leak-tight barrier to fission product release for 24 hours following an accident, and to remain as a barrier against uncontrolled releases following that time. The AP1000 containment is cooled via the passive containment cooling system (PCS). Barring hydrogen combustion and ex-vessel phenomena that are addressed elsewhere in the AP1000 containment event tree analysis, the AP1000 containment is not expected to exceed the design-basis pressure during a severe accident. No threat to the containment integrity from long-term overpressurization is predicted.

In the event that design-basis cooling fails, the containment pressure will exceed the design basis, although containment failure within 24 hours is predicted to be highly unlikely. After 24 hours, the operator may vent the containment to prevent uncontrolled failure of the containment per the severe accident management guidelines. Once vented, the steam concentration in the containment will increase and improve the heat removal capacity of the passive cooling such that no further venting would be required.

19.41 Hydrogen Mixing and Combustion Analysis

19.41.1 Introduction

In the course of a severe accident, a substantial amount of combustible gases can be generated in-vessel from the oxidation of the zirconium and other metals. The AP1000 containment is provided with nonsafety-related hydrogen igniters to control the concentration of combustible gases. If the igniters operate, combustion of hydrogen plumes may present a thermal load to the containment. Combustible gas can accumulate in the containment at flammable concentrations if the igniter system fails to function. The AP1000 hydrogen analysis quantifies the threat to containment integrity with and without hydrogen igniters.

If vessel failure does not occur, the amount of hydrogen in the containment is limited to the mass generated during the in-vessel core heatup and relocation. If vessel failure occurs with water in the cavity, an additional amount of hydrogen may be generated from ex-vessel fuel-coolant interactions. Furthermore, if the debris layer in the cavity is not coolable or if insufficient water is available in the containment to cool the debris, and subsequent thermal attack of concrete occurs, additional hydrogen and other combustible gas, such as carbon monoxide, will be generated. The AP1000 PRA assumes containment failure if vessel failure is predicted, so the evaluation of containment integrity from hydrogen combustion only considers in-vessel hydrogen generation.

Hydrogen combustion is evaluated during two time frames: early (during the in-vessel relocation and hydrogen generation) and intermediate (prior to 24 hours after the onset of core damage). In the early time frame, containment challenge is considered from hydrogen burning as an unmixed plume (diffusion flame) and from local detonation at high concentrations in confined compartments below the operating deck. In the intermediate time frame when the hydrogen is mixed, containment challenge from global deflagration and potential detonation due to stratification of gases is considered. The hydrogen is assumed to burn within 24 hours of core damage.

19.41.2 Controlling Phenomena

The conditions required for combustion in the containment are flammable gas mixtures and the presence of an ignition source. Typically, a spark is sufficient to cause ignition. If the mixture temperature is above ~1000 K, auto-ignition can occur without the presence of an ignition source. The flammability limits are determined by the concentrations and temperature of the combustible gas-air-diluent mixture. Hydrogen and the oxygen in the air are the reactants in the combustion reaction. Steam, carbon dioxide, and excess nitrogen in the mixture act as inertants that may inhibit the reaction.

Hydrogen-air-steam mixtures can burn in several modes: diffusion flames, slow and accelerated deflagrations, and detonations (Reference 19.41-1). Burning of an unmixed hydrogen plume near the source results in a diffusion flame. Diffusion flames are stationary and result primarily in thermal loads on nearby structures or equipment. Deflagrations or detonations are burning of premixed gases. In practical terms, a slow deflagration is a flame that travels at a speed much slower than the speed of sound such that the pressure inside the containment equilibrates during the combustion. No dynamic loads are generated. Accelerated deflagrations travel fast enough to generate shock waves and dynamic loads. Detonations travel at supersonic velocities and also generate dynamic loads. The static loads that result from deflagrations can be predicted and bounded. The maximum dynamic loads from accelerated flames and detonations are difficult to calculate.

Standing diffusion flames on the in-containment refueling water storage tank pool or at the in-containment refueling water storage tank vents can be postulated early into an accident following core uncovery for sequences in which the automatic depressurization system stages 1 through 3 provide a primary depressurization mechanism. A standing diffusion flame at the vent could present a

thermal load to the containment steel shell, which is close to some of the vents. If the primary system break is in one of the PXS valve/accumulator rooms which flood with water and submerge the break, diffusion flames can also be postulated at the room exit in the maintenance floor. This location has a direct line of sight with the personnel and equipment hatches, electrical penetrations, and the containment shell, and may present a thermal loading challenge.

The static loads associated with deflagrations are limited by thermodynamics. If all of the chemical energy available in the mixture is converted to temperature and pressure, then the maximum pressure is limited by the adiabatic, isochoric (constant volume), complete combustion (AICC) pressure. The actual pressure would drop over time from this peak because of heat losses to water, structures, and equipment in containment. Dynamic pressure loads are not limited by the adiabatic, isochoric, complete combustion value because the local pressure is due to very rapid, nonequilibrium combustion.

The mode of combustion depends on the mixture concentrations, initial conditions, and boundary conditions (Reference 19.41-1). Near the hydrogen source, hydrogen may not be mixed significantly with the air in the containment. If ignition occurs there, then a diffusion flame may be formed. Further downstream from the hydrogen source, mixing will have occurred and a deflagration or detonation may result, depending on the hydrogen concentration and geometric boundary factors. In some cases, accelerated flames may also develop to detonations, which are called deflagration-to-detonation transition (DDT). The occurrence of flame acceleration and deflagration-to-detonation transition is complex and not completely understood. It is dependent on a number of parameters. These include hydrogen and oxygen concentrations; nature and concentration of inertants; gas temperature and pressure before ignition; ignition source; the size and shape of the compartment in which the combustion occurs; and the number, size, and shape of any obstacles in the compartment.

In AP1000, direct initiation of detonation by sufficiently high-energy sources from equipment in containment is unlikely (Reference 19.41-2: Since AP1000 is very similar to AP600, the phenomenological evaluations are valid for AP1000.), but mechanisms to accelerate a flame to a detonation may occur. Deflagration-to-detonation transition is considered the most likely mechanism. Transition to detonation is considered in several sections of the containment for accident sequences that result in hydrogen concentrations greater than 10 volume percent, including the passage connecting the two steam generator compartments, the core makeup tank and equipment bay, in-containment refueling water storage tank gas space, steam generator compartments, and steam generator operating deck.

19.41.3 Major Assumptions and Phenomenological Uncertainties

Because of phenomenological uncertainties, a number of assumptions are necessary in the hydrogen analysis.

19.41.3.1 Hydrogen Generation

The degree to which the cladding is oxidized during the in-vessel phase of the accident sequence and the availability of water to the core determines the rate and the mass of hydrogen released to the containment during the early time phase. The rate and mass of hydrogen produced are important parameters in determining the hydrogen concentration and the flammability limits of the gas mixtures in the containment compartments.

19.41.3.2 Containment Pressure

The containment pressure is an important parameter in the determination of the pre-burn boundary conditions. A higher initial pressure can result in a higher peak pressure, but the increased steam

mass can inert the mixture and prevent combustion. If the passive containment cooling system water is not operational, containment pressures are elevated and combustion is steam inerted.

19.41.3.3 Flammability Limits

A flammable condition is determined by flammability limits. Flammability limits of a combustible gas mixture are defined as the limiting gas compositions at a given temperature and pressure in which a deflagration will propagate once ignited. There is information on flammability limits of hydrogen-air-steam mixtures at temperatures less than 149°C. For hydrogen, there are two lean propagation limits considered, upward and downward. At lean upward propagation limits, flames will propagate upward because of buoyancy. At lean downward propagation limits, flames will propagate upward and downward throughout the volume by their own reaction kinetics. Hence, the extent of flame propagation (or combustion completeness) for combustion at lean flammability limits is determined by the hydrogen concentration. This relation is a result from the Nevada Test Site (Reference 19.41-3). The addition of steam or other inert gas has a strong effect on the hydrogen concentration and flammability (Reference 19.41-4).

Combustion initiated by igniters occurs at lean upward flammability limits with a small pressure rise. However, with the failure of igniters, combustion at a hydrogen mixture at a concentration above the lean downward propagation limits may result in much larger pressure and temperature consequences. The global burn considered in the analysis is defined as combustion at or above the lean downward propagation limits. This definition includes the possibility that a global burn becomes a detonation, since the occurrence of a detonation requires a hydrogen concentration much above the lean downward propagation limits. Combustion regimes and associated adiabatic, isochoric, complete combustion pressure are approximately demonstrated for hydrogen-air mixtures in Reference 19.41-5.

19.41.3.4 Detonation Limits and Loads

A detonation is a supersonic combustion front that produces a dynamic load in excess of the adiabatic, isochoric, complete combustion value. The energy release from the combustion of the hydrogen-air-steam mixture sustains the shock structure that ignites and burns the mixture. The detonation limits cannot currently be predicted by any first-principles theory. Engineering correlations used to predict the limits have been developed based on a measurable quantity called the detonation cell width. For simplified discussion, the detonation cell width can be considered a characteristic length that describes the sensitivity of the mixture to detonation. The smaller the detonation width, the easier it is to get the mixture to detonate and sustain propagation. Deflagration-to-detonation transition is considered, and the method of NUREG/CR-4803 (Reference 19.41-6) is used to evaluate the potential for flame acceleration.

Since the lowest hydrogen concentration for which deflagration-to-detonation transition has been observed in the intermediate-scale FLAME facility at Sandia is 15 percent (Reference 19.41-7), and 10 CFR 50.44 limits hydrogen concentration to less than 10 percent, the likelihood of deflagration-to-detonation transition is assumed to be zero if the hydrogen concentration is less than 10 percent.

19.41.3.5 Igniter System

The AP1000 nonsafety-related hydrogen igniter system, if operational during a severe accident, will burn hydrogen as soon as the lean upward flammability limits are met. Thus, the concentration of hydrogen is maintained, on average, at the lean upward flammability limits. However, depending on the hydrogen release rate, location and oxygen availability, locally high concentrations may exist in the in-containment refueling water storage tank or in the subcompartment where the pipe break occurs.

The hydrogen igniters are actuated by manual action when core-exit temperature exceeds a predetermined temperature as directed by the emergency response guidelines (ERG). The indication and actuation are done with containment conditions within the equipment qualification limits of the systems used, within the design basis of the plant and systems, and before fission-product releases to the containment, so equipment survivability of the monitoring and actuation systems during the time frame that they are required to perform is supported.

19.41.3.6 Other Ignition Sources

A flammable mixture will not burn without an ignition source unless the temperature of the mixture is sufficiently high (~1000 K) that auto-ignition becomes possible. Hot surfaces or random sparks from equipment or static electricity may be postulated ignition sources. High-temperature gas jets exiting from the reactor coolant system may become an ignition source. However, the gas stream may not have enough momentum to entrain the surrounding flammable mixture, especially in the depressurized cases.

19.41.3.7 Severe Accident Management Actions

Severe accident management guidance that is considered in the AP1000 PRA is the operator action to flood the reactor cavity in the event of core damage. This action often results in the late reflooding of a damaged core due to the time required for the operator to diagnose the problem and take the action. Some events will lead to core reflooding through the natural progression of the accident.

19.41.4 Hydrogen Generation and Mixing

The design certification of the AP1000 included consideration by the NRC of the topic referred to in this section.

19.41.5 Hydrogen Burning at Igniters

Analyses of AP600 demonstrated the effectiveness of the hydrogen igniter system as placed in the passive containment geometry. The cases in the burning analysis were chosen for variation in hydrogen generation rate, release locations into containment, in-containment refueling water storage tank water level, and PXS compartment flooding. The cases considered 100 percent cladding reaction. The behavior of the AP1000 is essentially the same as the AP600 with respect to hydrogen release rates and locations.

Generally, the reactor coolant system is depressurized prior to hydrogen generation. Hydrogen is released to the containment through ADS stage 4 as it is generated in the core. Natural circulation in the containment provides oxygen for burning the hydrogen at the igniters in the loop compartments, close to the source. The loop compartments are shielded from the containment shell and most equipment and instrumentation that would be used to mitigate and monitor the accident.

Igniters located in the IRWST, PXS and CVS compartments, CMT room and at various elevations in the upper compartment provide coverage for hydrogen that may be released through the IRWST, PXS/CVS or in the CMT room.

The igniter system maintains the global uniform hydrogen concentration in the containment at or below lower flammability limits. In the most likely severe accidents, the hydrogen is burned primarily in a favorable location that protects the integrity of the containment and mitigative and monitoring equipment.

19.41.6 Early Hydrogen Combustion

Early hydrogen combustion is defined as burning that occurs during the period the hydrogen is released from the primary system to the containment. During this time, the hydrogen may not be well mixed in the containment and, depending on release locations, may be concentrated in the in-containment refueling water storage tank, PXS valve/accumulator rooms or chemical and volume control system room, steam generator compartments or maintenance floor. If sufficient oxygen is available, the compartments may become locally detonable. If oxygen is not available in the compartment, the plume may travel to a location where oxygen is available and it can burn as a diffusion flame.

19.41.6.1 Hydrogen Generation Rates

Qualitative hydrogen generation characteristics can be inferred from the availability of steam and the availability of overheated, unreacted zirconium in the reactor vessel. Based on the insights from hydrogen generation and mixing analyses, the hydrogen generation can be classified into one of three categories: boiloff generation rate, early-reflood generation rate, and late-reflood generation rate. This section briefly defines each type of hydrogen release in the AP1000 hydrogen analysis and the conditions under which they occur.

19.41.6.1.1 Boiloff Hydrogen Generation

Boiloff hydrogen generation occurs as the water inventory in the reactor vessel is depleted by decay heat. The steam generation is limited to the decay heat boiloff in the covered fraction of the core and overheated, unreacted zirconium surface area is limited to the upper regions of the core, which have not relocated below the water line. Core relocation to the lower head may produce a rapid steam generation that produces a brief period of rapid oxidation, but by this time, the core geometry is lost and very little unoxidized zirconium surface area is available for sustained hydrogen production.

19.41.6.1.2 Early-Reflood Hydrogen Generation

Early-reflood hydrogen generation occurs in the event of the reflooding of an overheated, relatively intact core. Quenching of the core provides a large quantity of steam and a large, overheated, unreacted zirconium surface area for oxidation. Shattering of the cladding due to thermal stresses can enhance the oxidation rate. In the early-reflood case, the oxidation of the zirconium is limited only by the degree of core uncovery prior to the reflood. The rate and degree of zirconium oxidation is expected to be greater than the no-reflood case.

19.41.6.1.3 Late-Reflood Hydrogen Generation

Late-reflood hydrogen generation occurs in the event of a reflood after the core has degraded significantly and possibly after relocation to the lower head. Much of the core geometry is lost and little surface area is available for oxidation, even when steaming from quenching debris is available.

19.41.6.2 Hydrogen Release Locations

The hydrogen release locations in the containment determine the hydrogen mixing in the containment and regions of high hydrogen concentration in the event that the igniters fail. The flow paths from release points in confined compartments to the volumes where oxygen is available determine possible locations where diffusion flames may occur.

19.41.6.2.1 Automatic Depressurization System Stages 1, 2, and 3

Stages 1, 2 and 3 of the automatic depressurization system relieve the reactor coolant system pressure from the top of the pressurizer to the in-containment refueling water storage tank. The water level in the in-containment refueling water storage tank at the time of the release determines the steam concentration in the tank. If the spargers are covered, the steam is quenched out of the gas flow and the hydrogen is released to the gas space of the tank. If the spargers are not covered, the steam concentration is high and will drive the air out of the tank. If the igniters are available, diffusion flames may be postulated at the in-containment refueling water storage tank vent exits for large sustained hydrogen releases. If igniters are not available, the possibility of hydrogen detonation is evaluated.

19.41.6.2.2 Automatic Depressurization System Stage 4

Stage 4 of the automatic depressurization system relieves steam and hydrogen from the hot leg of the reactor coolant system to the steam generator compartments in the containment. The steam generator compartments, along with the maintenance floor and the upper compartment, form the major natural-circulation path in the containment. Oxygen starvation of any potential diffusion flames in the steam generator compartment is not expected for low-pressure hydrogen releases from automatic depressurization system stage 4. The containment shell is sheltered from flames in the steam generator compartments by the concrete walls, so diffusion flames at the igniters in the steam generator compartments are not considered to be a threat to the containment integrity. If igniters are not available, good mixing in the compartment mitigates the threat of detonation for the low-pressure releases.

19.41.6.2.3 Break Location

The reactor coolant system break provides a pathway from the reactor coolant system to one of several compartments in the containment. A failure of a component in the reactor coolant system loop (hot leg or cold leg) will relieve hydrogen to the loop compartment. Hydrogen released from the break to the loop compartment will behave similarly to the hydrogen released from stage 4 automatic depressurization system.

A failure of the direct vessel injection line or a break in the chemical and volume control system piping will relieve hydrogen to one of the small compartments under the maintenance floor, the chemical and volume control system room or one of the two PXS valve/accumulator rooms. These compartments are dead-ended and communicate with the maintenance floor through stairway or room vents. The initial blowdown through the break fills the compartment with steam and drives the air out of the compartment. After the blowdown and reactor coolant system depressurization, countercurrent flow between the compartment and the maintenance floor slowly replenishes the air.

Each of the dead-ended compartments has a one-way drain to the containment sump in the cavity. The break flow into a dead-ended compartment will not fill the compartment with water, as the draining and flashing of the break flow removes the water to the containment sump. However, a broken direct vessel injection line in a PXS valve/accumulator room may allow the in-containment refueling water storage tank to drain into the PXS valve/accumulator room if the injection valves open in the broken line. The draining of the in-containment refueling water storage tank water into the PXS valve/accumulator room will fill the PXS valve/accumulator room and spill water over the curb into the maintenance floor.

If the igniters are available, hydrogen released to the dead-ended compartments during the core degradation may burn initially, but may become oxygen starved. The plume then rises through the stairway to the maintenance floor, which is amply supplied with oxygen by the containment natural circulation. A diffusion flame can be postulated at the exit of the dead ended compartments in the

maintenance floor. The exterior wall of the maintenance floor is the steel containment shell below the passive containment cooling system annulus, the lower-level equipment hatch, and the personnel hatch. Many electrical penetrations pass through the maintenance floor wall to the auxiliary building.

19.41.6.3 Early Hydrogen Combustion Ignition Sources

For a burn to be initiated, an ignition source is required. Igniters mitigate the threat to the containment integrity from global deflagration and detonation. If a hydrogen plume can produce a diffusion flame, the igniters provide the ignition source.

19.41.7 Diffusion Flame Analysis

Diffusion flames can be postulated to occur at vents or exits from compartments with a hydrogen source that are dead-ended or not well-mixed. Incombustible gas mixtures that include a high concentration of hydrogen may develop in the compartment. When the plume of hydrogen exits the compartment into a room containing oxygen and an ignition source, burning of the plume as a standing flame at the vent may produce locally high temperatures. If the release of hydrogen is sustained, the heat load from the burning may threaten equipment, including the containment shell integrity.

The overall geometry of the AP1000 containment is relatively open. Ninety-seven percent of the containment free volume participates in containment natural circulation and is well-mixed. However, the IRWST, PXS and CVS compartments are small, confined rooms that may have a hydrogen source, and thus may be postulated to produce a diffusion flame at vents. This section discusses the conditions that may produce a standing diffusion flame in these locations, and presents the quantification of the containment failure probability given the presence of a sustained diffusion flame at a dead-ended compartment vent.

AP1000 Diffusion Flame Mitigation Strategy

Hydrogen is a byproduct of a severe accident, and hydrogen pathways to the IRWST, PXS and CVS subcompartments cannot be completely ruled out, particularly in the IRWST, to which the effluent of the first stages of the reactor coolant system automatic depressurization system are directed. The other compartments can only have hydrogen releases in the event that a break occurs there, but some of the highest frequency severe accident sequences have breaks in a DVI line, which traverses a PXS compartment. Therefore, the potential for diffusion flames from these subcompartment locations cannot be excluded from the probabilistic risk assessment.

The AP1000 addresses diffusion flames by adopting a defense-in-depth philosophy in the design. In the highest frequency severe accidents, sustained hydrogen release is prevented from occurring in the dead-ended compartments. In sequences where diffusion flames at IRWST or PXS/CVS compartment vents may be postulated, design strategies are initiated to mitigate the threat to the containment integrity by locating hydrogen plumes away from the containment shell.

The first level of defense against the threat to containment integrity from diffusion flames is the prevention of sustained hydrogen releases to dead-ended compartments. The highest frequency severe accident sequences have full reactor coolant system depressurization prior to core damage. Hydrogen is released at low pressure to the containment as it is produced in the core. Stage four of the automatic depressurization system provides a pathway of substantially lower resistance (by approximately one order of magnitude) compared to the maximum break size in the DVI line that relieves to the PXS compartment and to the other three ADS stages that relieve to the IRWST. Additionally, the ADS spargers in the IRWST generally have a 10-ft static head of water above them, which further increases the resistance to flow of hydrogen to the IRWST.

Hydrogen released from ADS stage 4 is relieved to the loop compartments, which are supplied with oxygen by the containment natural circulation and shielded from the containment shell by high concrete walls. Hydrogen is able to burn in the loop compartments without threatening the containment integrity. Therefore, ADS stage 4 provides the first level of defense against diffusion flames.

In the event that ADS stage 4 fails to adequately direct hydrogen away from confined compartments, the compartment vents are designed to preferentially release the hydrogen at locations where it burns away from the containment shell.

Vents from the PXS and CVS compartments to the CMT room are located well away from the containment shell and containment penetrations. Access hatches to the subcompartments that are near the containment shell are covered and secured closed such that they will not open as a result of a pipe break inside the compartment. Therefore, hydrogen releases to the CMT room from the subcompartments are not considered as a threat to the containment integrity.

19.41.8 Early Hydrogen Detonation

Hydrogen detonation can be initiated from a high-energy ignition source or by deflagration-to-detonation transition during flame acceleration. A review of potential ignition sources in containment concludes that the maximum source is too small to directly initiate a detonation (Reference 19.41-2: Since AP1000 is very similar to AP600, the phenomenological evaluations are valid for AP1000.). Therefore, the occurrence of detonation is related to the potential for deflagration-to-detonation transition in the AP1000 containment analysis.

The methodology of Sherman and Berman (Reference 19.41-6) is used to evaluate the likelihood of deflagration-to-detonation transition. The analysis considers the hydrogen release rates to the containment, core reflooding, the containment release locations, and in-containment refueling water storage tank and PXS valve/accumulator room water levels to determine the probabilities.

19.41.9 Deflagration in Time Frame 3

The design certification of the AP1000 included consideration by the NRC of the topic referred to in this section.

19.41.10 Detonation in Intermediate Time Frame

The design certification of the AP1000 included consideration by the NRC of the topic referred to in this section.

19.41.11 Safety Margin Basis Containment Performance Requirement

The AP1000 containment meets the criteria of the safety margin basis containment performance requirement.

19.41.12 Summary

The major insights of the hydrogen mixing and combustion analysis are as follows:

- No containment failure from hydrogen is predicted if the hydrogen igniters are operational.

- Operation of the stage 4 automatic depressurization system valves releases much of the hydrogen generated in the reactor coolant system to the steam generator rooms where it can be well mixed in the containment to mitigate the threat of diffusion flames from sustained hydrogen released through the in-containment refueling water storage tank.

- The threat of detonation is predominantly due to hydrogen releases to the PXS valve/accumulator rooms below the 107′ 2″ containment elevation (direct vessel injection line breaks). The compartment is a confined region with little ventilation. Equipment and grating are present to promote turbulence. A break in the compartment induces a high-temperature environment creating good conditions for potential deflagration-to-detonation transition.

- The probability of containment failure due to diffusion flame is very small.

- No containment failure is predicted from deflagration.

Analyses are performed to meet the requirements of 10 CFR 50.44. Igniter burning analyses with rapid hydrogen generation and 100-percent cladding reaction conclude that the igniter system maintains the global uniform hydrogen concentration in the containment at or below lower flammability limits. If the stage 4 automatic depressurization system is available, the hydrogen is well mixed in the containment and no excessive concentrations are predicted in the in-containment refueling water storage tank or PXS valve/accumulator rooms. If the stage 4 automatic depressurization system is failed, hydrogen in the in-containment refueling water storage tank and PXS valve/accumulator rooms can reach high concentrations. However, the mixtures are oxygen starved and are not flammable or detonable. The safety margin basis containment performance requirement is met as the loss-of-coolant accident plus 100-percent active cladding reaction hydrogen burn peak pressure provides margin to the ASME Service Level C stress limits.

19.41.13 References

19.41-1. Tieszen, S. R., et al., “Hydrogen Distribution and Combustion,” in Ex-Vessel Severe Accident Review for the Heavy Water New Production Reactor (ed. by K. D. Bergeron), NPRW-SA90-3, Sandia National Laboratories, 1993.

19.41-2. “AP600 Phenomenological Evaluation Summaries,” WCAP-13388 (Proprietary) Rev. 0, June 1992 and WCAP-13389 (Nonproprietary), Rev. 1, 1994.

19.41-3. Ratzel, A. C., “Data Analysis for the Nevada Test Site (NTS) Premixed Combustion Tests,” NUREG/CR-4138, SAND85-0135, Sandia National Laboratories, 1985.

19.41-4. Hertzber, Martin, “Flammability Limits and Pressure Development in Hydrogen-Air Mixtures,” Proc. Workshop on the Impact of Hydrogen on Water Reactor Safety, Volume III, NUREG/CR-2017, SAND81-0661, Sandia National Laboratories, 1981.

19.41-5. Sherman, M. P., et al., “Deliberate Ignition and Water Fogs as H2 Control Measures for Sequoyah,” Proc. Workshop on the Impact of Hydrogen on Water Reactor Safety, Volume IV, NUREG/CR-2017, SAND81-0661, Sandia National Laboratories, 1981.

19.41-6. Sherman, M. P., and Berman, M., “The Possibility of Local Detonation During Degraded Core Accidents in the Bellefonte Nuclear Plant,” NUREG/CR-4803, SAND86-1180, Sandia National Laboratories, 1987.

19.41-7. Sherman, M. P., et al., “FLAME Facility,” NUREG/CR-5275, SAND85-1264, Sandia National Laboratories, 1989.

19.42 Conditional Containment Failure Probability Distribution

The design certification of the AP1000 included consideration by the NRC of the topic referred to in this section.

19.43 Release Frequency Quantification

The design certification of the AP1000 included consideration by the NRC of the topic referred to in this section.

19.44 MAAP4.0 Code Description and AP1000 Modeling

The design certification of the AP1000 included consideration by the NRC of the topic referred to in this section.

19.45 Fission Product Source Terms

The design certification of the AP1000 included consideration by the NRC of the topic referred to in this section.

19.46 Not Used

19.47 Not Used

19.48 Not Used

19.49 Offsite Dose Evaluation

The design certification of the AP1000 included consideration by the NRC of the topic referred to in this section.

19.50 Importance and Sensitivity Analysis

The design certification of the AP1000 included consideration by the NRC of the topic referred to in this section.

19.51 Uncertainty Analysis

The design certification of the AP1000 included consideration by the NRC of the topic referred to in this section.

19.52 Not Used

19.53 Not Used

19.54 Low Power and Shutdown PRA Assessment

The design certification of the AP1000 included consideration by the NRC of the topic referred to in this section.

19.55 Seismic Margin Analysis

19.55.1 Introduction

In accordance with Section II.N, Site-Specific Probabilistic Risk Assessments and Analysis of External Events, of SECY-93-087 (Reference 19.55-1), the U.S. Nuclear Regulatory Commission (NRC) approved the following staff recommendations:

> "PRA insights will be used to support a margins-type assessment of seismic events. A PRA-based seismic margin analysis will consider sequence-level High Confidence, Low Probability of Failures (HCLPFs) and fragilities for all sequences leading to core damage or containment failures up to approximately one and two-thirds the ground motion acceleration of the Design Basis SSE."

The PRA based seismic margin analysis (SMA) and the methodology described in this section is consistent with the recommendation of SECY-93-087.

Seismic margins methodology is employed to identify potential vulnerabilities and demonstrate seismic margin beyond the design-level safe shutdown earthquake (SSE). The capacity of those components required to bring the plant to a safe, stable condition is assessed. The structures, systems, and components identified as important to seismic risk are addressed. For this PRA-based seismic margin analysis, HCLPFs are calculated and reported at the sequence level. In addition, insights related to random and/or human failures are reported, as deemed appropriate, for each sequence.

19.55.2 Calculation of HCLPF Values

19.55.2.1 Seismic Margin HCLPF Methodology

The seismic margin analysis is based on established criteria, design specifications, existing qualification test reports, established basic design characteristics and configurations, and public domain generic data.

The seismic margin assessment is used to demonstrate margin over the SSE of 0.3g. Consistent with SECY-93-087 (Reference 19.55-1), the goal of the SMA is therefore to demonstrate that the plant HCLPF is at least 0.5g peak ground acceleration (pga). This is also called the review level earthquake (RLE). The AP1000 seismic response spectra are included in Tier 1, Chapter 5 (see Tier 1, Figures 5.0-1 through 5.0-4). It will be necessary for a COL (combined operating license) applicant to demonstrate that the seismic response for the applicant's plant is equal to or less than that used in the calculation of the HCLPF values, and to evaluate the potential for soil liquefaction using the applicant's site specific conditions. This will ensure a reserve margin that exceeds a 0.5g seismic level.

19.55.2.2 Calculation of HCLPF Values

A seismic margin analysis is made up of two major tasks:

1. A PRA-based model to determine the plant HCLPF
2. Determination of the plant structure and component HCLPFs

The second task, determination of HCLPF seismic acceleration values for plant structures and components, is discussed in this section; the PRA-based model is herein discussed as far as the seismic event trees and major assumptions associated with seismic fault trees development are

concerned. The HCLPF values used in the analysis, which now include HCLPF values for hard-rock, high-frequency sites and soil sites, are summarized in Table 19.55-1.

19.55.2.2.1 Review of Plant Information

The assessment uses the following plant information:

- Structural and seismic design criteria and procedures
- Structural design calculations
- Layout and design drawings
- Test reports
- Piping and instrumentation diagrams
- Equipment design specifications
- Generic fragility data
- AP1000 plant response spectra.

19.55.2.2.2 System Analysis

Section 7.4 provides a discussion of the systems required for safe shutdown. The structures and components associated with these systems are considered in the seismic margin assessment. It is noted that the same success criteria as in the AP1000 PRA sensitivity case where no credit is taken for non-safety related systems, is used as the starting point for the AP1000 PRA-based seismic margins analysis. This success criterion is not necessarily defined in terms of reaching specific plant modes, but rather on reaching a sustainable safe plant state. The bases for these success criteria are given in the AP1000 PRA report (Reference 19.55-5).

19.55.2.2.3 Analysis of Structure Response

The purpose of a seismic fragility analysis is to define the maximum limit, seismic capacity, of functional capability or operability with the associated uncertainty for plant components and structures that could have an effect on safe shutdown of the plant following a seismic event. Capacity in the seismic margin assessment, expressed in terms of the free field peak ground level acceleration, is the level of the seismic event that results in failure of a given component or structure to perform its safety-related function. Failures leading to loss of safety function could result from such things as: loss of a pressure boundary; significant inelastic deformation; partial collapse; loss of support functions; or a combination of failure modes. In the calculation of the HCLPF value for a system, structure, or component, the governing failure mode is established by examining the different potential failure modes possible. Each failure mode has different reserve margin. As an example, ductility may be very large for tension failure, whereas, for buckling, ductility generally does not contribute to reserve margin.

A fragility evaluation is made for the key structures and components. The HCLPF for the equipment and structures is established using one of the following:

- Probabilistic fragility analysis
- Conservative deterministic failure margin (CDFM) method
- Test results
- Deterministic approach
- Generic fragility data

These methods are briefly discussed below.

Probabilistic Fragility Analysis

This method is used to define HCLPF values for structures such as:

- Steam generator supports
- Reactor pressure vessel supports
- Pressurizer supports
- Containment vessel

There are many sources of conservatism and variability in the estimation of seismic peak ground acceleration capacity for seismic margin assessment. HCLPF values reflective of the seismic capacity are derived from median capacity using formulas based on the log-normal distribution. The HCLPF values reflect a 95-percent confidence (probability) of not exceeding a 5-percent probability of failure (Reference 19.55-2).

The HCLPF is defined by a lognormal probability distribution that is a function of median seismic capacity and composite standard deviation, βc:

$$\text{HCLPF} = \text{Median Capacity} \times e^{[-2.3 \times \beta c]}$$

The median seismic capacity is related to the mean seismic capacity by the expression:

$$\text{Median Capacity} = \text{Mean Capacity} \times e^{[-(\beta c \text{^} 2)/2]}$$

The mean peak seismic ground capacity, A_m, is related to the stress and strength design margin factors by the following expression:

$$A_m = (\Pi_i [X_i])A_o$$

where:

A_m = Mean peak seismic ground capacity

X_i = i^{th} design mean margin factor

Π_i = Product notation

A_o = Nominal seismic peak ground capacity

It is noted that the composite standard deviation is equal to the root mean square of the composite standard deviation associated with each of the margin factors. That is:

$$\beta_c = \sqrt{[\Sigma_i (\beta_c)_i^2]}$$

The conservatisms and variability identified and considered in this assessment are associated with stress and strength margin factors. The basic grouping of margin factors are: deterministic strength factor; variable strength factors; material; damping; inelastic energy absorption, ductility; and analysis or modeling error.

Conservative Deterministic Failure Margin Method

The HCLPF values for the shield building and the exterior walls of the Auxiliary Building were calculated using the conservative deterministic failure margin approach. A finite element analysis was performed of the structures that considered cracking of the concrete and redistribution of the loads. Deterministic margin factors were defined for three items: strength; inelastic energy absorption; and damping.

The polar crane HCLPF is calculated using the Westinghouse's design specification of Polar Crane and the vendor structural qualification calculation. The CDFM approach is used allowing the stress to reach yield and using a ductility factor of 1.25.

In addition, the HCLPF values for the Reactor Coolant Pump external heat exchanger and for the Passive Containment Cooling System are calculated with the CDFM approach.

Test Results

For the electrical equipment where documented test results are available, the HCLPF value is defined from comparison of required response spectra (RRS) and test response spectra (TRS). The method employed follows a deterministic approach using existing test data for similar types of equipment.

The existing test data was reviewed to determine a lower bound seismic capacity.

When the natural frequency of the equipment is not known, it was assumed that the natural frequency coincided with the required response spectra peak acceleration so that the lowest HCLPF value was calculated. It is noted that where equipment frequencies are known, and are used for comparing the RRS and TRS, these frequencies will be included in the design specification for the equipment to assure that the dynamic characteristics are the same as those expected.

Relay Chatter

Solid-state switching devices and electro-mechanical relays will be used in the AP1000 protection and control systems. Solid-state switching devices are inherently immune to mechanical switching discontinuities such as contact chatter. Robust electro-mechanical relays are selected for AP1000 applications such that inherent mechanical contact chatter is within the required system performance criteria. Therefore, contact chatter has no effect on system operation and was, therefore, not included in the seismic margin analysis. The COL must confirm the use of seismically robust electro-mechanical relays in the engineered safety features actuation and control systems.

Moreover, the loss of offsite power event has a very low HCLPF value (0.09g). The control rod motor generator sets are powered by AC load centers that are de-energized on loss of offsite power sources. When the control rod motor generator sets are de-energized, current to the magnetic jack mechanisms stops and the gripper coils open, allowing the rods to drop into the core. Therefore, relay chatter is not an issue for reactor trip.

Finally, passive residual heat removal (PRHR) and core makeup tank (CMT) system valves automatically fail open upon loss of instrument air due to loss of seismically induced loss of offsite power. Thus, relay chatter is not an issue for PRHR and CMT system functions.

Deterministic Approach

A lower bound estimate of the HCLPF is obtained for selected structures or equipment based on margin to design limit for the appropriate load combination defined by the fault tree logic. Where applicable, the increased capacity due to inelastic energy absorption is defined using the recognized and recommended ductility factor of 1.25.

This approach was used for the primary components to verify that their supports would control the HCLPF value. It was also used for a few cases to define the HCLPF when it was apparent that its seismic capacity would not control the plant HCLPF value. This approach was used for: containment baffle plate supports; Interior Containment Structure and IRWST; PRHR heat exchanger; core makeup tank; and valves.

Generic Fragility Data

Generic fragility data was used when insufficient information was available to define the HCLPF value using one of the methods described above. Those cases where this approach was use were:

- Reactor internals and core assembly that includes fuel
- Control rod drive mechanism (CRDM)
- Reactor coolant pump
- Accumulator tank
- Piping
- Cable trays
- Valves
- Ceramic insulators

The Utility Requirements Document for Advanced Light Water Reactor, Reference 19.55-3, was used for all of the components listed above except ceramic insulators, which used recognized industry low seismic capacity data.

19.55.2.2.4 Evaluation of Seismic Capacities of Components and Plant

Table 19.55-1 provides the HCLPF values for the equipment, structures, and systems considered in the seismic margin evaluation. Also shown in this table is the approach used to define the HCLPF value, as described in Subsection 19.55.2.2.3. The evaluation considers the effect of uplift and sliding of the nuclear island basemat foundation. The nuclear island seismic response has been evaluated at 1.1 times the Review Level Earthquake (RLE) and was found to retain its stability against sliding and overturning.

In the design of the AP1000, careful consideration is given to those areas that are recognized as important to plant seismic risk. In addition to paying special attention to those critical components that have HCLPF values close to the review level earthquake, the design process considers potential interaction with both safety-related and nonsafety-related systems or structures, as well as adequate anchorage load transfer and structural ductility. The seismic margin evaluation provides a means of identifying specific equipment and/or structures that are vulnerable to beyond design basis seismic events.

Equipment qualification is the generation and maintenance of evidence to ensure that safety systems and equipment will operate on demand to meet system performance requirements during normal/abnormal and accident environmental conditions. The methodology for qualification of safety-related electrical and mechanical equipment is defined in Appendix 3D and further expanded for seismic high frequency considerations in Appendix 3I. The intent of the qualification process defined in these Appendixes is to ensure a high reliability for equipment and system safety. Qualification by test, analysis or a combination of test and analysis is performed to verify the safety-related electrical and mechanical equipment will operate as intended under normal/abnormal and accident environmental conditions over the installed life. Details on the qualification process are provided to the equipment vendors in specifications and qualification methodology documents during procurement under a 10CFR50 Appendix B quality assurance program.

19.55.2.2.5 Verification of Equipment Fragility Data

The AP1000 safety-related equipment is designed to meet the safe shutdown earthquake requirements defined in Chapter 3. This seismic margin evaluation has focused on demonstrating that the design of the nuclear island structures, safety-related equipment, and equipment supports can carry the loads induced by the review level earthquake discussed here. This evaluation incorporates as-specified equipment data. After the plant has been built, it will be necessary to perform a verification of the seismic margin assessment for the installed conditions.

19.55.2.2.6 Turbine Building Seismic Interaction

As part of the seismic margin assessment, the seismic interaction between the turbine building and the nuclear island was evaluated according to guidance provided in Reference 19.55-4. It was determined that:

- To protect the adjacent nuclear island auxiliary building the first bay of the turbine building has been classified as seismic category II.

- It is not likely that the size and energy of debris from the turbine building will be large enough to result in penetration through the auxiliary building roof structure.

Even though it is not likely that penetration of turbine building debris could be large enough or have sufficient energy for penetration through the auxiliary building roof structure, this event was evaluated. The consequences of damage to the safety-related equipment in the auxiliary building were investigated. It was determined from this investigation that should an event occur that causes the failure of equipment in the upper elevations of the auxiliary building, the results of the seismic margin assessment, the plant HCLPF value, and the insights derived from the seismic margin assessment are not affected. Moreover, the steam line break events, which would result from the damage of equipment in the upper elevations, are not dominant contributors to the core damage frequency. Further, the loss of equipment in the upper elevations will not affect the passive safety systems that would be used to put the plant in a safe shutdown condition should an event occur.

19.55.3 Seismic Margin Model

In this section, the AP1000 Risk-Based Seismic Margins Model is summarized and the plant HCLPF for AP1000 is determined.

HCLPFs are calculated for the seismic Category I safety-related systems that are called upon via the seismic event trees to mitigate an accident caused by the initiating seismic event.

19.55.3.1 Major SMA Model Assumptions

In this section, the general characteristics and major assumptions of the AP1000 SMA model are discussed.

1. The seismic event is assumed to occur while the plant is operating at full power.

2. A review level earthquake equal to 0.5g is used for the seismic margin analysis.

3. It is assumed that the seismic event would result in loss of offsite power since the AC power equipment is not seismic Category I. (The offsite insulators on the feed lines from the offsite power grid fail such that a loss of offsite power occurs.) No credit is taken for onsite emergency AC power (diesel generators).

4. No credit is taken for non-safety related systems. They are assumed to have failed or be non-functional due to the seismic event. This includes all equipment in the turbine building and the turbine building itself; as discussed in Subsection 19.55.3.3, structural failure of the turbine building is assumed not to impact the structural integrity of the adjacent auxiliary building.

5. The seismically induced SMA initiating event categories and their event trees are taken from the AP600 PRA model. For each initiating event, the PRA logical modeling (i.e., seismic event and fault trees) developed for AP600 structures, systems, and components have been used as the starting point and their applicability to the AP1000 design has been assessed

and confirmed. The applicability of the base AP600 to the AP1000 has been addressed in a supporting calculation. Cutsets associated with each sequence are generated and then the min-max method is used to calculate the plant HCLPF value.

19.55.3.2 Seismic Initiating Events

The first step in Seismic Margins Model is to evaluate which initiating events could occur as a result of a seismic event. For this purpose, a Seismic Initiating Event Hierarchy Tree is constructed. This event tree is given in Figure 19.55-1 and discussed below. Based on this hierarchy event tree, seismic initiating event categories are defined and their event tree models are constructed (as discussed in Subsection 19.55.3.3).

Given that a seismic event occurs, the hierarchy event tree is constructed such that the seismically-induced initiating event with the most challenge to the plant safety systems is considered first: gross structure collapse. This category is labeled as EQ-STRUC and is the first initiating event category to be modeled and quantified.

If gross structure collapse does not occur, next the reactor coolant system (RCS) loss-of-coolant-accident (LOCA) category in excess of emergency core cooling system (ECCS) capacity (also termed as “Vessel Failure”) is considered. This category is labeled as EQ-RVFA.

If vessel failure does not occur, then large RCS LOCAs are considered. This category is labeled as EQ-LLOCA.

If EQ-LLOCA does not occur, then small RCS LOCAs are considered. This category is labeled as EQ-SLOCA. Steam generator tube rupture (SGTR) and large secondary line break (SLB) events are folded into the small LOCA category, as discussed in Subsection 19.55.3.3.

Next considered is the seismically induced anticipated transient without scram (ATWS) event. This event is labeled as EQ-ATWS.

Finally, all other transients are considered in the category labeled EQ-LOSP. The seismically induced LOSP event occurs at low HCLPF values (e.g., lower than the SSE at 0.3g) and does not affect the plant HCLPF, as discussed in Subsection 19.55.4.2. The cutsets for this event are all “mixed cutsets,” containing seismically induced initiating event coupled with random failures leading to core damage. This event is included in the model for additional insights and completeness.

Thus, the hierarchy tree defines six initiating event categories. Each of these is discussed and an event tree for each is constructed in Subsection 19.55.3.3.

The PRA-based seismic margins analysis does not consider seismic hazard curves. Therefore, initiating event frequencies are not calculated for each seismically generated initiating event category. Although seismically generated initiating event frequencies are not calculated, it is important to evaluate the seismic vulnerability of the components and systems that contribute to the initiating event categories. This is done by estimating a HCLPF for each seismic initiating event category, as discussed in Subsection 19.55.3.3.

19.55.3.3 Seismic Event Trees

The six seismically induced initiating event categories defined by the hierarchy event tree model of Subsection 19.55.3.2 are further discussed to model seismically induced failures that will determine the HCLPF for each of these initiating events. The six categories considered are:

1. EQ-STRUC Gross structural collapse
2. EQ-RVFA LOCA in excess of emergency core cooling system capacity
3. EQ-LLOCA Large LOCA
4. EQ-SLOCA Small LOCA
5. EQ-ATWS ATWS
6. EQ-LOSP Loss of offsite power

The small LOCA category also covers SGTR and SLB events. As discussed later in the success paths, the SLOCA success path used for SMA is also applicable (conservatively) to the SGTR and unisolated SLB events given that only safety-related systems are credited and considered in the PRA-based SMA.

The last event, LOSP, is postulated at 0.09g. This event may also be viewed to represent a larger family of transients associated with loss of main feedwater, loss of compressed air, turbine trip, reactor trip, loss of service water/component cooling water, etc, following a seismic event and LOSP since no credit is taken for these non-safety systems in the SMA models. Moreover, a seismically induced transient containing LOSP, becomes a station blackout (SBO) event since no credit is taken for diesel generators that are not seismically qualified.

Each of the SMA events are further discussed below.

1. EQ-STRUC (Gross Structural Collapse)

   This event includes seismically induced failures of AP1000 structures that may result in core damage and large fission product release.

   The AP1000 structures are classified in 5 groups:

   1. Nuclear Island

      This consists of the containment, shield building, and auxiliary building.

      Nuclear island is structurally designed to meet seismic Category I.

   2. Turbine Building

      The first bay (the portion of the turbine building adjacent to the nuclear island outlined in Table 3.2-2 and including the portion of the basemat under this area) of the turbine building is classified as Seismic Category II, and the main area of the turbine building structure is designed to meet the International Building Code. For the SMA model, it is assumed to have failed. Thus no credit is taken for systems in this building. RN-13-003

   3. Annex Building

      The high rise portion of the annex building is designed to meet seismic Category II. For the SMA model, it is assumed to have failed. Thus, no credit is taken for systems in this building.

4. Diesel Generator Building

   The diesel generator building is designed to meet the UBC. For the SMA model, it is assumed to have failed. Thus, no credit is taken for systems in this building.

5. Radwaste Building

   The radwaste building is designed to meet the UBC. For the SMA model, it is assumed to have failed. Thus, no credit is taken for systems in this building.

Thus, only the nuclear island is considered for the SMA model; the interaction between the other buildings and the nuclear island is assumed to have no detrimental effect on the nuclear island structures. This assumption needs to be verified by a plant walkdown when an AP1000 plant is built.

The failures of the nuclear island structures are modeled in terms of the driving structures of the steel containment vessel, the shield building, and the auxiliary building.

The EQ-STRUC event tree is shown in Figure 19.55-2; HCLPF value for EQ-STRUC is calculated in Subsection 19.55.4.

2. EQ-RVFA (LOCA in Excess of ECCS Capacity)

   This event represents the “vessel failures” where the event leads to excessive loss of RCS inventory that can not be made up by the ECCS capacity. In this case, core damage is postulated. A complete dependency between seismic induced failures of SSCs that share basic characteristics (i.e., component type, location/elevation, etc.), the “vessel failure” event comprises the following types of structural and component failures:

   1. Seismically induced failures of the reactor vessel
   2. Seismically induced failures of the steam generators
   3. Seismically induced failures of the other RCS components
   4. Seismically induced failures of two direct vessel injection (DVI) lines
   5. Seismically induced failures of fuel.

   The EQ-RVFA event tree is shown in Figure 19.55-3; HCLPF value for EQ-RVFA is calculated in Subsection 19.55.4.

3. EQ-LLOCA (Large LOCA)

   Seismically induced large LOCA initiating event category, EQ-LLOCA, contains RCS breaks with break sizes greater than 9 inches. Since the seismic event failures assume that if one pipe breaks by a seismic event, all redundant similar pipes will break at the same time, all major RCS pipe breaks are conservatively included in this category; thus, no medium LOCA is defined in the initiating event hierarchy tree. Also included in this category are the failures of the PRHR heat exchanger by a seismic event.

   The EQ-LLOCA event tree is shown in Figure 19.55-4; HCLPF value for EQ-LLOCA is calculated in Subsection 19.55.4.

4. EQ-SLOCA (Small LOCA)

   Seismically induced small LOCA initiating event category, EQ-SLOCA, contains RCS breaks with break sizes less than 2 inches of equivalent diameter. Since the seismic event failures assume

that if one pipe breaks by a seismic event, all redundant similar pipes will break at the same time, all major RCS pipe breaks are conservatively included in the large LOCA category. For the small LOCA category, RCS leaks from instrument lines are used as the representative event. The small LOCA category also includes and bounds events such as

- Steam Generator Tube Rupture (SGTR)
- Large Steam Line Breaks (SLB) (due to generation of SI signal and RCS inventory shrinkage)

For SGTR events, breaks of one or more (up to 5) tubes have been considered for the AP1000 design. An event with 5 steam generator tubes rupturing has an equivalent LOCA break flow area of a 1.46 inch diameter hole. The rupture of more than 5 tubes by a seismic event is conservatively bounded by the structural failure of a steam generator, which is included in the EQ-RVFA initiating event.

Due to the modification of the Reactor Coolant Pump (RCP) Heat Exchanger (HX) from the AP600 design to the AP1000 design, an additional entry is added to the seismic induced Small LOCA. This reflects the possibility that in the event of a RCP HX pipe break, a small LOCA will be induced. Flow from the RCS inventory will be restricted by the labyrinth seal surrounding the RCP motor shaft; tolerances on the labyrinth seal allow for a maximum flow area of $1.389in^2$. This corresponds to approximately a 1.3 inch pipe break. A postulated seismic induced break of all eight tubes does not change the equivalent break flow rate for each pump and when considering the break in all pumps, a total of approximately 2.7 inch pipe break equivalent LOCA needs to be considered. This is judged to be consistent with the definition of seismically induced small LOCA given above.

The EQ-SLOCA event tree is shown in Figure 19.55-5; HCLPF value for EQ-SLOCA is calculated in Subsection 19.55.4.

5. EQ-ATWS (Anticipated Transients without Scram)

   The EQ-ATWS event addresses the seismically induced ATWS initiating event related to the failure of the core assembly or guide tubes or the control rod drive systems to remain functional so that the rods can not fall into the core. The fuel is still intact and can be cooled. The failure mode associated with seismically induced fuel failure has been already addressed in EQ-RVFA event.

   Because offsite power is postulated to have been lost, the control rod motor generator sets would be de-energized even if the reactor trip function failed. If the core assembly or the control rod system failed, the rods are postulated to fail to insert into the core.

   The EQ-ATWS event tree is shown in Figure 19.55-6; the HCLPF value for EQ-ATWS is calculated in Subsection 19.55.4.

6. EQ-LOSP (Loss of Offsite Power)

   The EQ-LOSP event addresses the seismically induced loss of offsite power. This event occurs at relatively low intensity earthquakes. The driving failure for loss of offsite power is represented by failure of ceramic insulators in the switchyard. The HCLPF value for these insulators is 0.09g, which is lower than the review level earthquake of 0.5g, and the plant SSE of 0.3g. Such an earthquake does not challenge any of the safety-related systems that are built to withstand the SSE and have margin for higher g levels. Thus, this event does not lead to purely seismically driven failure combinations for a core damage sequence. This event model contains only “mixed

cutsets" for core damage; these are failure combinations of seismically induced initiating event coupled with random failures of safety-related systems.

The EQ-LOSP event tree is shown in Figure 19.55-7; this event does not contribute to plant HCLPF.

19.55.3.4 Seismic Fault Trees

System fault trees for mitigation functions have been modified to account for seismically-induced failures. The AP600 system seismic fault trees have been reviewed for applicability to the AP1000 and only limited and minor changes have been deemed necessary.

19.55.4 Calculation of Plant HCLPF

This section presents the SMA calculations based on the model developed in Subsection 19.55.3.

The initiating event HCLPFs are calculated in Subsection 19.55.4.2. The plant HCLPF is calculated in Subsection 19.55.4.3.

The analysis demonstrates that all structures and components required to maintain the plant in a safe stable state are expected to function following a seismic event of 0.5g acceleration.

19.55.4.1 HCLPFs for Basic Events

The HCLPF values for various AP1000 structures and components were determined in a supporting calculation and are given in Table 19.55-1. The basic events defined in the SMA model for seismic failures are assigned their own HCLPF values, as shown in Table 19.55-2. These HCLPF values are taken from Table 19.55-1. When not self-evident, the "Source" column in Table 19.55-2 explains how the information Table 19.55-1 has been used.

For reasons beyond the development of the PRA-based AP1000 SMA, Table 19.55-1 groups all the electrical equipment into two major categories: "Non-Sensitive to High Frequency Excitation" and "Sensitive to High Frequency Excitation". For the purposes of the PRA-based SMA, all electrical equipment has been assumed to be from the limiting categories among the two, which has an HCLPF value of 0.5; this assumption is for the purposes of this analysis only and is conservative for this purpose.

19.55.4.2 Calculation of Initiating Event HCLPFs

Initiating event HCLPFs are calculated by assigning the HCLPF values from Table 19.55-2 to the seismically induced failures modeled in Subsection 19.55.3.3 for initiating events. The HCLPF associated to the initiating events will be the minimum among those for each of the potential initiator; the results of these calculations are given in Tables 19.55-3 through 19.55-7; results are presented for the AP1000 before and after this modification for DCD Revision 17. EQ-IEV-LOSP is already assigned a HCLPF 0.09g, representing the failure of ceramic insulators but it does not contribute to plant HCLPF since it has only mixed cutsets (seismic and random failures combined in cutsets).

The initiating event HCLPFs are summarized below:

Initiating Event	HCLPF	Dominated by
EQ-IEV-STRUC	0.55g	Polar crane
EQ-IEV-RVFA	0.50g	Fuel and pressurizer failure
EQ-IEV-LLOCA	0.81g	RCS piping
EQ-IEV-SLOCA	0.54g	Steam generator tube failure
EQ-IEV-ATWS	0.50g	Core assembly failures
EQ-IEV-LOSP	0.09g	Ceramic insulator failure

When the min-max method is used, the HCLPF of seismic sequences resulting from an initiating event can not be less than the initiating event HCLPF since it appears in every cutset. If the initiating event is postulated to lead directly to core damage, the IE HCLPF is used in the determination of the plant HCLPF.

Since both EQ-STRUC and EQ-RVFA events are postulated to lead to core damage, and EQ-STRUC is postulated to go to large early release as well, plant HCLPF can be determined at this point to be at least 0.50g for core damage and at least 0.55g for large, early release consequences.

19.55.4.3 Calculation of AP1000 Plant HCLPF

The final AP1000 plant HCLPF calculation also considers the mitigation portion of the PRA logic. Even though this is not going to change the values identified in Subsection 19.55.4.2, the complete calculation provides further insights on the seismic margin of the AP1000 design.

All basic events in the AP1000 SMA model (listed in Table 19.55-2) are assigned a dummy probability value of 0.5; the model is then quantified and cutsets are generated. The min-max approach is then applied to the obtained cutsets at each failure sequence level to evaluate the sequence HCLPF value, the event tree HCLPF value and the overall plant HCLPF value.

The cutset generated from the SMA model are listed and analyzed through the min-max approach discussed above in a supporting calculation. Sequence level results are presented in Table 19.55-8 where also the plant level HCLPF value is presented.

19.55.5 Sensitivity Analyses

A 99% confidence associated with the test response spectra is expected for all the HCLPF extracted from tests (method [6] in Table 19.55-1). To address this expectation a sensitivity case was run to the AP1000 PRA-based SMA.

Since electrical equipment is tested and qualified to the SSE (i.e., 0.30g), the HCLPF values in Table 19.55-1 for all tested equipment are set to 0.3g. While the selected values are extremely conservative due to the engineering margins normally adopted for the qualification tests, such values would not change either the overall AP1000 plant HCLPF value or any sequence or event tree level HCLPF value.

The Polar Crane HCLPF value dominates the plant level HCLPF for the Gross Structural Collapse initiating event. Therefore, the fragility analysis of the polar crane was performed using both CDFM and PRA-based fragility analysis. It was demonstrated that the calculated HCLPF values from these two methods are above 0.5g and have a difference of less than 5%.

19.55.6 Results and Insights

19.55.6.1 AP1000 SMA Results

The AP1000 PRA-based SMA has demonstrated that for structures, systems, and components required for safe shutdown, the HCLPF magnitudes are equal to or greater than 0.50g. This HCLPF is determined by various structures, systems, and components with an HCLPF value of 0.5g.

Thus, the AP1000 plant can meet or exceed the requirement to withstand a review level earthquake of 0.5g. It is observed that electrical equipment qualification consistent with the Certified Seismic Design Response Spectra (CSDRS) at 0.3g (with a 99% confidence associated to the Test Response Spectra – TRS) supports the overall plant HCPLF value of 0.5g.

The success paths used for the SMA are taken conservatively in many cases, and credit for operator actions for events at 0.5g review level earthquake has been avoided. Thus, the results are valid without operator intervention, which indicates a strong point of the AP1000 design to mitigate seismically induced core damage and large release sequences.

All SMA sequences are evaluated with loss of offsite power and loss of onsite AC power leading to a station blackout event. The plant design is shown to be robust against seismic event sequences each of which contain station blackout coupled with other seismic or random failures.

19.55.6.2 AP1000 SMA Insights

The SMA results also point out the following insights:

1. Design Features

   The AP1000 design provides some aspects that make the plant more robust against the review level earthquakes. Namely:

   - Reactor trip is ensured without the actuation signal due to the loss of offsite power occurring and rods inserting by gravity.
   - PRHR system valves fail open without actuation signal following loss of power/loss of instrument air. Thus, PRHR cooling is immediately available.
   - CMT system valves fail open without actuation signal following loss of power/loss of instrument air. Thus, CMT injection is immediately available.

   Thus, three key mitigating systems, reactor trip, PRHR cooling, and CMT injection are available with high confidence and low probability of failure, without dependence on actuation signals immediately after a review level seismic event.

   Moreover, the passive containment cooling system air operated valves also fail open in a review level earthquake, due to loss of offsite power/instrument air. As a result, the passive containment cooling system is automatically actuated and has enough water inventory to last for 72 hours.

2. DC System Fragility

   Control rods, PRHR, CMT, and passive core cooling systems would be operational after potential loss of protection and safety monitoring system (PMS) or DC control power. Thus, the plant can successfully mitigate a transient event even with a failure of PMS or DC control power. However, the DC control power system HCLPF is the same as the plant HCLPF (0.50g). This HCLPF has

the potential to become a driving failure, if it were to be coupled with a LOCA event with low HCLPF. However, no such low HCLPF LOCA events are identified in the current model.

3. Importance of Valve Room Fragilities

   Fragility of certain valve rooms, where the passive core cooling system valves are concentrated, becomes an important factor; the SMA model depends on the successful functioning of these valves to mitigate LOCA accidents. These rooms are labeled as 11206/11207 and contain CMT, accumulator, IRWST injection, and cavity recirculation valves. Since the HCLPF of these rooms is relatively high, compared to the plant HCLPF value, the seismic failure of many passive core cooling system valves does not become a contributor to plant HCLPF.

4. Operator Actions

   Operator actions are not credited in the SMA model for the 0.50g review level events. Inclusion of operator actions in the models would provide additional success paths, such as manual actuation of the automatic depressurization system (ADS) after failure of CMTs to inject. However, this inclusion would not affect the plant HCLPF or the major conclusions of the SMA. Thus, the AP1000 design is already robust with respect to its response to seismic events, even without taking credit for operator actions.

5. IRWST Failure

   This failure is modeled to render PRHR, gravity injection, and recirculation systems inoperable. Thus, it becomes a single point failure that affects both the transient (e.g. LOSP events) and LOCA success paths. Failure of IRWST is modeled as a part of gross structural failure, as well as in PRHR and gravity injection system fault trees. The IRWST HCLPF is 0.71g and therefore significantly above the plant level HCLPF.

   Additionally, an argument can be made that when the IRWST fails, its inventory would end up in the containment cavity and can be used to recirculate cavity water back into the RCS, leading to successful core cooling. Although this scenario is plausible and credible, such success sequences (e.g. sequences where gravity injection is skipped, directly going into cavity recirculation) are not analyzed in the AP1000 PRA. For this purpose, no credit for such a success path is taken in the present model.

6. Large Fission Product Release

   The large fission product release is driven by the same seismic sequences that dominate the plant core damage. This is due to either the nature of the initiating event (such as gross structural failure initiating event, EQ-STRUC), or postulated containment failure following a reactor vessel failure (RVFA) (such as EQ-RVFA initiating event or some ATWS sequences leading the RVFA). Failure of containment isolation or containment cooling system due to their system components or system actuation failures does not dominate the plant large release HCLPF.

19.55.6.3 Site Specific Seismic Margin Analysis

The VCSNS site seismic demand based on the site-specific Ground Motion Response Spectra (GMRS) is enveloped by a seismic demand which combines both the Certified Seismic Design Response Spectra (CSDRS) and Hard Rock High Frequency (HRHF) design response spectra as defined by the Tier 1 criteria for SSE. Therefore, it can be concluded that the Seismic Margin Assessment analysis documented in Section 19.55 is applicable to the VCSNS Units 2 and 3 site.

The VCSNS Nuclear Island (NI) is founded on hard (sound) rock which eliminates any potential for site specific effects such as seismically induced liquefaction settlements, slope stability, foundation failure or relative displacements which would lower the HCLPF values calculated for the certified design. For non-safety related structures and foundations adjacent to the NI, these site specific effects are evaluated in Subsection 2.5.4 and shown to have no effect on the NI; therefore, having no potential to lower the HCLPF values calculated for the certified design.

19.55.7 References

19.55-1. "SECY-93-087 - Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs," USNRC Memorandum, July 21, 1993, Chilk to Taylor.

19.55-2. Budnitz, R. J., et al., "An Approach to the Quantification of Seismic Margins in Nuclear Power Plants," NUREG/CR-4334, UCID-20444, August 1985.

19.55-3. Advanced Light Water Reactor Utility Requirements Document, Volume III, ALWR Passive Plant, Chapter 1, Appendix A, PRA Key Assumptions and Groundrules, Revisions 5 & 6, Issued December 1993.

19.55-4. "A Methodology for Assessment of Nuclear Power Plant Seismic Margin," Electric Power Research Institute, EPRI NP-6041, October 1988.

19.55-5. APP-GW-GL-022, Revision 8, AP1000 Probabilistic Risk Assessment, Westinghouse Electric, LLC, August 2007.

Table 19.55-1 (Sheet 1 of 2)
Seismic Margin Parameters and HCLPF Values

Description	Median pga[1]	βc	HCLPF Value[1]	Basis
Buildings/Structures				
Shield Building – Tension Ring	-	-	0.73	[2]
Shield Building – Air Inlet	-	-	0.71	[2]
Shield Building – Conical Roof	-	-	0.71	[2]
Shield Building – PCS Tank	-	-	0.81	[2]
Shield Building – SC/RC Connection	-	-	>0.67	[2]
Shield Building – RC Cylindrical Wall	-	-	0.67	[2]
Steel Containment Vessel – Buckling	1.94	0.42	0.73	[3]
Steel Containment Vessel – Overturning	5.74	0.62	1.38	[3]
Containment Baffle – Support Failure	-	-	0.91	[4]
Interior Containment Structure & IRWST Tank	-	-	0.71	[4]
Exterior Walls of Auxiliary Building – Wall 1	-	-	0.97	[2]
Exterior Walls of Auxiliary Building – Wall 11	-	-	0.88	[2]
Primary Components				
Reactor Pressure Vessel	-	-	0.56	[4]
Reactor Pressure Vessel Supports	1.58	0.35	0.71	[3]
Reactor Internals and Core Assembly (includes fuel)	1.5	0.51	0.5	[5]
Control Rod Drive Mechanism (CRDM)	2.2	0.51	0.7	[5]
Steam Generator	-	-	0.54	[4]
Steam Generator Support Column Buckling	1.14	0.33	0.54	[3]
Steam Generator Lower Lateral Support	1.23	0.34	0.57	[3]
Steam Generator Intermediate Supports	1.17	0.30	0.59	[3]
Pressurizer	-	-	0.58	[4]
Pressurizer Upper Support Weld[10]	1.02	0.31	0.50	[3]
Pressurizer Upper Support Strut	1.11	0.29	0.56	[3]
Pressurizer Lower Support Strut	1.41	0.29	0.72	[3]
Reactor Coolant Pump[9]	2.2	0.51	0.68	[5]
Reactor Coolant Pump Heat Exchanger[9]	-	-	0.55	[2]
Mechanical Equipment				
Polar Crane	-	-	0.55	[2]

Table 19.55-1 (Sheet 2 of 2)
Seismic Margin Parameters and HCLPF Values

Description	Median pga[1]	βc	HCLPF Value[1]	Basis
Piping – Support Controlled	3.3	0.61	0.81	[5]
Cable trays – Support Controlled	2.2	0.61	0.54	[5]
Accumulator Tank	2.2	0.46	0.76	[5]
Core Make Up Tank	-	-	0.87	[4]
Heat Exchanger (PRHR)	-	-	1.11	[4]
Valves				
Higher than El. 100′	3.3	0.61	0.81	[5]
Equal to or Lower than El. 100′	-	-	1.02	[4]
Passive Containment Cooling System	-	-	0.67	[2]
Electrical Equipment				
Non-Sensitive to High Frequency Excitation	-	-	0.5	[6]
Sensitive to High Frequency Excitation	-	-	0.52	[6]
Ceramic Insulators[7]	0.2	0.35	0.09	[8]

Notes of Table 19.55-1:

[1] pga is the free field peak ground acceleration level for the seismic event.
[2] HCLPF based on conservative deterministic fragility margin approach.
[3] HCLPF based probabilistic fragility analysis.
[4] HCLPF based on deterministic approach.
[5] HCLPF based on URD recommended generic fragility data.
[6] HCLPF based on design margin, code requirements and test margins inherent to the seismic qualification testing. Qualification testing with 99% confidence on the TRS will be limited to 0.3g.
[7] The capacity of the ceramic insulators is less than the review level earthquake of 0.5g. The failure of the ceramic insulators is considered in the PRA analysis.
[8] HCLPF based on recognized generic fragility data
[9] Both the Reactor Coolant Pump Support and Reactor Coolant Pump External Heat Exchanger HCLPF values are controlled by Steam Generator Support.
[10] The HCLPF value of the Pressurizer Upper Support Weld is calculated as 0.6 g using conservative deterministic failure margin method. The value of 0.5 g in the table is used in the PRA/SMA and is more conservative.

Table 19.55-2 (Sheet 1 of 5)
Basic Events HCLPF Values

BE ID	BE Description	HCLPF (g)	Source
EQ-AB-EXTWALL	Failure of Auxiliary Building Exterior Wall	0.88	Exterior walls of auxiliary building, limiting values between *wall 1* and *wall 11*
EQ-AB-FLOOR	Failure of Auxiliary Building Floor	0.88	Same as auxiliary building exterior wall
EQ-AB-INTWALL	Failure of Auxiliary Building Interior Wall	0.88	Same as auxiliary building exterior wall
EQ-ACC-CV28	Accumulator Check Valves 28A and 28B Fail	1.02	In rooms 11206/11207, below elevation 100′
EQ-ACC-CV29	Accumulator Check Valves 29A and 29B Fail	1.02	In rooms 11206/11207, below elevation 100′
EQ-ACC-TANKS	Accumulator Tanks Fail	0.76	
EQ-ACDISPANEL	120 Volt AC Distribution Panels Fail	0.5	Limiting value among those provided for electrical equipment
EQ-ADS-S1MOVS	ADS Stage 1 MOVs RCS-PL-V001A/B and RCS-PL-V011A/B Fail	0.81	In rooms 11603/11703, above elevation 100′
EQ-ADS-S2MOVS	ADS Stage 2 MOVs RCS-PL-V002A/B and RCS-PL-V012A/B Fail	0.81	In rooms 11603/11703, above elevation 100′
EQ-ADS-S3MOVS	ADS Stage 3 MOVs RCS-PL-V003A/B and RCS-PL-V013A/B Fail	0.81	In rooms 11603/11703, above elevation 100′
EQ-ADS-S4VALVES	ADS Stage 4 Squib Valves 4A/B/C/D Fail	0.81	In rooms 11301/11302, above elevation 100′
EQ-BAF-SUPP	Failure of Containment Baffle Support	0.91	
EQ-BAT-RACK	Battery Racks Fail	0.5	Limiting value among those provided for electrical equipment.
EQ-BATTERY	250 Vdc Batteries Fail	0.5	Limiting value among those provided for electrical equipment.

Table 19.55-2 (Sheet 2 of 5)
Basic Events HCLPF Values

BE ID	BE Description	HCLPF (g)	Source
EQ-CABINETS	PMS Cabinet Fail	0.5	Limiting value among those provided for electrical equipment.
EQ-CABLETRAY	Cable Trays Fail	0.54	
EQ-CAS-AOV-1415	Containment CAS Isolation Valves AOV 14 and 15 Fail	0.81	In rooms 12405/11400, above elevation 100′
EQ-CER-INSULATOR	Seismically induced failure of ceramic insulators	0.09	
EQ-CMT-AOV	CMT AOV 14A/B and 15A/B Fail by Seismic Event	1.02	In rooms 11206/11207, below elevation 100′
EQ-CMT-CV	CMT CV 16A/B or 17A/B Fail by Seismic Event	1.02	In rooms 11206/11207, below elevation 100′
EQ-CMT-LEVELSWT	CMT Level Switch Fails	0.5	Limiting value among those provided for electrical equipment.
EQ-CMT-TANKS	CMT Tanks Fail by Seismic Event	0.87	
EQ-CONTPR-SENSOR	Containment Pressure Sensor or Transmitter Fails	0.5	Limiting value among those provided for electrical equipment.
EQ-CORE-ASSEMBLY	Failure of Core Assembly	0.5	
EQ-CRDM	Failure of Control Rod Drive Mechanism	0.7	
EQ-CV-BUCKLE	Containment Vessel Buckling	0.73	
EQ-CV-INTER	Failure of the Interior (concrete) Structure of Containment	0.71	
EQ-CV-OVERT	Containment Vessel Overturning	1.38	
EQ-DCDISPANEL	250 Vdc Distribution Panel Fails	0.5	Limiting value among those provided for electrical equipment.
EQ-DCMCC	DC Motor Control Centers Fail	0.5	Limiting value among those provided for electrical equipment.

Table 19.55-2 (Sheet 3 of 5)
Basic Events HCLPF Values

BE ID	BE Description	HCLPF (g)	Source
EQ-DC-SWBRD	250 Vdc Switchboard Fails	0.5	Limiting value among those provided for electrical equipment.
EQ-DVI-PIPES	Seismically Induced Failure of Both DVI Lines	0.81	
EQ-ELECTRONICS	PMS Electronic Fail	0.5	Limiting value among those provided for electrical equipment.
EQ-INSTR-PIPES	Failure of RCS Instruments Lines	0.81	
EQ-INVERTER	250 Vdc Inverters Fail	0.5	Limiting value among those provided for electrical equipment.
EQ-IRW-INJCV	IRWTS Injection CV 122A/B and 124A/B Fail by Seismic Event	1.02	In rooms 11206/11207, below elevation 100′
EQ-IRW-INJSQ	IRWTS Injection Squib Valves 123A/B and 125A/B Fail by Seismic Event	1.02	In rooms 11206/11207, below elevation 100′
EQ-IRW-RECCV	Sump Recirculation Check valves 119A/B Fail by Seismic Event	1.02	In rooms 11206/11207, below elevation 100′
EQ-IRW-RECMOV	Sump Recirculation MOVs 117A/B Fail by Seismic Event	1.02	In rooms 11206/11207, below elevation 100′
EQ-IRW-RECSQ	Failure of Recirculation Squib Valves 118A/B and 120A/B by Seismic Event	1.02	In rooms 11206/11207, below elevation 100′
EQ-IRWST-TANK	Failure of IRWST	0.71	
EQ-MSL-SENSOR	Main Steam Line Pressure Sensor or Transmitter Fails	0.5	Limiting value among those provided for electrical equipment.
EQ-PCC-TANK	Passive Containment Core Cooling Tank Fails	0.81	
EQ-POL-CRANE	Failure of the Polar Crane	0.55	
EQ-PRHR-AOV	Passive RHR AOVs PXS-PL-V108A and B Fail by Seismic Event	0.81	In room 11300, above elevation 100′
EQ-PRHR-HX	Failure of Passive RHR Heat Exchanger	1.11	

Table 19.55-2 (Sheet 4 of 5)
Basic Events HCLPF Values

BE ID	BE Description	HCLPF (g)	Source
EQ-PRZR-FAILS	Seismically Induced Failures of the Pressurizer	0.5	Pressurizer upper support weld (limiting HCLPF among pressurizer components)
EQ-PRZR-LVTRANS	Seismically Induced Failure of Pressurizer Level Transmitter	0.5	Limiting value among those provided for electrical equipment.
EQ-PRZR-SENSOR	Pressurizer Sensor Or Transmitter Fails	0.5	Limiting value among those provided for electrical equipment.
EQ-PRZR-SV	Pressurizer Safety Valves RCS-PL-V005A/B Fail Seismically	0.81	In rooms 11603/11703, above elevation 100′
EQ-RCP-FAILS	Reactor Coolant Pumps Fail	0.54	Same as SG due to connection between RCP & SG.
EQ-RCP-HX	Seismically Induced RCP HX Failure Inducing a LOCA	0.55	
EQ-RCS-PIPES	Failure of RCS Piping	0.81	
EQ-RV-FAILS	Reactor Pressure Vessel Fails	0.56	
EQ-RV-FUEL	Fuel in Reactor Vessel Fails	0.5	
EQ-RV-HDPK	Reactor Vessel Integrated Head Package Fails	0.7	Same as CRDM due to physical location
EQ-SG-FAILS	Seismically Induced Failures of the Steam Generators	0.54	
EQ-SGTR	Seismically Induced SGTR	0.54	Same as SG failure
EQ-SHBLD-ROOF	Shield Building Roof Fails	0.71	
EQ-SHBLD-WALL	Shield Building Wall Fails	0.71	Same as roof
EQ-SLB	Failure of Feed and Steam Pipes on Secondary Side	0.81	
EQ-TRSFSWITCH	Transfer Switches Fail	0.5	Limiting value among those provided for electrical equipment.

Table 19.55-2 (Sheet 5 of 5)
Basic Events HCLPF Values

BE ID	BE Description	HCLPF (g)	Source
EQ-VFS-AOV-0304	Containment Air Filtration System Containment Air Supply Isolation Valves AOV 03 and 04 Fail	0.81	In rooms 12452/11400, above elevation 100′
EQ-VFS-AOV-0910	Containment Air Filtration System Containment Air Exhaust Isolation Valves Fail (009, 010, 800A/B, and 803A/B)	0.81	In rooms 12452/11400, above elevation 100′
EQ-WLS-AOV-5557	WLS Cont. Sump Isolation Valves AOV 55 and 57 Fail	0.81	In rooms 11300/12244, above elevation 100′

Table 19.55-3
EQ-IEV-STRUC (EQSTR-02) HCLPF

		Original AP1000	Updated AP1000
1	EQ-AB-FLOOR	0.51g	0.88g
2	EQ-AB-EXTWALL	0.51g	0.88g
3	EQ-AB-INTWALL	0.51g	0.88g
4	EQ-BAF-SUPP	1.30g	0.91g
5	EQ-PCC-TANK	0.51g	0.81g
6	EQ-SHBLD-ROOF	0.51g	0.71g
7	EQ-SHBLD-WALL	0.51g	0.71g
8	EQ-CV-INTER	0.50g	0.71g
9	EQ-CV-BUCKLE	0.66g	0.73g
10	EQ-CV-OVERT	1.11g	1.38g
11	EQ-IRWST-TANK	0.50g	0.71g
12	EQ-POL-CRANE	0.77g	0.55g
	IE HCLPF=	0.50g	0.55g

Table 19.55-4
EQ-IEV-RVFA (EQRVF-02) HCLPF

		Original AP1000	Updated AP1000
1	EQ-DVI-PIPES	0.81g	0.81g
2	EQ-SG-FAILS	0.54g	0.54g
3	EQ-RCP-FAILS	0.68g	0.54g
4	EQ-PRZR-FAILS	0.55g	0.50g
5	EQ-RV-FUEL	0.50g	0.50g
6	EQ-RV-HDPK	0.70g	0.70g
7	EQ-RV-FAILS	0.64g	0.56g
	IE HCLPF =	0.50g	0.50g

Table 19.55-5
EQ-IEV-LLOCA HCLPF

		Original AP1000	Updated AP1000
1	EQ-PRHR-HX	0.76g	1.11g
2	EQ-RCS-PIPES	0.81g	0.81g
	IE HCLPF =	0.76g	0.81g

Table 19.55-6
EQ-IEV-SLOCA HCLPF

		Original AP1000	Updated AP1000
RCS Instrumentation Pipe Breaks	EQ-INSTR-PIPES	0.81g	0.81g
Secondary Line Breaks	EQ-SLB	0.81g	0.81g
SGTR	EQ-SGTR	0.54g	0.54g
RCP HX	EQ-RCP-HX	-	0.55g
	HCLPF =	0.54g	0.54g

Table 19.55-7
EQ-IEV-ATWS HCLPF

		Original AP1000	Updated AP1000
1	EQ-CORE-ASSEMBLY	0.50g	0.50g
2	EQ-CRDM	0.70g	0.70g
	HCLPF =	0.50g	0.50g

Table 19.55-8
Sequence and Plant HCLPF

ET	Original AP1000	Updated AP1000
EQ-STRUC	EQSTR-02	0.55
	EQ-STRUC HCLPF	*0.55*
EQ-RVFA	EQRVF-02	0.50
	EQ-RVFA HCLPF	*0.50*
EQ-LLOCA	EQLLO-02	0.81
	EQLLO-03	0.81
	EQLLO-05	0.81
	EQLLO-06	0.81
	EQLLO-08	0.81
	EQLLO-09	0.81
	EQLLO-10	0.81
	EQLLO-11	0.81
	EQ-LLOCA HCLPF	*0.81*
EQ-SLOCA	EQSLO-02	0.54
	EQSLO-03	0.54
	EQSLO-04	0.54
	EQSLO-05	0.87
	EQ-SLOCA HCLPF	*0.54*
EQ-ATWS	EQATW-02	0.50
	EQATW-03	0.50
	EQATW-04	0.50
	EQATW-05	0.87
	EQATW-06	0.81
	EQATW-07	0.71
	EQ-ATWS HCLPF	*0.50*
EQ-LOSP	*All mixed cut sets (IE HCLP =0.09)*	*N/A*
	Plant HCLPF	***0.50***

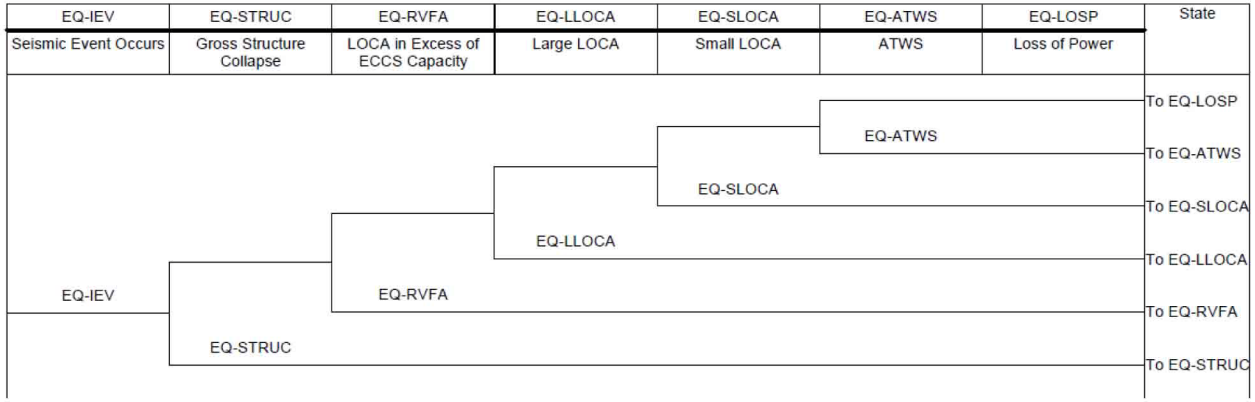

Figure 19.55-1 Seismic Initiating Event Hierarchy Tree

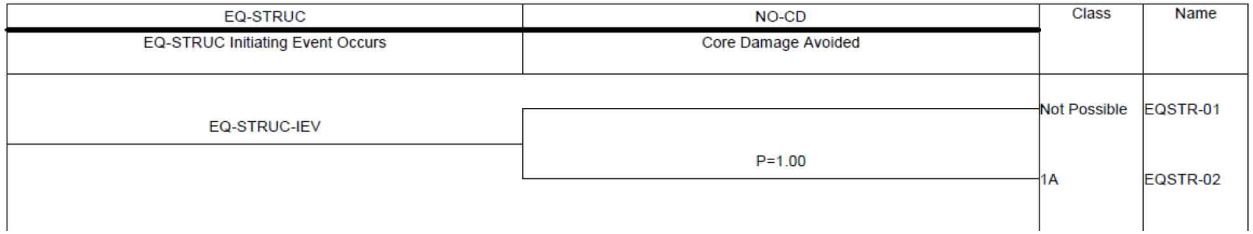

Figure 19.55-2 Seismic Induced Gross Structural Collapse Event Tree

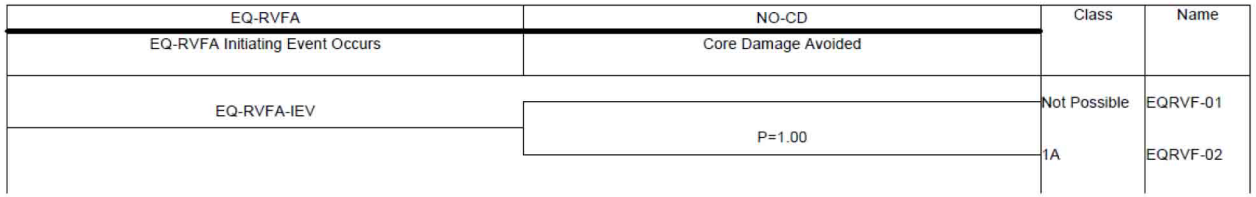

Figure 19.55-3 Seismic Induced Excessive LOCA Event Tree

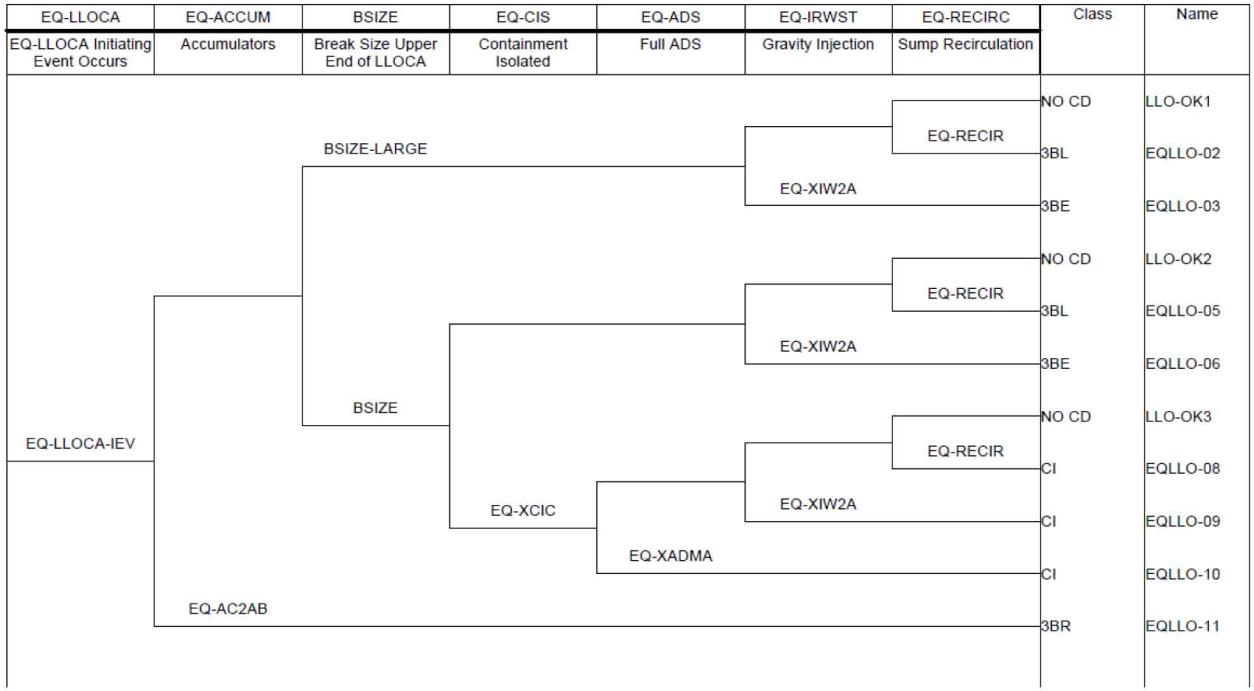

Figure 19.55-4 Seismic Induced Large LOCA Event Tree

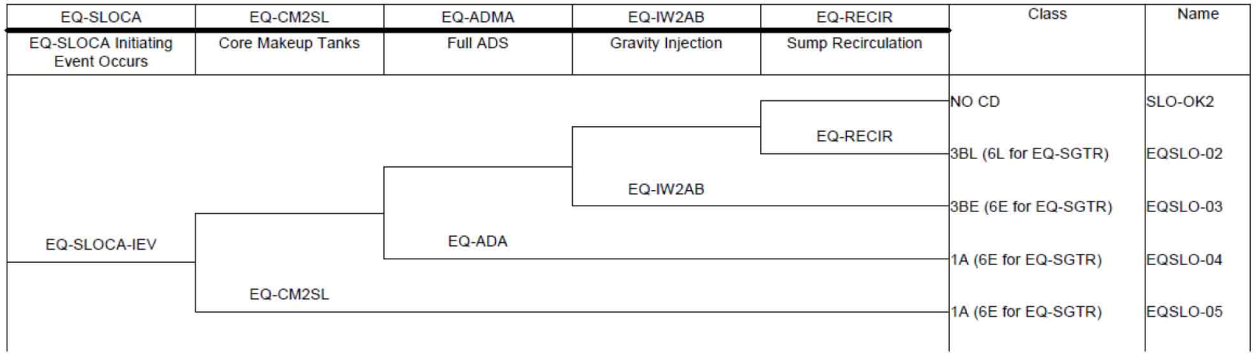

Figure 19.55-5 Seismic Induced Small LOCA Event Tree

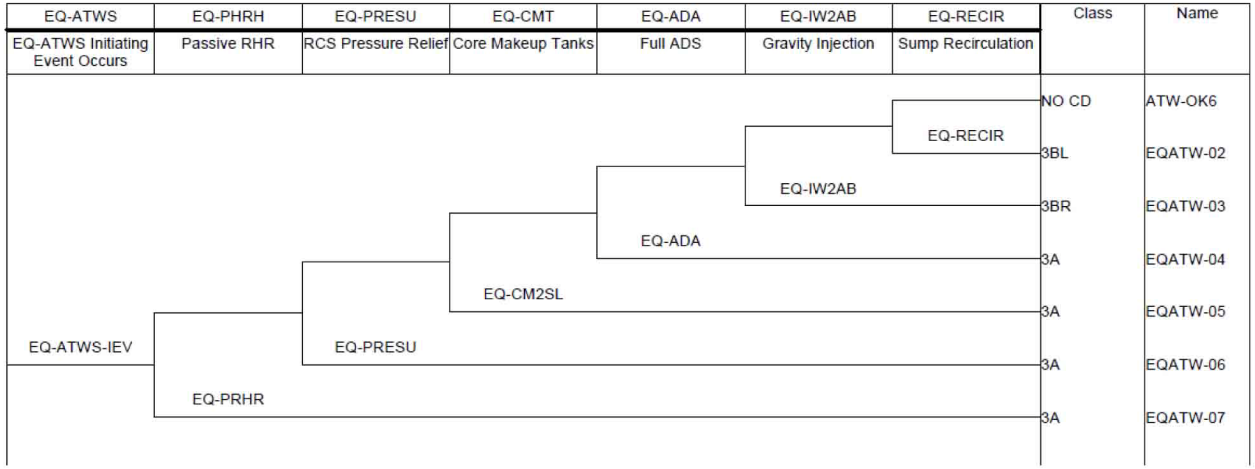

Figure 19.55-6 Seismic Induced ATWS Event Tree

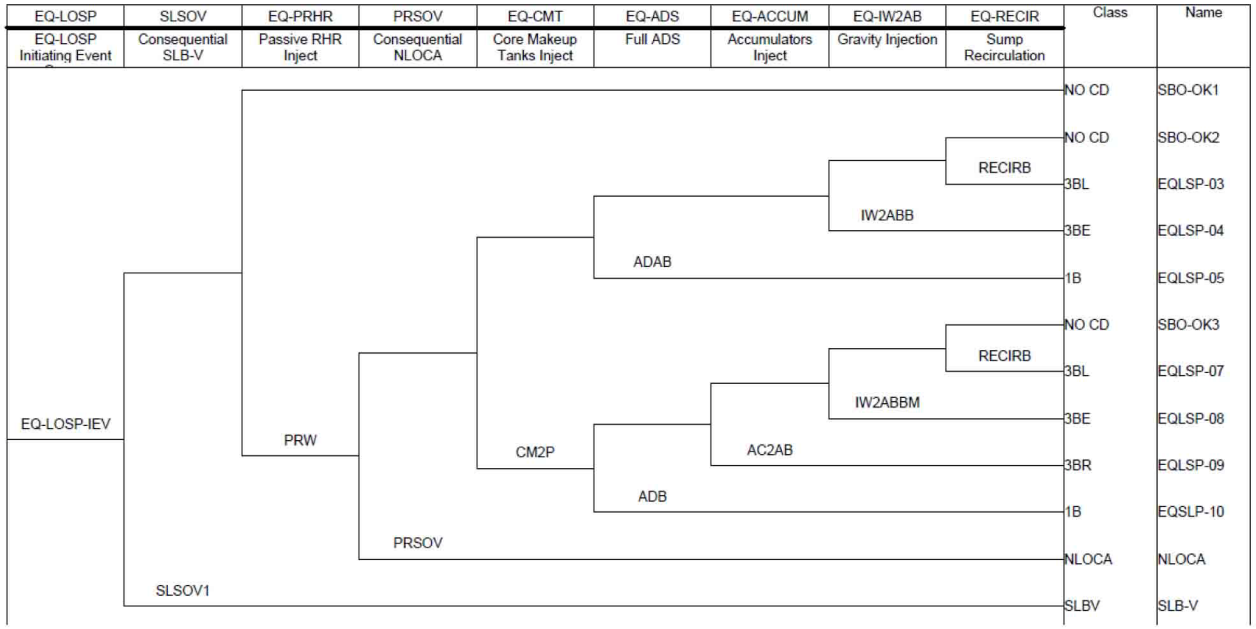

Figure 19.55-7 Seismic Induced LOSP Event Tree

19.56 PRA Internal Flooding Analysis

The design certification of the AP1000 included consideration by the NRC of the topic referred to in this section.

19.57 Internal Fire Analysis

The design certification of the AP1000 included consideration by the NRC of the topic referred to in this section.

19.58 Winds, Floods, and Other External Events

19.58.1 Introduction

External events considered in the AP1000 PRA are those events whose cause is external to all systems associated with normal and emergency operations situations. Some external events may not pose a significant threat of a severe accident. Some external events are considered at the design stage and have a sufficiently low contribution to core damage frequency or plant risk.

Based upon the guidelines provided in References 19.58-1 and 19.58-2, the following is a list of six external events that are included for AP1000 analysis:

- High winds and tornadoes
- External floods
- Transportation and nearby facility accidents
- Seismic events
- Internal fires
- External fires

The first three external events are addressed in this section. Seismic events and internal fires are addressed in the AP1000 PRA. Based on site-specific information, the COL applicant should reevaluate the qualitative screening of external fires. Accordingly, based on the criteria to screen out external hazards in the PRA, a risk evaluation should be performed if it cannot be demonstrated that the frequency of hazard is less than 1E-7/yr. If any site-specific susceptibilities are found, the site-specific PRA performed to address COL Holder Item 19.59.10-2 should include external fires.

Chapter 2 defines the site characteristics for which the AP1000 is designed. A site is acceptable if the site characteristics fall within the AP1000 site interface parameters.

19.58.2 External Events Analysis

19.58.2.1 Severe Winds and Tornadoes

The overall methodology recommended by NUREG-1407 for analyzing plant risk due to high winds and tornados is a progressive screening approach. This approach is modified to consider determining the acceptability of hazard frequency and risk. High winds (including tornadoes) can affect plant structures in at least two ways: (1) if wind forces exceed the load capacity of a building or other external facility, the walls or framing might collapse or the structure might overturn from the excessive loading; and (2) if the wind is strong enough, as in a tornado or hurricane, it may be capable of lifting materials and thrusting them as missiles against the plant structures that house safety-related equipment. Critical components or other contents of plant structures not designed to resist missile penetration might be damaged and lose their function.

The NUREG-1407 criterion for high winds and tornados states that “these events pose no significant threat of a severe accident because the current design criteria for wind are dominated by tornadoes having an annual frequency of exceedance of about 10^{-7}.” This is interpreted to mean that events with an annual frequency of exceedance less than 1.0E-07 may be removed from further consideration and events with an annual frequency of exceedance greater than 1.0E-07 must be further evaluated. However, the NUREG-1407 criterion was developed for currently operating plants.

High winds and tornados tend to behave as a loss of offsite power (LOSP) since the site switchyard is unprotected and not designed against high wind velocities. For wind velocities greater than the design basis, additional structures, systems, and components (SSC) may also fail. Therefore, two analyses are performed, one considering only a LOSP, and another considering a LOSP with failure

of the standby nonsafety systems. This analysis considers not only excessive wind forces, but also missile generation. A conditional core damage probability will be calculated for each of those scenarios. Risk due to the event can be estimated using the following equation:

$$CDF = IEF * CCDP \quad \text{(Equation 19.58-1)}$$

Where CDF is annual core damage frequency, IEF is the initiating event frequency, and CCDP is the conditional core damage probability. If this evaluation indicates an acceptably small contribution to risk (e.g., less than 10% of the total plant CDF), then the progressive screening is complete and no detailed PRA will be necessary.

A sensitivity study is performed for the above two cases with a loss of component cooling water/ service water considered also because those systems may not be available following above design basis winds.

The analysis for winds and tornadoes is site-specific. It is anticipated that a high wind or tornado event would result in a loss of offsite power because the switchyard is likely to become unavailable during the event.

The analysis for high winds and tornados begins with an examination of the design basis for the plant, which is documented in Chapter 2.

The AP1000 design basis wind speed for tornados is 300 mph as discussed in Chapter 2. This value is assumed to be the maximum wind speed that will not challenge the safety-related structures. The AP1000 operating basis wind speed is 145 mph as discussed in Chapter 2. This value is assumed to be the maximum wind speed that will not challenge the nonsafety-related structures.

The structures protecting safety-related features of the AP1000 are designed for extreme winds and missiles associated with these winds. As long as the external event winds are less than these design basis winds, the safety features of the AP1000 will be unaffected. If the winds exceed the design values, then the integrity of the safety-related structures may be compromised.

RN-13-003

The structures protecting nonsafety-related features of the AP1000 are designed according to Uniform Building Code or International Building Code and have some level of protection against seismic and high wind events. As long as the external event winds are less than the operating basis winds (145 mph, per Chapter 2), the nonsafety features of the AP1000 will be unaffected. If the winds exceed the operating basis values, then the integrity of the nonsafety relates structures may be compromised.

In summary of the design against high winds, the plant is designed against 300 miles per hour (mph) winds. The operating basis of the plant is winds up to 145 mph. This means that the safety structures are protected against winds up to 300 mph and nonsafety system (NSS) structures are protected against winds up to 145 mph. Per the Enhanced Fujita Scale for Tornados (Table 19.58-1), no tornados are expected to exceed 300 mph; however, EF3, EF4, and EF5 tornados do exceed the operating basis of the AP1000. Per the Saffir-Simpson Scale for Hurricanes (Table 19.58-2), no hurricanes are expected to reach 300 mph winds; however, Category 3, Category 4 and Category 5 hurricane winds do exceed the operating basis of the AP1000.

Three studies are performed to evaluate the high wind events. The Case 1 study is a LOSP induced by each of the events, with no other equipment unavailable. A conditional core damage probability (CCDP) is developed for this scenario, which may be multiplied by the high wind event frequency. All tornados and hurricanes are considered in this Case 1 as they may challenge the AP1000 switchyard. Extratropical cyclones are normal storms and thunderstorms with winds expected to fall below the operating basis for the AP1000. They are also included in the Case 1 analysis.

As stated above, the EF3, EF4, and EF5 tornados and Category 3, Category 4 and Category 5 hurricanes may challenge the nonsafety-related structures in the AP1000. Therefore, these events will be evaluated with the loss of additional SSCs. The Case 2 study is created by modifying the Case 1 analysis for the EF3, EF4, and EF5 tornados, and Category 3, Category 4 and Category 5 hurricanes to have a LOSP with additional failures of nonsafety systems unavailable. A CCDP is developed for this scenario, which may be multiplied by the high wind event frequency.

The final Case 3 is a conservative study where all high wind events are evaluated as a LOSP with failure of the nonsafety systems. This case is created to represent the worst case scenario. In this analysis, events are considered of low risk importance if their initiating event frequency is less than 1.0E-07 or if their estimated CDF is less than 1.0E-08 events/yr.

The results of the CDF calculation are shown in Table 19.58-3. Equation 19.58-1 was used to determine the resultant CDF.

In Table 19.58-3, none of the initiating event frequencies were sufficiently low to be removed from further consideration. Therefore, the CDF calculation was performed. In each case, the resultant CDF is less than 1.0E-08 events/yr. The Category 4 and Category 5 hurricane frequency is considered to be extremely conservative at 1.00E-02 events/yr. An event with the conservative initiating event frequency, and the worst case sensitivity study (Case 3), the resultant CDF is still less than the CDF criterion of 1.0E-08 events/yr. Case 2 is considered to be the representative model for high winds, with Case 1 and Case 3 being treated as sensitivity studies on the baseline. Case 3 is conservative in that it assumes total failure of the standby non-safety systems (CVS, RNS, SFW, automatic DAS, and diesel generators) for all high wind events. As AP1000 non-safety structures have been designed to building codes that offer an added level of protection, the above failures are considered extreme and conservative. Therefore, while the total Case 3 CDF does fall above the 1.0E-08 events/yr CDF screening criteria, the results are considered very conservative for the above reasons. Therefore, no further detailed PRA is necessary for the AP1000 high winds and tornados analysis. RN-13-003

19.58.2.2 External Floods

An external flooding analysis is performed to verify that any significant contribution to core damage frequency resulting from plant damage caused by storms, dam failure, and flash floods is accounted for as follows:

> The analysis for external floods begins with an examination of the design basis for the plant, which is documented in Chapter 2. The AP1000 is protected against floods up to the 100′ level. The 100′ level corresponds to the plant ground level. From this point, the ground is graded away from the structures. Thus, water will naturally flow away from the structures. Additionally, all seismic Category I SSCs are designed to withstand the effects of flooding. The seismic Category I SSCs below grade (below ground level) are protected against flooding by a waterproofing system. None of the non-safety SSCs were found to be important based on flooding considerations. RN-12-038
>
> The basic steps involved in an external flooding analysis are similar to those followed for internal flooding in the individual plant examination. However, the focus of attention is on areas, which due to their location and grading, may be susceptible to external flood damage. This requires information on such items as dikes, surface grading, locations of structures, and locations of equipment within the structures. Information such as meteorological data for the site, historical flood height, and frequency data, is also needed.

Only one site indicated susceptibility to external floods due to hurricane surge water. That site is located at an elevation of 45 feet above sea level. Therefore, the AP1000 100′ level, for this site,

corresponds to 45′ above sea level. Per Subsection 3.4.1.1, the ground will be graded away from the structures beginning at the 100′ level and sloping downward away from the structures.

Category 5 hurricanes, per the Saffir-Simpson scale, are capable of storm surges greater than18 feet. The storm surge of record for a hurricane is 27.8 feet recorded for Katrina (2005). Based on historical information, a hurricane storm surge above the 28-foot level may be classified as an extremely rare event. Engineering judgment is used to establish that the frequency of this type of flood is significantly less than the 10^{-7} per year criterion for initiating event frequency.

As a sensitivity study, the 1.0E-07/yr initiating event frequency is taken as the frequency of an event that may challenge the nonsafety structures in the plant. This sensitivity study also considers failure of the switchyard due to flooding. LOSP with failure of the nonsafety systems CCDP was developed. Equation 1 was used to determine the resultant CDF.

As expected, the risk due to a flooding event is low for the AP1000. The resultant CDF of 5.85E-15/yr is an insignificant contribution to total plant CDF.

For other sites, the AP1000 is designed to site characteristics described in Chapter 2. The site selection criterion provides that for an accident that has potential consequences serious enough to affect the safety of the plant to the extent that 10 CFR 50.34 guidelines are exceeded, the annual frequency of occurrence is less than 1.0E-06 per year. This criterion should be extended to an annual frequency of occurrence less than 1.0E-07 per year for the AP1000 design. As none of the surveyed sites indicated susceptibility to floods due to dam failure and/or flash floods, those events should be considered on a site-by-site basis.

19.58.2.3 Transportation and Nearby Facility Accidents

These events consist of accidents related to transportation near the nuclear power plant and accidents at industrial and military facilities in the vicinity. The following modes of transportation are considered:

- Aviation (commercial/general/military)
- Marine (ship/barge) and nearby facility
- Pipeline (gas/oil)
- Railroad
- Truck

19.58.2.3.1 Aviation Accidents

For limiting event frequency of 1.21E-06/year with most of that frequency for small aircraft, and with commercial aircraft contribution 9.40E-09/year, then the following discussion is applicable.

A conservative analysis was performed to evaluate the risk due to small aircraft accidents onsite. This analysis assumes a LOSP and loss of component cooling water/service water event, and conservatively fail a set of standby nonsafety systems. This is acceptable because it is unlikely that a small aircraft accident would challenge the passive safety systems inside containment. This leaves only the nonsafety systems outside containment as vulnerable. However, this evaluation is conservative because it is unlikely that a small aircraft would have the capacity to fail such a large area of the AP1000.

Equation 19.58-1 is used to determine the resultant CDF. A CDF of 7.08E-14/yr is calculated and is an insignificant contribution to total plant CDF of approximately 5.08E-07/yr. Therefore, sites that can demonstrate an aviation event frequency less than or equal to 1.21E-06/yr for small aircraft accidents are bounded by this evaluation.

Larger commercial aircraft may have the capacity to challenge SSCs within the AP1000 containment. However, the containment structure and safety systems are designed to withstand various earthquake levels so that many of the safety system SSCs will still be available following the accident. To consider the already low risk of the AP1000 design, the 1.0E-07 events/yr criterion for event frequency is applicable for larger commercial aircraft. Sites that can demonstrate a commercial aircraft aviation event frequency less than the 1.0E-07/yr criterion are also bounded by this analysis. For this current evaluation, the highest initiating event frequency reported for large commercial aircraft is 9.40E-09 events/yr. This value falls below the 1.0E-07 events/yr screening criteria. Therefore, no further evaluation is necessary.

19.58.2.3.2 Marine and Nearby Facility Accidents

Only sites with large waterways with ship and/or barge traffic that goes through or near the site need to consider marine accidents.

Marine (ship/barge) accidents and nearby land-based facility accidents pose a potential hazard to a nuclear power plant due to two possibilities:

1. Release of hazardous material towards the plant
2. Explosion with resulting damage to the plant

The potential exists for a marine (or any other mode of transportation) or nearby facility accident that leads to a release of toxic materials into the atmosphere. This type of event may compromise the safety of the plant operators, resulting in reduced operator reliability. However, the toxic release does not directly lead to any failure of plant equipment. To evaluate the risk impact of this scenario, a CCDP is developed that models a reactor trip followed by the guaranteed failure of all PRA credited operator actions. Failure of all PRA credited operator actions obviates the need to evaluate specific toxic release events with respect to differences in the type and amount of material released and duration of the release. The resulting CCDP is 6.26E-08.

Equation 19.58-1 (CDF = IEF * CCDP) is used to determine the maximum frequency for toxic releases, from all sources combined, that would keep the resulting CDF below the 1.0E-08 screening threshold. That maximum value is (1.0E-08/6.3E-08) or 0.15 events per year. This initiating event frequency represents hazardous chemical releases that exceed the assumptions and screening criteria described in U.S. NRC Regulatory Guide 1.78 for screening out release events that need not be considered in the evaluation of control room habitability. The number of events to consider could be determined by the COL applicant contacting the county public safety or emergency management departments and requesting a list of chemical spills that occurred within 5 miles of the plant and required HAZMAT intervention. Only these cases would need to be screened in accordance with Regulatory Guide 1.78 to determine if each event warranted the classification of a toxic release initiating event. If the frequency of toxic releases from all possible sources is demonstrated to be less than 0.15 events per year, the toxic release event is screened out from the need to do additional detailed PRA analyses.

The above analysis is conservative. The AP1000 has an additional level of defense against toxic airborne material. With advanced warning, the operators may actuate passive control room habitability. This system isolates the control room from normal HVAC and actuates a separate system supplied from compressed air containers. The compressed air slightly pressurizes the control room above atmospheric pressure, preventing the entrance of toxic material in the control room. This system is available for 72 hours, which is adequate time to withstand the event.

There is also a potential for marine explosion accidents. The AP1000 is not designed with a service water intake structure. Therefore, loss of service water events as a consequence of marine explosions are not a concern for the AP1000 design. As long as Regulatory Guide 1.91 acceptance

criterion is met, marine explosion accidents do not need to be considered further for the AP1000 PRA.

19.58.2.3.3 Pipeline Accidents

Pipeline accidents could pose a hazard to the AP1000 due to the release of hazardous material or the possibility of an explosion and resulting damage to the plant. For a site with a 30-inch gas line approximately 5800 feet away, a semi-quantitative evaluation is performed.

Considerations for the evaluation are as follows:

- Gas pipe rupture frequency
- Gas cloud formation probability
- Gas cloud transportation and nondispersion probability
- Gas cloud ignition probability onsite

Figure 19.58-1 is considered to further evaluate the probability of this accident. When considering the probability of forming a dense gas cloud, and the probability of the wind speed and direction to be in the ranges necessary to transport the gas cloud 5800 feet to the site, without dispersing the gas, including ignition of the gas cloud onsite in a location that may challenge the plant, this probability becomes very low.

Site habitability is also a concern for toxic materials. However, the AP1000 has an additional level of defense against toxic airborne material. With advanced warning, the operators may actuate passive control room habitability. This system isolates the control room from normal HVAC and actuates a separate system supplied from compressed air containers. The compressed air slightly pressurizes the control room above atmospheric pressure, preventing the entrance of toxic material in the control room. This system is available for 72 hours, which is adequate time to withstand the event. The expected frequency value is expected to be below the initiating event criterion of 1.0E-07 events/year. Therefore, no further quantitative evaluation is necessary.

19.58.2.3.4 Railroad and Truck Accidents

Railroad accidents could pose a hazard to the AP1000 due to the release of hazardous material or the possibility of an explosion and resulting damage to the plant. Toxic material releases were evaluated in the marine accident evaluation as to not be important to AP1000 plant risk. Significant damage to the AP1000 plant was evaluated in the aviation accident evaluation. No railroad accidents are expected to result in the amount of damage that may be seen from an aviation accident. This is especially true considering the increased security barriers established at U.S. nuclear power plants.

The AP1000 is designed to site characteristics described in Chapter 2. The site selection criterion provides that, for an accident that has potential consequences serious enough to affect the safety of the plant to the extent that 10 CFR 50.34 guidelines are exceeded, the annual frequency of occurrence is less than 1.0E-06 per year. This criterion should be extended to an annual frequency of occurrence less than 1.0E-07 per year for the AP1000 design.

19.58.2.4 Malevolent Aircraft Impact

Malevolent aircraft impact is discussed in Appendix 19F.

19.58.3 Conclusion

The risk due to external hazards is low for the AP1000 design for the participating sites listed in Section 3.2. The AP1000 design is shown to be highly robust against the external events discussed

in this section. The design is resilient against high winds, external floods, and other external events that challenge various equipment in the plant.

Based on site-specific information, the COL applicant should reevaluate the qualitative screening of external fires. Accordingly, based on the criteria to screen out external hazards in the PRA, a risk evaluation should be performed if it cannot be demonstrated that the frequency of hazard is less than 1E-7/yr. If any site-specific susceptibilities are found, the site-specific PRA performed to address COL Holder Item 19.59.10-2 should include external fires.

The following conclusions and insights are derived from the AP1000 external events assessment for events at power:

1. High winds and tornados were quantitative evaluated to be of low risk to the AP1000 design for each of the participating sites. A bounding assessment is provided to show that the expected CDF due to any one of these events does not exceed 1.0E-08 events/year. The same is true for the aggregate results. Sensitivity studies were performed to determine that there is low risk for more limiting scenarios. No further analysis is suggested.

2. The AP1000 is designed to flooding levels described in Chapter 2. The site selection criterion provides that, for an accident that has potential consequences serious enough to affect the safety of the plant to the extent that 10 CFR 50.34 guidelines are exceeded, the annual frequency of occurrence is less than 1.0E-06 per year. This criterion can be extended to an annual frequency of occurrence less than 1.0E-07 per year for the AP1000 design. No further analysis is suggested.

3. Transportation and nearby facilities accidents are qualitatively evaluated to be of low risk importance and do not warrant further evaluation.

A site-specific review of the generic PRA should be conducted to verify that the assumptions in the PRA bound the site-specific conditions for the applicant's site.

Table 19.58-201 documents the site-specific external events evaluation that has been performed to VCSNS Units 2 and 3. This table provides a general explanation of the evaluation and resultant conclusions and provides a reference to applicable sections of the FSAR where more supporting information (including data used, methods and key assumptions) regarding the specific event is located. Based upon this evaluation, it is concluded that the VCSNS Units 2 and 3 site is bounded by the High Winds, Floods and Other External Events analysis documented in Section 19.58 and APP-GW-GLR-101 (Reference 201) and no further evaluations are required at the COL application stage.

19.58.4 References

19.58-1. "Individual Plant Examination of External Events (IPEEE) for Severe Accident Vulnerabilities - 10 CFR 50.54(f)," Generic Letter 88-20, Supplement 4, June 28, 1991.

19.58-2. NUREG-1407, "Procedural and Submittal Guidance for the Individual Plant Examination of External Events (IPEEE) for Severe Accident Vulnerabilities," June 1991.

19.58-3. National Weather Service, "The Enhanced Fujita Scale," February 2, 2007, http://www.spc.noaa.gov/efscale/.

19.58-4. National Weather Service, “The Saffir-Simpson Hurricane Scale,” June 22, 2006, http://www.nhc.noaa.gov/aboutsshs.shtml.

19.58-5. U.S. Nuclear Regulatory Commission Regulatory Guide 1.91, “Evaluation of Explosions Postulated to Occur on Transportation Routes Near Nuclear Power Plants,” Revision 1, February 1978.

201. Westinghouse Electric Company LLC, “AP1000 Probabilistic Risk Assessment Site-Specific Considerations,” Document Number APP-GW-GLR-101, Revision 1, October 2007.

Table 19.58-1
Description of the Enhanced Fujita Scale (Tornados)

(Reference 19.58-3)

Scale Number	Intensity Phrase	Wind Speed	Type of Damage Done
EF0	Gale tornado	65-85 mph	Some damage to chimneys; breaks branches off trees; pushes over shallow-rooted trees; Some damage to chimneys; branches broken off trees; shallow-rooted trees pushed over; sign boards damaged.
EF1	Moderate tornado	86-110 mph	Peels surface off roofs; mobile homes pushed off foundations or overturned; moving autos blown off roads.
EF2	Significant tornado	111-135 mph	Roofs torn off frame houses; mobile homes demolished; boxcars overturned; large trees snapped or uprooted; light-object missiles generated; cars lifted off ground.
EF3	Severe tornado	136 - 165 mph	Roofs and some walls torn off well-constructed houses; trains overturned; most trees in forest uprooted; heavy cars lifted off the ground and thrown.
EF4	Devastating tornado	166-200 mph	Well-constructed houses leveled; structures with weak foundations blown away some distance; cars thrown and large missiles generated.
EF5	Incredible tornado	>200 mph	Strong frame houses leveled off foundations and swept away; automobile-sized missiles fly through the air in excess of 100 meters (109 yds); trees debarked; incredible phenomena will occur.

Table 19.58-2
Description of Saffir-Simpson Scale (Hurricanes)

(Reference 19.58-4)

Category Number	Wind Speed	Category Description
1	74-95 mph	Storm surge generally 4-5 ft above normal. No real damage to building structures. Damage primarily to unanchored mobile homes, shrubbery, and trees. Some damage to poorly constructed signs. Also, some coastal road flooding and minor pier damage.
2	96-110 mph	Storm surge generally 6-8 feet above normal. Some roofing material, door, and window damage of buildings. Considerable damage to shrubbery and trees with some trees blown down. Considerable damage to mobile homes, poorly constructed signs, and piers. Coastal and low-lying escape routes flood 2-4 hours before arrival of the hurricane center. Small craft in unprotected anchorages break moorings.
3	111-130 mph	Storm surge generally 9-12 ft above normal. Some structural damage to small residences and utility buildings with a minor amount of curtain wall failures. Damage to shrubbery and trees with foliage blown off trees and large trees blown down. Mobile homes and poorly constructed signs are destroyed. Low-lying escape routes are cut by rising water 3-5 hours before arrival of the center of the hurricane. Flooding near the coast destroys smaller structures with larger structures damaged by battering from floating debris. Terrain continuously lower than 5 ft above mean sea level may be flooded inland 8 miles (13 km) or more. Evacuation of low-lying residences with several blocks of the shoreline may be required.
4	131-155 mph	Storm surge generally 13-18 ft above normal. More extensive curtain wall failures with some complete roof structure failures on small residences. Shrubs, trees, and all signs are blown down. Complete destruction of mobile homes. Extensive damage to doors and windows. Low-lying escape routes may be cut by rising water 3-5 hours before arrival of the center of the hurricane. Major damage to lower floors of structures near the shore. Terrain lower than 10 ft above sea level may be flooded requiring massive evacuation of residential areas as far inland as 6 miles (10 km).
5	>155 mph	Storm surge generally greater than 18 ft above normal. Complete roof failure on many residences and industrial buildings. Some complete building failures with small utility buildings blown over or away. All shrubs, trees, and signs blown down. Complete destruction of mobile homes. Severe and extensive window and door damage. Low-lying escape routes are cut by rising water 3-5 hours before arrival of the center of the hurricane. Major damage to lower floors of all structures located less than 15 ft above sea level and within 500 yards of the shoreline. Massive evacuation of residential areas on low ground within 5-10 miles (8-16 km) of the shoreline may be required.

Table 19.58-3
High Winds and Tornados Results

Category	Event	Limiting Initiating Event Freq. (/yr)	CDF (/yr)		
			LOSP (Case 1) (/yr)	LOSP with Nonsafety Systems Unavailable for Select Events (Case 2) (/yr)	LOSP with Nonsafety Systems Unavailable for All Events (Case 3) (/yr)
High Winds	EF0 Tornado	1.00E-03	9.81E-12	9.81E-12 (1)	5.85E-11
	EF1 Tornado	1.00E-03	9.81E-12	9.81E-12 (1)	5.85E-11
	EF2 Tornado	1.00E-03	9.81E-12	9.81E-12 (1)	5.85E-11
	EF3 Tornado	1.00E-03	9.81E-12	5.85E-11	5.85E-11
	EF4 Tornado	1.00E-03	9.81E-12	5.85E-11	5.85E-11
	EF5 Tornado	1.00E-03	9.81E-12	5.85E-11	5.85E-11
	Cat. 1 Hurricane	1.00E-01	9.81E-10	9.81E-10(1)	5.85E-09
	Cat. 2 Hurricane	5.00E-02	4.91E-10	4.91E-10(1)	2.93E-09
	Cat. 3 Hurricane	3.00E-02	2.94E-10	1.76E-09	1.76E-09
	Cat. 4 Hurricane	1.00E-02	9.81E-11	5.85E-10	5.85E-10
	Cat. 5 Hurricane	1.00E-02	9.81E-11	5.85E-10	5.85E-10
	Extratropical Cyclones	3.00E-02	2.94E-10	2.94E-10(1)	1.76E-09
Totals			2.32E-09	4.90E-09	1.38E-08

Note:
1. CDF values from Case 1 were used to illustrate the winds from these events will not challenge additional plant SSCs.

Table 19.58-201 (Sheet 1 of 3)
External Event Frequencies for VCSNS Units 2 and 3

Category	Event	Applicable to site? (Y/N)[a]	Explanation of Applicability Evaluation	Event Frequency
High Winds	EF0 Tornado	Y	Tornado activity in the surrounding counties of the VCSNS Units 2 and 3 site is provided in Table 2.3-227 from 1950 through August 2003. Due to the relative proximity of Laurens County to the other surrounding counties, activity in this area was also included within the evaluation. The event frequency was determined for each tornado category using a point probability method [**PS=n(a/A)**]. First, the average impacted area (**a**) was calculated by averaging the area of each category of tornado activity (events with an area of zero value were conservatively disregarded in determining the average area). Second, the tornado frequency (**n**) was calculated by dividing the total count of tornado events in each category including those with zero area by the measured duration (54 years). Third, the point probability of a tornado impacting a square mile (site area estimated as 1 mi^2.) is calculated by taking the product of the average impacted area and the average tornado frequency and dividing by the total area of the surrounding counties (**A**). This computation assumes that tornadoes with a zero path length have an area equal to the average area of the category.	1.17E-05
	EF1 Tornado	Y		1.26E-05
	EF2 Tornado	Y		8.38E-05
	EF3 Tornado	Y		7.34E-05
	EF4 Tornado	Y		3.91E-05
	EF5 Tornado	Y		No Recorded Events
	Cat. 1 Hurricane	Y	Historical data for tropical weather is archived by the National Coastal Services Center and covers from 1851 to 2006. Subsection 2.3.1.3.3 summarizes the frequencies of occurrence of the various categories of hurricanes that have tracked within approximately 100 nautical miles of the VCSNS site. This data was used to analyze the event frequency of hurricane activity (in an extremely conservative manner since the site is located greater than 100 miles inland from the coast) traveling in the vicinity of the VCSNS site. The storms were sorted to remove duplicate values. The event frequency is determined by dividing the number of occurrences of tropical weather by the measured duration (155 years).	4.52E-02
	Cat. 2 Hurricane	Y		1.94E-02
	Cat. 3 Hurricane	Y		6.45E-03
	Cat. 4 Hurricane	Y		6.45E-03
	Cat. 5 Hurricane	Y		No Recorded Events
	Extratropical Cyclones	Y	The “Extratropical Cyclone” subcategory of storms, used in APP-GW-GLR-101, was assigned an initiating event frequency of 3E-02 events per year. However, if an evaluation indicates a CDF less than 1.0E-08 events per year, then no detailed PRA is necessary. Initially, a 25 mile radius around the site was evaluated for extratropical storms. 5 storms were observed. When obtaining weather data for a radius of 100 nautical miles, the observed number of storms is 31. Utilizing the 31 events, the incident event frequency (IEF) increases from 3.22E-02 to 2.0E-01. The CCDP used in APP-GW-GLR-101 for the Case 1 Loss of Offsite Power (LOOP) scenario is 9.81E-09. Even with the increased event frequency, the core damage frequency (CDF) remains less than 1E-08 at 1.9E-09. Therefore, no detailed PRA is necessary. As documented in Table 2.0-201, the VCSNS site characteristic tornado wind loadings are equal to the AP1000 DCD site characteristic tornado wind loadings. The VCSNS site characteristic operating basis wind speed (102 mph) is below the DCD site characteristic operating basis wind speed of 145 mph. Therefore, it is concluded that the safety features of the AP1000 are unaffected and the resultant CDFs given in APP-GW-GLR-101 Table 3.0-1 for these events are applicable to VCSNS Units 2 and 3.	2.0E-01

Table 19.58-201 (Sheet 2 of 3)
External Event Frequencies for VCSNS Units 2 and 3

Category	Event	Applicable to site? (Y/N)[a]	Explanation of Applicability Evaluation	Event Frequency
External Flood	External Flood	N	As discussed in Subsections 2.4.1.1 and 2.4.10 the site grade of 400 ft NAVD88 (which corresponds to DCD grade elevation 100 ft.) is about 150 ft above the Broad River flood plain. Additionally, as discussed in Subsections 2.4.2.2 and 2.4.2.3, the maximum water level in the power block area due to any local PMP flood event is below the entrance and openings to safety related structures. Therefore, no external flood protection measures are required for VCSNS Units 2 and 3. Subsections 2.4.3 and 2.4.4 also discuss other natural and man-made (dams) flooding scenarios which further reinforce the VCSNS site is not susceptible to any external floods which would adversely impact safe operation of VCSNS Units 2 and 3.	N/A
Transportation and Nearby Facility Accidents	Aviation (commercial/ general/military)	N	Subsections 2.2.2.7 and 2.2.2.7.6 provide the detailed evaluation that confirms the probability of an aviation accident is less than 10E-07 and therefor requires no further evaluation. Therefore, it is concluded that the PRA remains applicable.	N/A
	Marine (ship/barge)	N	As discussed in Subsection 2.2.2.4, since neither the Broad River, Parr Reservoir, nor the Monticello Reservoir is used as commercial transport waterways, the potential safety effect to the site is regarded as being insignificant. Thus, no further analysis is necessary.	N/A
	Pipeline (gas/oil)	N	As stated in Subsection 2.2.2.3.1, the only pipeline in the general vicinity of the site is a 12 inch natural gas buried pipeline located greater than a mile from VCSNS Units 2 and 3. This pipeline is bounded by the evaluation performed in APP-QW-GLR-101, and therefore no further evaluation is necessary.	N/A
	Railroad	N	Potential explosion and flammable vapor cloud hazards to VCNS Units 2 and 3 resulting from railroad accidents are discussed in FSAR Subsection 2.2.3.1.1.3. The results of this evaluation concluded that no adverse impacts to VCSNS Units 2 and 3 are expected. Based upon the quantitative consequence evaluations performed, no risk-important events related to rail transportation have been identified for VCSNS Units 2 and 3. Therefore, the potential for hazards from these sources are minimal and will not adversely affect safe operation of VCSNS Units 2 and 3.	N/A
	Truck	N	Potential hazards resulting from trucks were discussed in Subsection 2.2.2.5. The evaluation that was performed to address the explosion of a tanker truck on site as it filled on-site storage tanks was considered bounding for any highway accident and therefore no additional evaluation was required. The evaluations to address these onsite truck hazards are described in Subsections 2.2.3.1.1.1 and 2.2.3.1.2.1, and the results of these evaluations concluded that the hazards do not result in any significant damage to the plant.	N/A

Table 19.58-201 (Sheet 3 of 3)
External Event Frequencies for VCSNS Units 2 and 3

Category	Event	Applicable to site? (Y/N)[a]	Explanation of Applicability Evaluation	Event Frequency
Other Events	A number of external events beyond those evaluated in Section 19.58 were evaluated for the VCSNS site. These events are discussed below.		Based on the evaluations below, these events do not pose a credible threat to the safe operation of VCSNS Units 2 and 3. Thus, these events are not considered to be risk-important and it can be concluded that the VCSNS Units 2 and 3 site is within the bounds of the Floods and Other External Events analysis documented in Section 19.58.	
	Additional events at nearby facilities	N	Based on the discussions in Subsections 2.2.3.1.1, 2.2.3.1.2 and 2.2.3.1.3, the effects of explosions, flammable vapor clouds and toxic chemicals at the Parr Combustion Turbines and VCSNS Unit 1 were evaluated and determined to meet the safe distance requirements and toxicity limits of Regulatory Guides 1.91 and 1.78. Therefore, because no risk significant consequences were identified for these events, the potential safety effect to the site is regarded as being insignificant. Thus, no further analysis is necessary.	N/A
	External fires	N	As stated in Subsection 2.2.3.1.4, for an assumed wildfire in the vegetation surrounding the site, given the low incident heat flux calculated, the long separation distances to safety-related structures, and the various conservatisms assumed in the analysis, a wildfire would not affect the safe operation or shutdown of Units 2 and 3. In addition, as described in Subsection 2.2.2, due to the lack of other facilities with hazardous materials that could create nonflammable gases or chemical bearing clouds as a result of a forest fire located within 5 miles of the site, these clouds are not considered to be a concern. Therefore. no further evaluation is necessary for these external fire events.	N/A

(a) An event is applicable (Y) to the VCSNS site if the initiating event frequency is greater than 1E-07, or if a quantitative consequence evaluation has demonstrated that there are site specific parameters that exceed the parameters used in APP-GW-GLR-101. An event is not applicable (N) to the VCSNS site if the initiating event frequency is less than 1E-07 or if the quantitative consequence evaluation has demonstrated that the event will not adversely impact the safe operation of VCSNS Units 2 and 3.

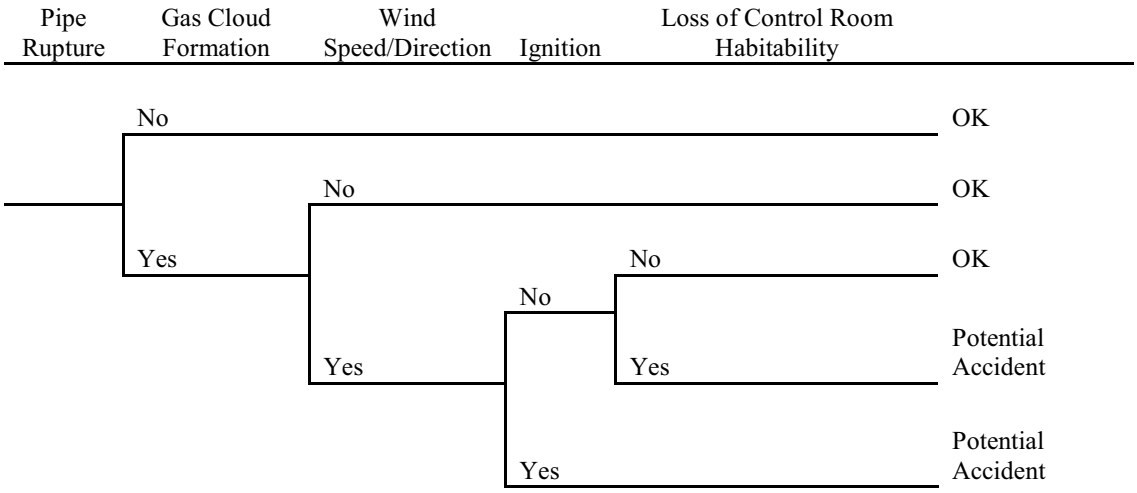

Figure 19.58-1 Pipeline Accident Model

19.59 PRA Results and Insights

19.59.1 Introduction

This chapter summarizes the use of the AP1000 PRA in the design process, PRA results and insights, plant features important to reducing risk, and PRA input to the design certification process.

AP1000 is expected to achieve a higher standard of severe accident safety performance than current operating plants, because both prevention and mitigation of severe accidents have been addressed during the design stage, taking advantage of PRA insights, PRA success criteria analysis, severe accident research, and severe accident analysis. Since PRA considerations have been integrated into the AP1000 design process from the beginning, many of the traditional PRA insights relating to current operating plants are not at issue for the AP1000. The Level 1, Level 2, and Level 3 results show that addressing PRA issues in the design process leads to a low level of risk. The PRA results indicate that the AP1000 design meets the higher expectations and goals for new generation passive pressurized water reactors (PWRs).

The core damage frequency (CDF) and large release frequency (LRF) for at-power internal events (excluding seismic, fire, and flood events) are 2.41E-07 events per reactor-year and 1.95E-08 events per reactor-year, respectively. These frequencies are at least two orders of magnitude less than a typical pressurized water reactor plant currently in operation. This reduction in risk is due to many plant design features, with the dominant reduction coming from highly reliable and redundant passive safety-related systems that impact both at-power and shutdown risks. These passive systems are much less dependent on operator action and support systems than plant systems in current operating plants.

Conservative, bounding fire and flood assessments show the core damage risk from these events is small compared to the core damage risk from at-power and shutdown events.

A synopsis of the insights gained from the PRA about the AP1000 design includes:

- The AP1000 design benefits from the high level of redundancy and diversity of the passive safety-related systems. The passive systems have been shown to be highly reliable; their designs are simple so that a limited number of components are required to function.

- AP1000 is less dependent on nonsafety-related systems than current plants or advanced light water reactor evolutionary plants.

- The nonsafety-related support systems (ac power, component cooling water, service water, and instrument air) have a limited role in the plant risk profile because the passive safety-related systems do not require cooling water or ac power.

- AP1000 is less dependent on human actions than current plants or advanced light water reactor evolutionary plants. Even when no credit is taken for operator actions, the AP1000 meets the NRC safety goal, whereas current plants may not.

- The core damage and large release frequencies are low despite the conservative assumptions made in specifying success criteria for the passive systems. The success criteria have been developed in a more systematic, rigorous manner than typical PRA success criteria. The baseline success criteria are bounding cases for a large number of PRA success sequences. The baseline success sequences, in most cases, have been defined with:

  – Worst (i.e., the most limiting) break size and location for a given initiating event

  - Worst automatic depressurization system (ADS) assumption in the success criterion
  - Worst number of core makeup tanks (CMT) and accumulators
  - Worst containment conditions for in-containment refueling water storage tank (IRWST) gravity injection

  Many less-limiting sequences are therefore represented by a baseline success criterion.

- Single system or component failures are not overly important due to the redundancy and diversity of safety-related systems in the design. For example, the following lines of defense are available for reactor coolant system (RCS) makeup:
  - Chemical and volume control system (CVS)
  - Core makeup tanks
  - Partial automatic depressurization system in combination with normal residual heat removal
  - Full automatic depressurization system with accumulators and in-containment refueling water storage tank
  - Full automatic depressurization system with core makeup tanks and in-containment refueling water storage tank
- Typical current PRA dominant initiating events are significantly less important for the AP1000. For example, the reactor coolant pump (RCP) seal loss-of-coolant accident (LOCA) event has been eliminated as a core damage initiator since AP1000 uses sealless reactor coolant pumps. Another example is the loss of offsite power (LOOP) event. The station blackout and loss of offsite power event is a minor contributor to AP1000 since the passive safety-related systems do not require the support of ac power.
- Passive safety-related systems are available in all shutdown modes. Planned maintenance of passive features is only performed during shutdown modes when that feature is not risk important. In addition, planned maintenance of nonsafety-related defense-in-depth features used during shutdown is performed at power.
- The AP1000 passive containment cooling design is highly robust. Air cooling alone is significant and may prevent containment failure, although the design has other lines of defense for containment cooling such as fan coolers and passive containment cooling water.
- The potential for containment isolation and containment bypass is lessened by having fewer penetrations to allow fission product release. In addition, normally open and risk important penetrations are fail-closed, thus eliminating the dependence on instrumentation and control (I&C) and batteries.
- The reactor vessel lower head has no vessel penetrations, thus eliminating penetration failure as a potential vessel failure mode. Preventing the relocation of molten core debris to the containment eliminates the occurrence of several severe accident phenomena, such as ex-vessel fuel-coolant interactions and core-concrete interaction, which may threaten the containment integrity. Therefore, AP1000, through the prevention of core debris relocation to the containment, significantly reduces the likelihood of containment failure.

- The potential for the spreading of fires and floods to safety-related equipment is significantly reduced by the AP1000 layout.

19.59.2 Use of PRA in the Design Process

The AP1000 design has evolved over a period of years, including the work done for the AP600 design. PRA techniques have been used since the beginning in an iterative process to optimize the AP600/AP1000 with respect to public safety. Each of these iterations has included:

- Development of a PRA model
- Use of the model to identify weaknesses
- Quantification of PRA benefits of alternate designs and operational strategies
- Adoption of selected design and operational improvements.

The scope and detail of the PRA model has increased from the early studies as the plant design has matured. This iterative design process has resulted in a number of design and operational improvements.

19.59.3 Core Damage Frequency from Internal Initiating Events at Power

Internal initiating events are transient and accident initiators that are caused by plant system, component, or operator failures. External initiating events, which include internal fire and flooding events and events at shutdown are discussed in other subsections.

The AP1000 mean plant core damage frequency for internal initiating events at power is calculated to be 2.41E-07 events per year. Twenty-six separate initiating event categories were defined to accurately represent the AP1000 design. Of these event categories, 11 are loss-of-coolant accidents, 12 are transients, and 3 are anticipated transients without scram precursors (initiating events that result in an anticipated transient without scram sequence as a result of failure to trip the reactor). Initiating event categories unique to the AP1000 design have been defined and evaluated, including safety injection line breaks, core makeup tank line breaks, and passive residual heat removal heat exchanger (HX) tube ruptures. The resulting core damage frequency is very small; a value of 2.41E-07 means that only one core damage event is expected in 4 million plant-years of operation. This core damage frequency value is two orders of magnitude (i.e., 100 times) smaller than corresponding values typically calculated for current pressurized water reactors.

The contribution of initiating events to the total plant core damage frequency is summarized in Table 19.59-1. Figure 19.59-1 illustrates the relative contributions to core damage frequency from the various at-power initiating events. Table 19.59-2 shows the conditional core damage probability of the initiating events. The conditional core damage probability listed in Table 19.59-2 is the ratio of the core damage frequency contribution for an initiating event divided by the initiating event frequency.

Seven initiating events, including 6 loss-of-coolant accidents, and steam generator tube rupture (SGTR), make up approximately 92 percent of the total at-power plant core damage frequency. The remaining initiating events contribute a total of approximately 8 percent to the core damage frequency from internal events. The dominant initiating events are:

- Safety injection (DVI) line break
- Large loss-of-coolant accident
- Spurious ADS actuation
- Small loss-of-coolant accident
- Medium loss-of-coolant accident
- Reactor vessel rupture
- Steam generator tube rupture

Within this group of events, each of the first three contributes more than 10 percent to the total core damage frequency. These three events account for approximately 70 percent of the total core damage frequency. Small LOCA, medium LOCA, and reactor vessel rupture events contribute 7 percent, 6 percent and 4 percent, respectively.

The results show a very low core damage frequency dominated by rare events (initiating events that are not expected to occur during the lifetime of a plant). This indicates that the AP1000 design is robust with respect to its ability to withstand challenges from more frequent events (e.g., transients) and that adequate protection against the more severe events is provided through the defense-in-depth features.

Information regarding loss-of-coolant accident categories defined for the AP1000 PRA was presented in the discussion of PRA success criteria. For the PRA, the various loss-of-coolant accident categories have been defined based on which plant features are required to mitigate the events. As a result, the PRA and loss-of-coolant accident size definitions are not identical to the loss of coolant accident size definitions used in the Chapter 15, Accident Analyses included in the *AP1000 Design Control Document* (DCD). The following listing shows how the PRA and DCD break sizes are related and identifies the PRA size criteria:

- Chapter 15 break size definitions are large (break size greater than 1 $ft.^2$) or small (break size less than 1 $ft.^2$).

- PRA break sizes are defined as follows:

  – Large breaks are those with an equivalent inside diameter of approximately 9 in. or larger. Reactor vessel rupture is included in this category. The automatic depressurization system is not required for in-containment refueling water storage tank injection for large breaks. (For large breaks that are slightly larger than a medium break, there is a potential effect of containment isolation upon in-containment refueling water storage tank injection. The success criteria include automatic depressurization system in these cases.)

  – Medium breaks are those with an equivalent inside diameter between approximately 2 in. and 9 in. Core makeup tank line breaks and safety injection line breaks are included in this category (but are evaluated separately). Operation of automatic depressurization system stages 1, 2, or 3 (or, alternatively, passive residual heat removal) is not required to satisfy the automatic depressurization system stage 4 automatic actuation pressure interlock, but is required to depressurize the reactor coolant system to the normal residual heat removal system operating pressure.

  – Small breaks are those with an equivalent inside diameter between approximately 3/8 in. and 2 in. Steam generator tube rupture and passive residual heat removal heat exchanger tube rupture break sizes fall within this range, but are evaluated as separate events based on differing initial plant response. Small breaks are larger than those for which the chemical and volume control system can maintain reactor coolant system water level, but not large enough to allow automatic actuation of automatic depressurization system stage 4 without operation of either automatic depressurization system stages 1, 2, or 3 or passive residual heat removal.

  – Coolant losses smaller than those resulting from small breaks are defined as reactor coolant system leaks. Operation of one chemical and volume control system makeup pump can maintain reactor coolant system water inventory for reactor coolant system leaks.

19.59.3.1 Dominant Core Damage Sequences

A total of 791 potential core damage event sequences for internal initiating events at power are modeled in the AP1000 PRA. These core damage sequences are the combinations of initiating event occurrences and subsequent successes and failures of plant systems and operator actions that result in core damage. Of these 791 event sequences, 190 result in frequencies ranging from 7-08 to 1E-15 events per year. The remaining sequences do not produce any cutsets representing them in the top 19,000 cutsets; that is, their core damage frequencies are not significant relative to the core damage frequencies for the other sequences.

- The 10 sequences with the highest core damage frequencies together contribute 79 percent of the total (approximately 1.92E-07 events per year).
- The top 19 sequences contribute 90 percent of the total (approximately 2.18E-07 events per year).
- The top 58 sequences contribute 99 percent of the total (approximately 2.39E-07 events per year).
- The top 100 sequences contribute 99.9 percent of the total (approximately 2.41E-07 events per year).

The 19 dominant sequences are given in Table 19.59-3.

Moreover, each core damage sequence is composed of component-level cutsets, with a total of approximately 19,000 cutsets included in the baseline internal initiating events at-power analysis (100 percent of 2.41E-07 events per year core damage frequency). A cutset is a combination of initiating event occurrence and the component or operator failures that constitute the various system-level failures that lead to core damage.

- The 100 highest-frequency cutsets together contribute approximately 86 percent of the total core damage frequency (approximately 2.1E-07 events per year).
- The top 200 cutsets contribute approximately 91 percent (2.2E-07 events per year). These cutsets are reported in Section 36.
- The top 500 cutsets contribute approximately 95 percent (2.3E-07 events per year).
- The top 1,000 cutsets contribute approximately 97 percent (2.35E-07 events per year).
- The top 2,000 cutsets contribute approximately 98 percent (2.37E-07 events per year).

The top 10 accident sequences contribute 79 percent of the core damage frequency from internal initiating events at power. These sequences are listed in Table 19.59-3. The top 25 cutsets for these sequences are given in Tables 19.59-4 through 19.59-13.

The first four dominant accident sequences make up 63 percent of the core damage frequency. These sequences are:

1. Safety injection line break event occurs, which is postulated to lead to spilling of one train of core makeup tank, in-containment refueling water storage tank, and recirculation flows. The reactor is tripped. The second core makeup tank successfully injects, and the automatic depressurization system is successfully actuated. Thus, the reactor coolant system pressure is low. However, the remaining in-containment refueling water storage tank line fails to inject;

core damage occurs with low reactor coolant system pressure, leading to a postulated 3BE end state. The sequence frequency is 6.9E-08 per year, contributing 29 percent to the plant core damage frequency.

2. Large loss-of-coolant accident event occurs, and the reactor is tripped or is rendered subcritical because of voids in the reactor coolant system. Reactor coolant system rapidly depressurizes but one of the accumulators does not inject water into the RCS. Core damage with low reactor coolant system pressure, leading to the 3BR end state is postulated. The sequence frequency is 4.3E-08 per year, contributing 18 percent to the plant core damage frequency.

3. Spurious ADS actuation event occurs, and the reactor is tripped or is rendered subcritical because of voids in the reactor coolant system. Reactor coolant system rapidly depressurizes and at least one of the two accumulators injects, making up the RCS water loss in the short time frame. The CMT injection or ADS actuation fails. Thus, automatic IRWST injection is not actuated. Core damage with medium reactor coolant system pressure, leading to the 3D end state is postulated. The sequence frequency is 2.1E-08 per year, contributing 9 percent to the plant core damage frequency.

4. Safety injection line break event occurs, which is postulated to lead to spilling of one train of core makeup tank, in-containment refueling water storage tank, and recirculation flows. The reactor is tripped. The second core makeup tank successfully injects, but the automatic depressurization system actuation fails. Core damage is postulated with a medium reactor coolant system pressure, leading to a 3D end state. The sequence frequency is 2.0E-08 per year, contributing 8 percent to the plant core damage frequency.

The fifth dominant sequence, with 4 percent contribution to plant core damage frequency, is a reactor vessel rupture event. By the definition of this event, core damage is postulated to occur. The end state is 3C.

19.59.3.2 Component Importances for At-Power Core Damage Frequency

Chapter 50 presents tables of the relative importances of all basic events appearing in the cutsets for the baseline core damage quantification. These tables indicate risk decrease and risk increase. Risk decrease is the factor by which the core damage frequency would decrease if the failure probability for a given basic event is set to 0.0; it is a useful measure of the benefit that might be obtained as a result of improved component maintenance or testing, better procedures, or operator training. Risk increase is the factor by which the core damage frequency would increase if the failure probability for a given basic event is set to 1.0; it is a useful measure of which components or actions would most adversely affect the core damage frequency if actual operating practices resulted in higher failure probabilities than assumed in the PRA.

The risk decrease results (as discussed in detail in Chapter 50) show that only six components have a risk reduction worth (RRW) of greater than or equal to 1.05. The in-containment refueling water storage tank discharge line strainer plugging has the highest RRW value, followed by common cause failure (CCF) of various components as shown in the following table.

IWA-PLUG	1.27	IRWST discharge Line “A” strainer plugged
ADX-EV-SA2	1.11	CCF of 2 squib valves to operate
REX-FL-GP	1.08	CCF plugging of both recirculation lines due to sump screens
ADX-EV-SA	1.05	CCF of 4th stage ADS squib valves to operate
IWX-CV-AO	1.05	CCF of 4 gravity injection check valves
IWX-EV-SA	1.05	CCF of 4 gravity injection & 2 recirculation squib valves

The remaining components each have a risk reduction worth of 1.04 or less. The contribution to the core damage frequency from unscheduled maintenance is also small. These results indicate that there are no components for which an improvement in design, test, or maintenance (i.e., a change resulting in a significant reduction of the component failure rate) would have a significant impact on the core damage frequency.

Excluding common cause failures, the risk increase results indicate that the accumulator system components have high risk achievement worth (RAW) values, followed by one Non-Class 1E dc and uninterruptible power supply system (EDS) bus, various Class 1E dc and uninterruptible power supply system (IDS) components and CMT components. Other single-component failures have significantly lower risk increase values, corresponding to a factor of six or lower increase in core damage frequency given an assumption of total unreliability for these components.

19.59.3.3 System Importances for At-Power Core Damage

System importances for plant core damage frequency from internal initiating events at power are presented in Chapter 50. They are obtained by setting the failure probabilities for the affected system components to 1.0 in the baseline cutsets and recalculating the core damage frequency.

The results of the sensitivity analyses show that the protection and safety monitoring system and the Class 1E dc power system are most important in maintaining a low core damage frequency. The risk-important systems are safety-related systems. The safety-related systems are all of high or medium importance. The nonsafety-related systems are only marginally important to the plant core damage frequency.

A sensitivity analysis is made for the unavailability of all five of the standby non-safety related systems (chemical and volume control system (CVS), startup feedwater system (SFW), normal residual heat removal system (RNS), diverse actuation system (DAS), diesel generators (DGs)). The plant CDF obtained is 7.40E-6, which is a factor of 31 increase over the base case. This sensitivity analysis shows that the plant CDF is somewhat sensitive to the simultaneous failure of the five systems listed above.

19.59.3.4 System Failure Probabilities for At-Power Core Damage

Some selected system failure probabilities for typical success criteria used in the at-power PRA are listed in Table 19.59-14. A system may have different failure probabilities based on the success criteria assigned. For a key safety-related system such as the automatic depressurization system, this is especially pronounced; the automatic depressurization system has many success criteria and corresponding failure probabilities that range over a factor of 100. The values in the table are representative of the various cases.

As can be seen from the system unavailabilities listed in Table 19.59-14, the highest unavailabilities (i.e., 10^{-2} to 10^{-3}, indicating lower reliability) are associated with nonsafety-related systems or

functions. The lower unavailabilities (i.e., 10^{-4} to 10^{-6}, indicating higher reliability) are associated with safety-related systems.

19.59.3.5 Common Cause Failure Importances for At-Power Core Damage

The common cause importance results are presented in Chapter 50. The risk increase importances for common cause failures of the following sets of components show that these are also of potential significance to the current low level of core damage frequency from internal events: common cause failure of software in the protection and safety monitoring system and plant control system, logic board failures of the protection and safety monitoring system; failures of transmitters used in the protection and safety monitoring system; failures of reactor trip breakers; plugging of containment sump recirculation screens; failures of in-containment refueling water storage tank gravity injection line check valves and squib valves; plugging of strainers in the in-containment refueling water storage tank; failures of fourth-stage automatic depressurization system squib valves and failures of output cards for the protection and safety monitoring system. These and similar common cause failures are of potential significance in maintaining the current level of low plant core damage frequency.

The leading risk decrease common cause failures of hardware are associated with ADS fourth stage squib valves, gravity injection and recirculation line components, and I&C components and sensors.

19.59.3.6 Human Error Importances for At-Power Core Damage

In the PRA, credit is taken for various tasks to be performed in the control room by the trained operators. These tasks are rule-based and proceduralized. Although these tasks are usually termed operator actions, the tasks almost always refer to the completion of a well-defined mission by trained operators following procedures. Further, not every individual or group error during a mission necessarily fails the mission, since procedural recovery is built into the emergency procedures. Moreover, a very strong diversity is introduced through monitoring of the emergency procedure status trees by a shift technical advisor. These considerations are factored into the PRA evaluation of human errors.

The risk decrease results for operator actions (discussed in Chapter 50) show that there are 10 human actions with importances greater than 1 percent. There are no actions for which the internal initiating events at-power core damage frequency contribution would decrease by more than 3 percent if it were assumed that the operators always were successful. This indicates that there would be no significant benefit from additional refinement of the actions modeled, or from special emphasis on operator training in these actions (versus other emergency actions).

The risk increase results show that there are only 7 operator actions with importance greater than 100 percent; i.e., these are the only modeled operator actions whose guaranteed failure would result in a core damage increase greater than the base case core damage frequency. The most important action in this ranking (operator fails to diagnose a steam generator tube rupture event) has a risk achievement worth of 6.3. It is followed by manual actuation of ADS with a RAW value of 4.25. These results indicate that the plant design is not overly sensitive to failure of operator actions and the core damage models do not take undue credit for operator response.

A sensitivity analysis was performed in which the failure probabilities for the 30 operator actions are set to 0.0 (perfect operator). The resulting core damage frequency is only slightly smaller. This indicates that perfection in human error probabilities is not risk important at the level of plant risk obtained by the base case; there is no significant benefit to be gained by improving operator response beyond the assumptions made in the PRA.

Another sensitivity analysis was performed in which the failure probabilities for the 30 human error probabilities and also for indication failure (protection and safety monitoring system, plant control system, or diverse actuation system originated) are set to 1.0 (failure). The result of the sensitivity analysis shows that the core damage frequency increased to 1.4E-05 events per year. The resulting core damage frequency with no credit for operator actions is still low (about one event in 71,000 reactor-years), on the order of core damage frequency for current plants with credit for operators. This means that, in general, operator actions are important in maintaining a very low plant core damage frequency for internal events at power but are not essential to establishing the acceptability of plant risk. The presence of trained operators will help ensure that the very low core damage frequency prediction is valid. This finding demonstrates a significantly lower dependence on human actions than exists for current plants. The AP1000 meets the core damage frequency safety goal without human action, whereas current plants typically do not.

19.59.3.7 Accident Class Importances

The accident classes (also referred to as end states) are described in Chapter 44, and the contribution of accident classes to plant core damage frequency is presented in the same chapter. Two low-pressure reactor coolant system core damage end states, 3BE and 3BL, contribute 43 percent to the total core damage frequency. Together with 3BR and 3D, full or partially depressurized core damage states make up 87 percent of the core damage. In these end states, the probability of retaining containment integrity is very likely. Thus, severe release potential for these end states is low.

19.59.3.8 Sensitivity Analyses Summary for At-Power Core Damage

Thirty-six importance and sensitivity analyses were performed on the core damage model for internal initiating events at power. These cases and results are discussed in Chapter 50.

The analyses were chosen to address the following issues:

- Importances of individual basic events and their effect on plant core damage frequency
- Importances of safety-related and nonsafety-related systems in maintaining a low plant core damage frequency
- Importances of containment safeguards systems in maintaining a low large-release frequency
- Effect of human reliabilities as a group on plant core damage frequency
- Other specific issues such as passive system check valve reliability, etc.

The sensitivity analyses results are discussed in Chapter 50. They show that:

- If no credit is taken for operator actions, the plant core damage frequency is 1.4E-05 events per year. This compares well with core damage frequencies for existing plants where credit is taken for operator actions.
- The most important systems for core damage prevention are the protection and safety monitoring system, Class 1E dc power, automatic depressurization system, in-containment refueling water storage tank recirculation, core makeup tanks, and accumulators. None of the nonsafety-related systems have high system importance.

- There are no operator actions that would provide a significant risk decrease if they were made to be more reliable. There are only eight operator actions that would increase the core damage frequency by more than the base case if they were assumed to fail. The most important of these is the failure to diagnose a steam generator tube rupture event.

- If the reliability of all check valves is assumed to be a factor of 10 worse, the total plant core damage frequency would only increase to 8.8E-7 events per year. This shows that the passive safety-related systems that depend on check valve opening will perform acceptably, even if pessimistic check valve reliabilities are assumed.

- The plant core damage frequency is not affected by the diesel generator mission time duration. This is due to the AP1000 design's passive features, which do not require ac power for operation.

- The common cause failure basic events, particularly those associated with safety-related systems, are important individually, and also as a group for plant core damage frequency. This is expected for a plant with highly redundant safety-related systems, for which individual component random failure contributions are of reduced significance.

19.59.3.9 Summary of Important Level 1 At-Power Results

The results of the PRA show that the following AP1000 design features provide the ability to respond to internal initiating events and contribute to a very low core damage frequency:

- The manual feed and bleed operation in current pressurized water reactors is replaced by the automatic depressurization system and core makeup tank/in-containment refueling water storage tank injection. This increases the success probability for feed and bleed and helps reduce core damage contribution from transients with failure of decay heat removal.

- The switchover-to-recirculation operation in current pressurized water reactors is replaced with automatic recirculation of sump water into the reactor coolant system loops by natural circulation.

- The diverse actuation system provides diverse backup for automatic or manual actuation of safety-related systems, increasing the system reliability for the passive residual heat removal, core makeup tank, and automatic depressurization systems.

- The AP1000 plant design is based on a defense-in-depth concept. There are several means (both active and passive) of providing reactor coolant system makeup following a loss-of-coolant accident, at both high and low pressures (i.e., chemical and volume control system pumps, core makeup tanks, accumulators, in-containment refueling water storage tank gravity injection, and normal residual heat removal system). Similarly, there are diverse means of core cooling, including the passive residual heat removal and normal residual heat removal systems.

- The ability to depressurize and establish feed and bleed heat removal via the automatic depressurization system and core makeup tanks without operator action provides an additional reliable means of core cooling and inventory control.

- The diversity and redundancy in the design of the automatic depressurization system provide a highly reliable system for depressurizing to allow injection and core cooling by the various sources of water.

- The design of the reactor coolant pumps eliminates the dependence on component cooling water and accompanying reactor coolant pump seal loss-of-coolant accident core damage contribution, which is typically significant for current plants.

- The design of the safety-related heat removal systems eliminates the dependence on service water and ac power during accidents; such dependencies can be significant contributors to core damage for current plants.

Core Damage Contribution from Important Initiating Events

Loss-of-Coolant Events. The at-power core damage results are dominated (top 8 dominant contributors with 93 percent) by various loss-of-coolant events. Thirty-four percent of the contribution is due to the safety injection line break, which is a special initiator, in that its occurrence partially defeats features incorporated into the plant to respond to losses of primary coolant. Even though the safety injection line break core damage frequency dominates the results, its value is very small (one event in 10 million reactor years), with little credit for nonsafety-related systems.

The conditional probability of core damage, given the occurrence of a “conventional” loss-of-coolant accident, is generally in the range of about 1E-03 to 1E-05 (with the exception of reactor vessel rupture and interfacing systems loss-of-coolant accident, for which core damage is assumed). These events have frequencies of about 1E-08 per year to 5E-04 per year. This indicates that the various features of the AP1000 would act to prevent core damage from all but between 1 in 1000 and 1 in 100,000 loss-of-coolant accidents. Since loss-of-coolant accidents are relatively rare events, this is a significant level of protection.

Anticipated Transients Without Scram. Anticipated transients without scram (ATWS) sequences contribute about 2 percent of the at-power core damage frequency, in part due to modeling simplifications whereby, in the absence of specific modeling and success criteria, it has been assumed that core damage will occur given certain combinations of failures. With additional analysis and modeling detail, it is expected that the anticipated transient without scram core damage frequency could be shown to be lower.

Transients. The contribution of transients to core damage frequency is about 5 percent of the at-power core damage frequency (total contribution from all transient initiators with reactor trip is 1 event in 100 million reactor years). This is the result of the defense-in-depth features of the AP1000 design, whereby core cooling following transients is available from main feedwater, startup feedwater, and passive residual heat removal, as well as from feed and bleed, using diverse and redundant sources of makeup (core makeup tanks, accumulators, in-containment refueling water storage tank, normal residual heat removal system), and of depressurization (four stages of automatic depressurization system).

Loss of Offsite Power. The loss of offsite power core damage frequency contribution at power is insignificant (less than 1 percent). AP1000 passive systems require only dc power provided by the long-term batteries for actuation to provide cooling. In addition, the passive residual heat removal heat exchanger is backed up by bleed and feed cooling using the automatic depressurization system and core makeup tanks or in-containment refueling water storage tank gravity injection, which also require only dc power provided by long-term batteries. With onsite power available, startup feedwater provides an additional means of decay heat removal.

Steam Generator Tube Rupture. The steam generator tube rupture event contributes about 3 percent of the at-power core damage frequency. Compared to operating pressurized water reactors this is a very low contribution. Among the reasons for the small steam generator tube rupture core damage contribution are the following:

- The first line of defense is the startup feedwater system and chemical and volume control system

- A reliable safety-related passive residual heat removal system coupled with the core makeup tank subsystem, which provides automatic protection

- A third line of defense using automatic depressurization system and in-containment refueling water storage tank for accident mitigation should the above-mentioned systems fail.

Further, the automatic depressurization system provides a more reliable alternate decay heat removal path through feed and bleed than the high-pressure manual feed and bleed cooling of current operating plants.

Finally, the large capacity of the in-containment refueling water storage tank increases the long-term recovery probability for unisolable steam generator leaks that bypass containment, by preventing depletion of borated water and core damage.

Dependence on Operator Action

The results of the PRA show that the AP1000 is significantly less dependent on operator action to reduce plant risk to acceptable levels than are current plants. This was shown through the sensitivity analyses and the operator action contributions from both the risk decrease and risk increase measures. Almost all operator actions credited in this PRA are performed in the control room; there are very few local actions outside the control room. Further, the human actions modeled in the AP1000 PRA are generally simpler than those for current plants. Thus, the tasks for AP1000 operators are easier and less likely to fail. If it were assumed that the operators never perform any actions credited in the PRA, the internal events core damage frequency would still be lower than the result obtained for many current pressurized water reactors including operator actions.

Dominant System/Component Failure Contributors

Contribution to Core Damage Frequency. Component-related contributors to core damage frequency from internal events at power are dominated by common cause failures. The single component failures are limited to strainer or tank failures, and accumulator check valve failures.

Dependence on Component Reliability. Most of the component failures with relatively high risk increase worth are common cause failures. This is an indication of the high degree of built-in redundancy and diversity of AP1000 safety-related systems, particularly in view of the low baseline core damage frequency. The results demonstrate a well-balanced design, for which diversity eliminates the strong dependence on active valves or on the specific type of valve.

Sensitivity to Numerical Values and Modeling Assumptions. The core damage results are not strongly sensitive to increases in the failure probabilities of basic events. Check valves are relatively important; if the check valve failure probability is increased by a factor of 10, the core damage frequency increases by a factor of 4. This increase is not large, and the core damage goal of 1E-05 is comfortably met. Finally, the modeling assumptions in system and accident sequence success criteria are bounding (e.g., conservative) whenever a range of conditions are represented by a single selected condition or success criterion. Since the modeling assumptions already represent an upper bound type estimate, there are no significant contributions to core damage due to conditions outside the assumed ranges that are unaccounted for. As an example, the automatic depressurization system success criteria for loss-of-coolant accident events are selected to cover the worst conditions (e.g., break size, break location) of the range.

System Reliability and Defense-in-Depth. The results show that the safety-related systems have demonstrated high reliabilities (e.g., failure probability in the range of 1E-05 to 1E-03) due to the

nature of the system designs (passive systems). Moreover, multiple means of success exist for transients and credible loss-of-coolant accident events. This means that a failure of a safety-related system will not lead to core damage, because other diverse systems back up the first one. This defense-in-depth philosophy contributes to the low core damage frequency.

19.59.4 Large Release Frequency for Internal Initiating Events at Power

The results of the Level 2 (containment response) and Level 3 (plant risk) analyses for the internal initiating events at power demonstrate that the AP1000 containment design is robust in its ability to prevent releases following a severe accident and that the risk to the public due to severe accidents for AP1000 is very low. The large release frequency (containment failure frequency) of the AP1000 can be divided into two types of failures: 1) initially failed containment, in which the integrity of the containment is either failed due to the initiating event or never achieved from the beginning of the accident; and 2) containment failure induced by high-energy severe accident phenomena. The total of these failures is the overall large release frequency. The following summarizes important results of the containment event tree quantification with respect to large release frequency.

The overall release frequency for AP1000 is 1.95E-08 events per year. This is approximately 8 percent of the core damage frequency for internal initiating events at power. The ability of the containment to prevent releases (i.e., the containment effectiveness) is 92 percent.

The Level 3 analysis shows that the resulting risk to the population is small and well within the established goals.

19.59.4.1 Dominant Large Release Frequency Sequences

The large release frequency is dominated by release categories BP (bypass), with a 54-percent contribution and CFE (early containment failure) with a contribution of 38 percent. The total frequency of these two categories is 1.8E-08 events per year. These two categories make up 92 percent of the plant large release frequency, followed by 7.0 percent contribution from containment isolation failure category. Contributions of the late containment failure (CFL) and intermediate containment failure (CFI) release categories to large release frequency are negligible.

The early containment failures are caused by sump flooding, vessel failure, and core reflooding failure plus containment overtemperature failure due to diffusion flame.

The dominant accident class in the large release frequency is the Class 6 with a 21-percent contribution. This class represents sequences in which steam generator tube rupture or interfacing LOCA events occur. It is followed by accident class 3A, with a 21 percent contribution. 3A contains core damage events with high RCS pressure and ATWS events.

The dominant large release frequency sequences are shown below. These sequences make up 98 percent of the large release frequency. Two containment bypass sequences from 3A and 6 accident classes contribute 21 percent and 19 percent, followed by 2 early containment failures from 3BE and 3D accident sequences with 14 and 11 percent contributions. These four sequences add up to 65 percent of the plant LRF.

Dominant Containment Event Tree (CET) Sequences					
CET SEQ	**REL CAT**	**PDS**	**FREQ**	**%**	**SEQUENCE DESCRIPTION**
23	BP	3A	4.08E-09	20.9%	Containment Bypass
23	BP	6	3.78E-09	19.4%	Containment Bypass
21	CFE	2E	2.67E-09	13.7%	Sump Flooding Fails
21	CFE	3D	2.05E-09	10.5%	Sump Flooding Fails
23	BP	1A	2.04E-09	10.5%	Containment Bypass
10	CFE	3C	9.97E-10	5.1%	Vessel Failure
12	CFE	3D	9.71E-10	5.0%	Core Reflooding Fails; Diffusion Flame
23	BP	1P	6.05E-10	3.1%	Containment Bypass
22	CI	2L	5.83E-10	3.0%	Containment Isolation Fails
6	CFE	2E	4.75E-10	2.4%	Hydrogen Igniters Fail; Early deflagration to detonation transition (DDT)
22	CI	3D	3.62E-10	1.9%	Containment Isolation Fails
21	CFE	6	1.86E-10	1.0%	Sump Flooding Fails
4	CFI	2E	1.82E-10	0.9%	Hydrogen Igniters fail; Intermediate DDT

19.59.4.2 Summary of Important Level 2 At-Power Results

The results of the PRA show that the following AP1000 design features provide the ability to respond to various severe accidents and contribute to a very small release frequency and a small release of radioactive material to the environment.

- The capability to flood the reactor cavity prevents the failure of the reactor vessel given a severe accident without water in the cavity. The vessel and its insulation are designed so that the water in the cavity is able to cool the vessel and prevent it from failing (in-vessel retention - IVR). By maintaining the vessel integrity, the core debris in the vessel eliminates the potential of a large release due to ex-vessel phenomena and its potential to fail the containment.

- The capability to depressurize the reactor coolant system in a high-pressure transient mitigates the consequences of a high-pressure severe accident. Such accidents have a large potential to fail the reactor coolant system pressure boundary vessel, piping, or steam generator tubes, and such a failure is assumed without further analysis if the reactor coolant system remains at high pressure. A high-pressure failure of the reactor coolant system pressure boundary is assumed to fail or bypass the containment. Thus, the capability to depressurize the reactor coolant system reduces the large release frequency due to high-pressure severe accidents.

- The annular spaces between the steel containment vessel and the shield building help to reduce the release of radioactive materials to the environment by enhancing the deposition of the materials before they exit the containment.

The Level 2 results highlight some insights in the AP1000 design:

- The containment effectiveness for AP1000 is over 90 percent, which provides an order of magnitude decrease from CDF to LRF. Since this result already includes CDF sequences that directly bypass the containment, the containment effectiveness for remaining sequences is actually much better. For example, for 5 (3BE, 3BL, 3BR, 3C, 3D) of the 9 accident classes studied, the containment effectiveness ranges from 90 to 99.8 percent.

- The containment effectiveness is lowest for the 3A accident class where the RCS pressure is high after core damage. The post-core-damage depressurization for this class proves to be ineffective since failure of ADS by common cause failures leading to core damage also causes failure of post-core-damage depressurization.

- Based on detailed analysis, the containment effectiveness for accident class 6, mainly SGTR events, is 56.9 percent, due to those sequences where the RCS pressure is low after the postulated core damage. In such sequences, the fission products can be retained in the pressure vessel, shielded by the water in the faulted steam generator. A sensitivity analysis where all accident class 6 events are assigned to LRF shows that the plant containment effectiveness drops slightly to 89.7 percent (from 91.9 percent). Thus, the LRF results are not very sensitive to the treatment of the SGTR events for LRF.

- A frequency of 1.0E-08/year has been assigned to the vessel failure initiating event (accident class 3C). In 90 percent of these events, the vessel is assumed to undergo failures that will be above the beltline – in which case the molten core could be cooled and containment would not be challenged. In the remaining 10 percent of the cases, the failure is assumed to be below the pressure vessel beltline, whereby the molten core would drop into the containment. In this case, it is conservatively assumed that the containment would fail. A sensitivity analysis is made where by 100 percent of the failures would be below the beltline. The result shows that the containment effectiveness drops to 88.2 percent. This change is not significant, and the assumptions behind the case are very conservative.

- The LRF results are sensitive to failure of hydrogen igniters. If no credit is taken for hydrogen igniters, the containment effectiveness drops to 74 percent.

- However, LRF is not very sensitive to the reliability of hydrogen igniters; if IG reliability is assumed to be degraded (0.1) across the board for all accident classes, the containment effectiveness becomes 90.5 percent, which is an insignificant change from the base case.

- For accident classes 3D and 1AP, if the large hydrogen releases through the IRWST is conservatively assumed to cause containment failure, the containment effectiveness drops to 84.5 percent. The LRF increases to 7.58E-08/year. The increase is about a factor of 4 of the base. Such an increase is significant. This sensitivity analysis addresses the uncertainties in hydrogen mixing model for the case where the hydrogen is released into the IRWST and comes out from the IRWST vents above the operating deck.

- The LRF is dominated (53.9 percent) by containment failures or bypasses due to SGTR, and unmitigated high-RCS-pressure core damage sequences, classified as BP. The remaining containment failures are dominated by an early containment failure due to reactor cavity flooding failure.

- The LRF is not very sensitive to the reliability of PCS. If PCS reliability is assumed to be 0.001 across the board for all accident classes, the LRF becomes 1.97E-08, which is an insignificant change from the base case.

- The LRF is sensitive to the operator action to flood the reactor cavity in a short time following core damage. This operator action has been moved to the beginning of Emergency Response Guideline (ERG) AFR.C-1 to increase its likelihood of success.

- The potential for a release of radioactive materials to the environment is very small. This is largely due to the very small core damage frequency and very small release frequency. The containment design provides enhanced deposition of core materials that could be released in a severe accident, and the passive containment cooling system minimizes the energy available to expel such materials from the containment.

The results of the at-power analyses show the AP1000 design includes redundancy and diversity not found in current plants. The safety-related passive systems do not require ac power or operator actions to actuate, and the plant design is robust in the prevention and mitigation of the consequences of an accident. The AP1000 core damage frequency and large release frequency are much lower than has been seen in current generation plants, despite the many conservatisms built into the PRA models. The assumed dose to the environment given a severe accident and a large release is well within the goals set for that analysis.

19.59.5 Core Damage and Severe Release Frequency from Events at Shutdown

19.59.5.1 Summary of Shutdown Level 1 Results

As shown by the dominant cutsets of the AP600 and AP1000 shutdown models, the risk profiles of these plants for events during shutdown conditions are almost identical. The results indicate that the three events dominating the CDF are loss of component cooling/service water during drained condition, loss of RNS during drained condition, and loss of offsite power during drained condition. The AP1000 and AP600 initiating event core damage contributions are similar for the two plants.

The dominant sequences are described in the subsections that follow. The dominant accident sequences comprise 95.3 percent of the level 1 shutdown PRA core damage frequency. These dominant sequences consist of:

- Loss of component cooling or service water system initiating event during drained condition with a contribution of 76.7 percent of the CDF

- Loss of RNS initiating event during drained condition with a contribution of 10.4 percent of the CDF

- Loss of offsite power initiating event during drained condition with a contribution of 8.2 percent of the CDF

Loss of Component Cooling or Service Water System Initiating Event During Drained Condition

These sequences are described as the loss of decay heat removal initiated by failure of the component cooling water or service water system during drained condition. The loss of decay heat removal occurs following loss of component cooling water system (CCS) or service water system (SWS) during mid-loop/vessel flange operation, which has an estimated duration of 120 hours per 18 months refueling cycle.

The major contributors to risk due to loss of CCS or SWS during drained condition are the following:

- Hardware failures of both service water pumps or common cause failure of digital input/output modules from the protection and monitoring system (PMS)

- Common cause failure of the ADS 4^{th} stage squib valves

- Common cause failure of the recirculation line squib valves

- Common cause failure of the IRWST injection squib valves
- Common cause failure of the strainers in the IRWST tank
- Common cause failure of the recirculation sump strainers

Loss of RNS Initiating Event During Drained Condition

This sequence is described as the loss of decay heat removal initiated by failure of the RNS during drained condition. The loss of decay heat removal occurs following loss of RNS during mid-loop/ vessel flange operation, which has an estimated duration of 120 hours per 18 months refueling cycle.

The major contributors to risk due to loss of RNS during drained condition are the following:

- Common cause failure of the RNS pumps to run
- Common cause failure of the recirculation line squib valves
- Common cause failure of the ADS 4th stage squib valves
- Common cause failure of the IRWST injection squib valves
- Common cause failure of the strainers in the IRWST tank
- Common cause failure of the recirculation sump strainers

Loss of Offsite Power Initiating Event During Drained Condition (with failure of grid recovery within 1 hour)

This sequence is initiated by loss of offsite power during mid-loop/vessel flange operation, which has an estimated duration of 120 hours per 18 months refueling cycle. Following this initiating event, the RNS does not restart automatically, and the grid is not recovered within 1 hour.

The major contributors to risk given loss of offsite power (without grid recovery) are the following:

- Failure of the RNS pump to run or restart
- Failure of the diesel generator to start or run
- Failure of the main breaker to open
- Failure to recover ac power within 1 hour
- Failure of Ovation digital output modules for RNS-V055
- Common cause failure of the ADS 4th stage squib valves
- Common cause failure of batteries IDSA-DB-1A/1B
- Common cause failure to start engine-driven fuel pumps
- Common cause failure of the IRWST injection squib valves
- Common cause failure of the strainers in the IRWST tank
- Common cause failure of the recirculation sump strainers

Loss of Offsite Power Initiating Event During Drained Condition (with success of grid recovery within 1 hour)

This sequence is initiated by loss of offsite power during mid-loop/vessel flange operation which has an estimated duration of 120 hours per 18 months refueling cycle. Following this initiating event, the RNS does not restart automatically, the grid is recovered within 1 hour but manual RNS restart after grid recovery fails.

The major contributors to risk, given loss of offsite power (with grid recovery), are the following:

- Failure of the RNS pump to run or restart
- Common cause failure of the ADS 4th stage squib valves
- Failure of Ovation digital output modules for RNS-V055
- Common cause failure of the recirculation line squib valves

- Common cause failure of the IRWST injection squib valves
- Common cause failure of the strainers in the IRWST tank
- Common cause failure of the recirculation sump strainers

Conclusions

The conclusions drawn from the shutdown Level 1 study are as follows:

- The overall shutdown core damage frequency is very small (1.03E-07/year).

- Initiating events during reactor coolant system drained conditions contribute approximately 95 percent of the total shutdown core damage frequency. Loss of decay heat removal capability (during drained condition) due to failure of the component cooling water system or service water system is the initiating event with the greatest contribution (approximately 77 percent of the shutdown core damage frequency).

- Common cause failures of in-containment refueling water storage tank components contribute approximately 56 percent of the total shutdown core damage frequency. Common cause failure of the in-containment refueling water storage tank valves contributes approximately 45 percent of the total shutdown core damage frequency.

- Common cause failures of the automatic depressurization system stage 4 squib valves contribute approximately 26 percent to the total shutdown core damage frequency. The function of the automatic depressurization system is important to preclude the effects of surge line flooding. This indicates that maintaining the reliability of the automatic depressurization system is important.

- Common cause failures of the containment sump recirculation squib valves contribute approximately 22 percent to the total shutdown core damage frequency. This function is important during drained conditions. This indicates that maintaining the reliability of the recirculation line squib valves is important.

- Human errors are not overly important to shutdown core damage frequency. There is no particular dominant contributor. Sensitivity results show that the shutdown core damage frequency would remain very low even with little credit for operator actions.

- One action, operator failure to recognize the need for reactor coolant system depressurization during safe/cold shutdown conditions, is identified as having a significant risk increase value. This indicates it is important that the procedures include this action and the operators understand and are appropriately trained for it.

- Individual component failures are not significant contributors to shutdown core damage frequency, and there is no particular dominant contributor. This confirms the at-power conclusion that single independent component failures do not have a large impact on core damage frequency for AP1000 and reflects the redundancy and diversity of protection at shutdown as well.

- The in-containment refueling water storage tank provides a significant benefit during shutdown because it serves as a passive backup to the normal residual heat removal system.

19.59.5.2 Large Release Frequency for Shutdown and Low-Power Events

The baseline PRA shutdown large release frequency for AP600 was calculated to be 1.5E-08 per reactor-year, associated with a shutdown CDF of 9.0E-08 per year. The AP1000 LRF is estimated to

be 1.72E-08 per year, with the same risk profile as that of AP600 (see Table 19.59-15). This LRF compares well with the at-power LRF of 1.95E-08 per year.

19.59.5.3 Shutdown Results Summary

The results of the low-power and shutdown assessment show that the AP1000 design includes redundancy and diversity at shutdown not found in current plants. In particular, the in-containment refueling water storage tank provides a unique safety backup to the normal residual heat removal system. Maintenance at shutdown has less impact on the defense-in-depth features for AP1000 than for current plants. In accordance with plant technical specifications, safety-related system planned maintenance is performed only during those shutdown modes when the protection provided by the safety-related system is not required. Further, maintenance of nonsafety systems, such as the normal residual heat removal system, component cooling water system, and service water system, is performed at power to avoid adversely affecting shutdown risk. These contribute to the extremely low shutdown core damage frequency and the low large release frequency.

19.59.6 Results from Internal Flooding, Internal Fire, and Seismic Margin Analyses

19.59.6.1 Results of Internal Flooding Assessment

A scoping internal flooding analysis was performed based on AP1000 design information, with conservative assumptions or engineering judgement used for simplifying the analysis.

The AP1000 design philosophy of minimizing the number of potential flooding sources in safety-related areas, along with the physical separation of redundant safety-related components and systems from each other and from nonsafety-related components, minimizes the consequences of internal flooding. The core damage frequencies from flooding events at power are not an appreciable contributor to the overall AP1000 core damage frequency. The internal flooding-induced core damage frequencies are estimated to be 8.8E-10 events per year for power operations.

The internal flooding analysis conservatively assumes that flooding of nonsafety-related equipment results in system failure of the affected system. As shown in AP600 PRA, this results in a higher flooding-induced core damage frequency at shutdown than at power, because of the use of the nonsafety-related normal residual heat removal system as the primary means of decay heat removal at shutdown.

The top five at-power flooding scenarios comprise 91 percent of the at-power flooding-induced core damage frequency. Each of these scenarios relate to large pipe breaks in the turbine building with an initiating event frequency in the range of 1.4 - 2.0E-03/year, leading to a loss of CCS/SWS event. Each scenario has a CDF of 1.2 - 1.8E-10/year.

Internal flooding events during shutdown operations are also evaluated. A quantitative internal flooding PRA of AP1000 design performed to estimate plant CDF and LRF for at-power and during low-power and shutdown events provided the following results:

	Plant CDF	Plant LRF
Internal Flooding During At-Power Events	8.82E-10/yr	7.14E-11/yr
Internal Flooding During Low-Power and Shutdown Events	3.22E-09/yr	5.37E-10/yr

The minimization of potential flooding sources in the safety-related areas, in addition to the physical separation of redundant safety-related components and systems from each other and from nonsafety-related components, reduces the consequences of internal flooding. The core damage

and large release frequencies arising from flooding events during shutdown operations are not appreciable contributors to overall AP1000 risk.

19.59.6.2 Results of Internal Fire Assessment

The total at-power, fire-induced core damage frequency is 5.61E-08 per reactor year. The estimated LRF is 4.54E-09/yr. Results of the AP1000 fire PRA analysis are summarized below.

The estimated core damage frequency from main control room fires at power is insignificant (less than 3.18E-12 per year). This low contribution is a result of the following:

- The ignition frequency is low because of the use of low-voltage 48v 10 mA dc cables in the control room. These low-voltage cables do not produce enough energy to heat the cables, thus ignition is not probable.

- Redundancy in control room operations is available within the control room itself; that is, if control room evacuation is not required, there is at least one other means available within the control room to shut down and control the plant.

- If control room evacuation is necessary, the remote shutdown workstation provides complete redundancy in terms of control for safe shutdown functions.

- Loss of control of one division of power or for a whole system is not risk-significant. In addition, the passive systems are designed to operate without the need for operator interaction. Therefore, operator actions that might be disrupted by the fire scenario are backup actions, and are not significant.

The results of the internal fire evaluation indicate that the plant's system and layout promote a low fire-induced core damage frequency compared with existing plants. Also, the results indicate that, when nonsafety-related systems are not credited and containment is treated as a special case, the fire-induced core damage frequency profile is relatively flat (i.e., no fire area is significantly more important than others).

The results from the AP1000 fire analysis confirm that the inherent design characteristics of the AP1000 also provide an effective barrier against fire hazards. This is true even within the pessimistic assumptions used throughout the study.

Conservatisms employed in the AP1000 fire analysis included the following:

- In order to minimize potential uncertainty in the results arising from the lack of as-built equipment location and cable routing information, a bounding approach to quantification, using the focused PRA models, was taken in accordance with the Reference methodology.

- A fire originating from any ignition source in an area is assumed to disable all equipment located in the fire area. The historical evidence indicates that most fires are localized fires with limited severity.

- An assumed total at-power fire initiating event frequency corresponding to about one fire with significant consequences every 4 reactor years, well in excess of current plant experience and of that anticipated for AP1000, was assumed.

- Manual fire suppression is not credited to limit the extent of damage in an area nor to prevent fire propagation to an adjoining area. Historical evidence indicates that the majority of suppressed fires were manually suppressed with little or no additional damage.

- The assumption was made that a single hot short could result in spurious automatic depressurization system actuation.

- The estimation of containment fire frequency, not normally included in fire risk assessments, was done by making a conservative interpretation of the limited available data.

Because the approach taken in performing the internal fire analysis makes various conservative assumptions and is bounding, the results of uncertainty, sensitivity, or importance analyses would be biased. Therefore, these analyses were not performed based on the judgement that they would be of little value in providing additional insights to determine whether fire vulnerabilities exist for beyond-design-basis fires.

The major reasons for the AP1000's relatively low overall fire-induced core damage frequency, even on a bounding basis, include the following:

- The fire protection design provides, to the extent possible, separation of the alternate safety-related shutdown components and cabling using 3-hour-rated fire barriers. For example, areas containing safety-related cabling or components are physically separated from one another and from the areas that do not contain any safety-related equipment by 3-hour-rated fire barriers. This defense-in-depth feature diminishes the probability of a fire to impact more than one safety-related shutdown system.

- Since the passive safety-related systems do not require cooling water or ac power, they are less susceptible to being unavailable due to a fire than currently operating plants' active safe shutdown equipment. As a result, the impact of fires on the shutdown capability is significantly reduced compared to current plants.

The results of this analysis show that the AP1000 design is sufficiently robust that internal fires during either power operation or shutdown do not represent a significant contribution to core damage frequency.

19.59.6.3 Results of Seismic Margin Analysis

The seismic margin analysis (SMA) shows the systems, structures, and components required for safe shutdown. The high confidence, low probability of failure (HCLPF) values are greater than or equal to 0.50g. This HCLPF is determined by the seismically induced failure of the fuel in the reactor vessel, core assembly failures, IRWST failure, or containment interior failures. The SMA result assumes no credit for operator actions at the 0.50g review level earthquake, and assumes a loss of offsite power for all sequences.

The seismic margin analysis shows the plant to be robust against seismic event sequences that contain station blackout coupled with other seismic or random failures. The analysis also shows the plant's capability to respond to seismic events without benefit of the operators' actions.

19.59.7 Plant Dose Risk from Release of Fission-Products

The design certification of the AP1000 included consideration by the NRC of the topic referred to in this section.

19.59.8 Overall Plant Risk Results

The total plant risk expressed in terms of plant core damage frequency and severe release frequency for all events studied in this PRA are summarized in Table 19.59-17.

The contribution of various events to the at-power core damage frequency is shown in Figure 19.59-1.

The total plant core damage and large release frequency analysis results show the following:

- The total mean core damage frequency is at least two orders of magnitude smaller than those for existing pressurized water reactors. The cumulative core damage probability for a population of 50 AP1000 units operating for 60 years each would be less than 0.001, which is a low probability of occurrence.

- The total plant severe release frequency is another order of magnitude smaller than that of the core damage frequency; that places such a release frequency in the range of incredible events.

- A bounding analysis of the core damage due to internal fire and internal flooding events shows that these two categories of internal events are lower for AP1000 than are calculated for currently operating plants.

- The severe release frequency is about equal for at-power and shutdown events. The severe release frequency as a percentage of core damage frequency is 8 percent for at-power events and 17 percent for shutdown events.

- The results show that the design goals of low core damage frequency and low severe release frequency have been met. The AP1000 frequencies are lower than the Nuclear Regulatory Commission (NRC) goals set for new plant designs, as shown in Table 19.59-17. These results show the effectiveness of passive systems in mitigating severe accidents and reflect the reduced dependence of AP1000 on nonsafety systems and human actions.

19.59.9 Plant Features Important to Reducing Risk

Westinghouse used PRA results extensively in the AP1000 design process to identify areas for design improvement and areas for further risk reduction. These results were also compared with existing commercial nuclear power plants to identify additional area of risk reduction. Examples of the more significant AP1000 plant features and operator actions that reduce risk are discussed in this section. Examples are provided in the area of reactor design, system design, plant structures and layout, and containment design.

AP1000 has more lines of defense as compared to current operating plants, which provide more success paths following an initiating event and provide redundancy and diversity to address common cause-related concerns. Examples of extensive AP1000 lines of defense follow:

- Criticality control:
  - Control rod insertion via reactor trip breaker opening
  - Control rod insertion via motor-generator set de-energization
  - Ride out via turbine trip

- Core heat removal:
  - Main feedwater
  - Startup feedwater
  - Passive residual heat removal

  - Automatic depressurization system and feed-and-bleed via normal residual heat removal injection
  - Automatic depressurization system and passive feed-and-bleed via in-containment refueling water storage tank injection

- Reactor coolant system makeup:
  - Chemical and volume control system
  - Core makeup tanks
  - Automatic depressurization system and normal residual heat removal
  - Automatic depressurization system, accumulators, and in-containment refueling water storage tank injection
  - Automatic depressurization system, core makeup tanks, and in-containment refueling water storage tank injection

- Containment cooling:
  - Fan coolers
  - Normal residual heat removal
  - Passive containment cooling system with passive water drain
  - Passive containment cooling system with alternate water supply
  - Passive containment cooling system without water (air only)
  - Fire water

19.59.9.1 Reactor Design

The AP1000 reactor coolant system has many features that reduce the plant risk profile. The pressurizer is larger than those used in comparable current operating plants, resulting in a longer drainage time during small loss-of-coolant accident events. The larger pressurizer increases transient operation margins, resulting in a more reliable plant with fewer reactor trips, avoiding challenges to the plant and operator during transients. The larger pressurizer also eliminates the need for fast-acting power-operated relief valves (PORVs), which are a possible source of reactor coolant system leaks.

The AP1000 steam generators have large secondary-side water inventories, allowing significant time to recover steam generator feedwater or other means of core heat removal. The AP1000 steam generators also employ improved materials and design features that significantly reduce the probability of forced outages or tube rupture.

The AP1000 has sealless reactor coolant pumps, thus avoiding seal loss-of-coolant accident issues related to shaft seals and simplifying the chemical and volume control system. The reactor coolant system has fewer welds, which reduces the potential for loss-of-coolant accident events. The probability of a loss-of-coolant accident is also reduced by the application of “leak-before-break” to reactor coolant system piping.

19.59.9.2 Systems Design

System design aspects intended to reduce plant risk are discussed in terms of safety-related and nonsafety-related systems.

19.59.9.2.1 Safety-Related Systems

The AP1000 uses passive safety-related systems to mitigate design basis accidents and reduce public risk. The passive safety-related systems rely on natural forces such as density differences, gravity, and stored energy to provide water for core and containment cooling. These passive systems do not include active equipment such as pumps. One-time valve alignment of safety-related valves actuates the passive safety-related systems using valve operators such as:

- DC motor-operators with power provided by Class 1E batteries
- Air-operators that reposition to the safeguards position on a loss of the nonsafety-related compressed air that keeps the safety-related equipment in standby
- Squib valves
- Check valves

The passive systems are designed to function with no operator actions for 72 hours following a design basis accident. These systems include the passive containment cooling system and the passive residual heat removal system.

Diversity among the passive systems further reduces the overall plant risk. An example of operational diversity is the option to use passive residual heat removal versus feed-and-bleed for decay heat removal functions, and an example of equipment diversity is the use of different valve operators (motor, air, and squib) to avoid common cause failures.

The passive residual heat removal heat exchanger protects the plant against transients that upset the normal steam generator feedwater and steam systems. The passive residual heat removal subsystem of the passive core cooling system contains no pumps and significantly fewer valves than conventional plant auxiliary feedwater systems. This increases the reliability of the system. There are fewer potential equipment failures (pumps and valves) and less maintenance activities.

For reactor coolant system water inventory makeup during loss-of-coolant accident events, the passive core cooling system uses three passive sources of water to maintain core cooling through safety injection: the core makeup tanks, accumulators, and in-containment refueling water storage tank. These sources are directly connected to two nozzles on the reactor vessel so that no injection flow can be spilled for larger pipe break events.

The automatic depressurization system is incorporated into the design for depressurization of the reactor coolant system. The automatic depressurization system has 10 paths with diverse valves to avoid common cause failures, and it is designed for automatic or manual actuation by the protection and safety monitoring system or manual actuation by the diverse actuation system. The automatic depressurization system can be used in a partial depressurization mode to provide long-term reactor coolant system cooling with normal residual heat removal system injection, or it can be used in full depressurization mode for passive in-containment refueling water storage tank injection for long-term reactor coolant system cooling. Switchover from injection to recirculation is automatic without manual actions.

The safety-related Class 1E dc and UPS system has a battery capacity sufficient to support passive safety-related systems for 72 hours. This system has four 24-hour batteries, two 72-hour batteries, and a spare battery. The presence of the spare battery improves testability.

The passive containment cooling system provides the safety-related ultimate heat sink for the plant. Heat is removed from the containment vessel following an accident by a continuous natural

circulation flow of air, without any system actuations. By using the passive containment cooling system following an accident, the containment stays well below the predicted failure pressure. The steaming and condensing action of the passive containment cooling system enhances activity removal.

AP1000 containment isolation is significantly improved over that of conventional PWRs due to a large reduction in the number of penetrations. The number of normally open penetrations is reduced. Containment isolation is improved due to the chemical and volume control system being a closed system; the safety-related passive safety injection components being located inside the containment; and the number of heating, ventilation, and air conditioning (HVAC) penetrations being reduced (no maxi purge connection).

Vessel failure potential upon core damage is reduced (in-vessel retention of the damaged core) by providing a provision to dump in-containment refueling water storage tank water into the reactor cavity. The vessel insulation enables this water to cool the vessel.

For events at shutdown, the AP1000 has passive safety-related systems for shutdown conditions as a backup to the normal residual heat removal system. This reduces the risk at shutdown through redundancy and diversity.

Post-72-hour connections are incorporated into the passive system design to allow for long-term accident management. These connections allow for the refill of the in-containment refueling water storage tank, or the reactor cavity, should such actions become necessary.

19.59.9.2.2 Nonsafety-Related Systems

The AP1000 has nonsafety-related systems capable of mitigating accidents. These systems use redundant components, which are powered by offsite and onsite power supplies. The AP1000 has certain design features in the nonsafety-related systems to reduce plant risk compared to current operating plants. During transient events, the startup feedwater system can act as a backup to the main feedwater system if the latter is unavailable due to the nature of the initiating event or fails during the transient. During loss of ac power events, startup feedwater pumps are powered by the diesel generators and can be used to remove decay heat since main feedwater is not available. The main feedwater and startup feedwater pumps are motor-driven, rather than steam-driven, for better reliability. Main feedwater controls are digital for better reliability. Thus, the main feedwater and startup feedwater system creates fewer transients and provides additional nonsafety-related means for decay heat removal for transients. This makes the plant response to transients very robust due to the existence of two nonsafety-related systems in addition to the passive safety-related means of removing decay heat.

The nonsafety-related normal residual heat removal system plays a role in decay heat removal in response to power and shutdown events. The normal residual heat removal system has additional isolation valves and is designed to withstand the reactor coolant system pressure to eliminate interfacing systems loss-of-coolant accident concerns that lead to containment bypass. The normal residual heat removal system provides reliable shutdown cooling, incorporating lessons learned from shutdown events. During mid-loop operations, operation procedures require both normal residual heat removal system pumps to be operable for risk reduction.

Component cooling water and service water systems have a limited role in the plant risk profile because the passive safety-related systems do not require cooling, and the reactor coolant pumps do not require seal cooling from the component cooling water.

The nonsafety-related ac power system (onsite and offsite) also has a limited role in the plant risk profile since the plant safety-related systems do not depend on ac power. The loss of offsite power

event is less important for the AP1000 than in current operating plants. The plant has full load rejection capability to minimize the number of reactor trips although this is not modeled in the PRA and no credit is taken for it. The onsite ac power has two nonsafety-related diesel generators. The diesel generator life is improved and the run failure rate is reduced by avoiding fast starts.

The compressed and instrument air system has low risk importance since the safety-related air-operated valves are fail safe if the air system fails. This causes the loss of air event to be less important than in current plant PRAs.

19.59.9.3 Instrumentation and Control Design

Three instrumentation and control systems are modeled in the AP1000 PRA: protection and safety monitoring system, plant control system, and diverse actuation system. Both the protection and safety monitoring system and plant control system are microprocessor-based. Four trains of redundancy are provided for the protection and safety monitoring system; 2-out-of-4 actuation logic in the protection and safety monitoring system reduces the potential for spurious trips due to testing and allows for better testing. Automatic testing for the protection and safety monitoring system, and diagnostic self-testing for the protection and safety monitoring system and the plant control system, provide higher reliability in these systems. Both the protection and safety monitoring system and the plant control system use fiber-optic cables (with fire separation) for data transmission. Unlike current plants, there is no cable spreading room. This eliminates a potential fire hazard. Additional fault tolerance is built into the plant control system so that one failure does not prevent the operation of important functions.

Improvements in the plant control system and the protection and safety monitoring system are coupled with an improved control room and man-machine interfaces; these include improvements in the form and contents of the information provided to control room operators for decision making to limit commission errors. In addition, the remote shutdown workstation is designed to have functions similar to the control room.

The diverse actuation system provides a diverse automatic and manual backup function to the protection and safety monitoring system and reduces risk from anticipated transients without scram events. The diverse actuation system also compensates for common cause failures in the protection and safety monitoring system.

19.59.9.4 Plant Layout

The plant layout minimizes the consequences of fire and flooding by maximizing the separation of electrical and mechanical equipment areas in the non-radiologically controlled area of the auxiliary building. This separation is designed to minimize the potential for propagation of leaks from the piping areas and the mechanical equipment areas to the Class 1E electrical and Class IE instrumentation and control equipment rooms. The potential flooding sources and volumes in areas of the plant that contain safety-related electrical and I&C equipment are limited to minimize the consequences of internal flooding.

The AP1000 is designed to provide better separation between divisions of safety-related equipment.

19.59.9.5 Containment Design

The containment pressure boundary is the final barrier to the release of fission products to the environment. The AP1000 containment has provisions that help to maintain containment integrity in a severe accident.

19.59.9.5.1 Containment Isolation and Leakage

Failure of the containment isolation system before a severe accident will lead to a direct release pathway from the containment volume to the environment. The AP1000 has approximately 55 percent fewer piping penetrations and a lower percentage of normally open penetrations compared to current generation plants. Normally open penetrations are closed by automatic valves, and diverse actuation is provided for valves on penetrations with significant leakage potential. All isolation valves have control room indication to inform the operator of the current valve position.

Similarly to containment isolation failure, leakage of closed containment isolation valves in excess of technical specifications may result in larger releases to the environment. Valves that historically have the greatest leakage problems have been eliminated, or their number significantly reduced in the design. Large purge valves have been replaced by smaller more reliable valves, and check valves have been used only in mild service where wear and service conditions would not be a challenge to successful operation.

Equipment and personnel hatches have the capability of being tested individually to ensure a leak-tight seal. Hatch seals can easily be verified.

Therefore, the AP1000 provides significant protection against the failure to isolate the containment and against the failure of isolation valves to fully close.

19.59.9.5.2 Containment Bypass

Historically, containment bypass, an accident in which the fission products are released directly to the environment from the reactor coolant system, is the leading contributor to risk in a nuclear power plant. Typically the containment bypass accident class consists of two types of accident sequences: interfacing systems loss-of-coolant accidents and steam generator tube ruptures.

An interfacing systems loss-of-coolant accident is the failure of valves that separate the high pressure reactor coolant system with a lower pressure interfacing system, which extends outside the containment pressure boundary. The failure of the valve causes the reactor coolant system to pressurize the interfacing system beyond its ultimate capacity and can result in a loss-of-coolant accident outside the containment. Reactor coolant is lost outside the containment, providing a pathway for the direct release of fission products to the environment. In AP1000, systems connected to the reactor coolant system are designed with higher design pressure, which reduces the likelihood of a pipe rupture in the event of the failure of the interfacing valves. This results in a very low interfacing systems loss-of-coolant-accident contribution to core damage to containment bypass.

Steam generator tube ruptures release coolant from the reactor coolant system to the secondary system. The AP1000 has multiple and diverse automatically actuated systems to reduce the reactor coolant system pressure and mitigate the steam generator tube rupture. The passive residual heat removal subsystem is actuated automatically on the S-signal and effectively reduces the reactor coolant system pressure to stop the break flow. If the passive residual heat removal does not stop the loss of coolant, the secondary relief valve can open to keep the secondary system pressure below the opening pressure of the steam generator safety valve. If the loss of reactor coolant continues, the RCS automatic depressurization system will actuate and depressurize the system. No operator actions are required to mitigate the accident, and the secondary system remains sealed against releases to the environment after the relief valve or its block valve are closed.

To create a containment bypass release pathway from a steam generator tube rupture, the accident scenario must include multiple system failures such that the steam generator tube rupture is not mitigated, and the secondary system pressure increases enough to open a safety valve. The safety

valve must fail to reseat, and thereby provide a containment bypass pathway for the loss of coolant and for the possible release of fission products to the environment.

Multiple, diverse systems act to mitigate steam generator tube rupture. Therefore, the likelihood of a steam generator tube rupture progressing to containment bypass has been significantly reduced in AP1000.

19.59.9.5.3 Passive Containment Cooling

The passive containment cooling system provides protection to the containment pressure boundary by removing the decay and chemical heat that slowly pressurize the containment. The heat is transferred to the environment through the steel pressure boundary. The heat transfer on the outside of the steel shell is enhanced by an annular flow path, which creates a convective air flow across the shell, and by the evaporation of water that is directed onto the top of the containment in the event of an accident. The evaporative heat transfer prevents the containment from pressurizing above the design conditions during design basis accidents.

In some postulated multiple-failure accident scenarios, the water flow may fail. The heat removal is limited to convection heat transfer to the air flow and radiation to the annulus baffle. With no water film on the containment shell to provide evaporative cooling, the containment pressurizes above the design pressure to remove decay heat. Containment failure within 24 hours is highly unlikely.

19.59.9.5.4 High-Pressure Core Melt Scenarios

The automatic depressurization system and the passive residual heat removal heat exchanger provide reliable and diverse reactor coolant system depressurization, which significantly reduces the likelihood of high-pressure core damage. High-pressure core damage sequences have the potential to fail steam generator tubes and create a containment bypass release, or to cause severe accident phenomena at the time of vessel failure, which may threaten the containment pressure boundary. Reducing the reactor coolant system pressure during a severe accident significantly lowers the likelihood of phenomena that may induce large fission product releases early in the accident sequence.

19.59.9.5.5 In-Vessel Retention of Molten Core Debris

The AP1000 reactor vessel and containment configuration have features that enhance the design's ability to maintain molten core debris in the reactor vessel. The AP1000 automatic depressurization system provides reliable pressure reduction in the reactor coolant system to reduce the stresses on the vessel wall. The reactor vessel lower head has no vessel penetrations. This eliminates penetration failure as a potential vessel failure mode. The containment configuration directs water to the reactor cavity and allows the in-containment refueling water storage tank water to be drained into the cavity to submerge the vessel to cool the external surface of the lower head. Cooling the vessel and reducing the stresses prevent the creep rupture failure of the vessel wall. The reactor vessel reflective insulation has been designed with provisions to allow water inside the insulation panel to cool the vessel surface, and with vents to allow steam to exit the insulation without failing the insulation support structures. The insulation is designed so that it promotes the cooling of the external surface of the vessel.

Preventing the relocation of molten core debris to the containment eliminates the occurrence of several severe accident phenomena, such as ex-vessel fuel-coolant interactions and core-concrete interaction, which may threaten the containment integrity. Through the prevention of core debris relocation to the containment, the AP1000 design significantly reduces the likelihood of containment failure.

19.59.9.5.6 Combustible Gases Generation and Burning

In severe accident sequences, high-temperature metal oxidation, particularly zirconium, results in the rapid generation of hydrogen and possibly carbon monoxide. The first combustible gas release occurs in the accident sequence during core uncovery when the oxidation of the zircaloy cladding by passing steam generates hydrogen. A second release may occur if the vessel fails and ex-vessel debris degrades the concrete basemat. Steam and carbon dioxide are liberated from the concrete and are reduced to hydrogen and carbon monoxide as they pass through the molten metal in the debris. These gases are highly combustible and in high concentrations in the containment may lead to detonable mixtures.

The AP1000 uses a nonsafety-related hydrogen igniter system for severe releases of combustible gases. The igniters are powered from ac buses from either of the nonsafety-related diesel generators or from the non-Class 1E batteries. Multiple glow plugs are located in each compartment. The igniters burn the gases at the lower flammability limit. At this low concentration, the containment pressure increase from the burning is small and the likelihood of detonation is negligible. The igniters are spaced such that the distance between them will not allow the burn to transition from deflagration to detonation. The combustible gases are removed with no threat to the containment integrity.

There is little threat of the failure of the system power in the event that it is required to operate. The igniters are needed only in core damage accidents, and the AP1000 is designed to mitigate loss of power events without the sequence evolving into a severe accident. Loss of ac power is a small contributor to the core damage frequency.

The reliability of reactor coolant system depressurization reduces the threat to the containment from sudden releases of hydrogen from the reactor coolant system. Low pressure release of in-vessel hydrogen enhances the ability of the igniter system to maintain the containment atmosphere at the lower flammability limit.

During a severe accident, hydrogen, which could be injected from the reactor coolant system into the containment through the spargers in the in-containment refueling water storage tank or into the core makeup tank room, has the potential to produce a diffusion flame. A diffusion flame is produced when a combustible gas plume that is too rich to burn enters an oxygen-rich atmosphere and is ignited by a glow plug or a random ignition source. The plume is ignited into a standing flame, which lasts as long as there is a fuel source. Via convection and radiation, the flame can heat the containment wall to high temperatures, increasing the likelihood of creep rupture failure of the containment pressure boundary. The AP1000 uses a defense-in-depth approach to release hydrogen in benign locations away from the containment shell and penetrations. Therefore, the potential for containment failure from the formation of a diffusion flame at the in-containment refueling water storage tank vents is considered to be low.

There is little threat to the containment integrity from severe accident hydrogen releases and hydrogen combustion events. The igniter system maintains the hydrogen concentration at the lower flammability limit.

19.59.9.5.7 Intermediate and Long-Term Containment Failure

The passive containment cooling system reduces the potential for decay heat pressurization of the containment. However, containment failure can also occur as a result of combustion. Due to the high likelihood of in-vessel retention of core debris, the potential for ex-vessel combustible gas generation from core-concrete interaction is low. The frequency of containment failures due to hydrogen combustion events is low given the high reliability of the hydrogen igniters.

19.59.9.5.8 Fission-Product Removal

The AP1000 relies on the passive, natural removal of aerosol fission products from the containment atmosphere, primarily from gravitational settling, diffusiophoresis, and thermophoresis. Natural removal is enhanced by the passive containment cooling system, which provides a large, cold surface area for condensation of steam. This increases the diffusiophoretic and thermophoretic removal processes. Accident offsite doses at the site boundary, which could exist in the first 24 hours after a severe accident, are either less than 25 rem, or for those releases that are greater than 25 rem, have a frequency of much less than 1E-06. Minimal credit is taken for deposition of fission products in the auxiliary building. The site boundary dose and large release frequency are much less than the established goals.

19.59.10 PRA Input to Design Certification Process

The AP1000 PRA was used in the design certification process to identify important safety insights and assumptions to support certification requirements, such as the reliability assurance program (RAP).

19.59.10.1 PRA Input to Reliability Assurance Program

The AP1000 RAP identifies those systems, structures, and components (SSC) that should be given priority in maintaining their reliability through surveillance, maintenance, and quality control actions during plant operation. The PRA importance and sensitivity analyses identify those systems and components that are important in plant risk in terms of either risk increase (for example, what happens to plant risk if a system or component, or a train is unavailable), or in terms of risk decrease (for example, what happens to plant risk if a component or a train is perfectly reliable/available). This ranking of components and systems in such a way provides an input for the reliability assurance program. For more information on the AP1000 reliability assurance program, refer to Section 17.4.

19.59.10.2 PRA Input to Tier 1 Information

Section 14.3 summarizes the design material contained in AP1000 that has been incorporated into the Tier 1 Information from the PRA.

19.59.10.3 PRA Input to MMI/Human Factors/Emergency Response Guidelines

The PRA models, including modeling of operator actions in response to severe accident sequences, follow the ERGs. The most risk important of these actions is manual actuation of systems in the highly unlikely event of automatic actuation failure. These operator actions and the main human reliability analysis (HRA) model assumptions are reviewed by human factors engineers for insights that they may provide to the human system interface (HSI) and human factors areas. For more information on the AP1000 HSI, refer to Chapter 18.

In addition, the human reliability analysis models and operator actions modeled in the PRA were reviewed by the engineers writing the ERGs for consistency between the PRA models and the actual ERGs.

The PRA results and sensitivity studies show that the AP1000 design has no critical operator actions and few risk important actions. A critical operator action is defined as that action, when assumed to fail, would result in a plant core damage frequency of greater than 1.0E-04 per year; there are no such operator actions in the AP1000 PRA.

19.59.10.4 Summary of PRA Based Insights

The use of the PRA in the design process is discussed in Subsection 19.59.2. A summary of the overall PRA results is provided in Subsections 19.59.3 through 19.59.8. A discussion of the AP1000 plant features important to reducing risk is provided in Subsection 19.59.9. PRA-based insights are developed from this information and are summarized in Table 19.59-18.

19.59.10.5 Combined License Information

A review of the differences between the as-built plant and the design used as the basis for the AP1000 seismic margins analysis will be completed prior to fuel load. A verification walkdown will be performed with the purpose of identifying differences between the as-built plant and the design. Any differences will be evaluated and the seismic margins analysis modified as necessary to account for the plant-specific design, and any design changes or departures from the certified design. A comparison of the as-built SSC high confidence, low probability of failures (HCLPFs) to those assumed in the AP1000 seismic margin evaluation will be performed prior to fuel load. Deviations from the HCLPF values or assumptions in the seismic margin evaluation due to the as-built configuration and final analysis will be evaluated to determine if vulnerabilities have been introduced.

The requirements to which the equipment is to be purchased are included in the equipment specifications. Specifically, the equipment specifications include:

1. Specific minimum seismic requirements consistent with those used to define the AP1000 Table 19.55-1 HCLPF values.

   This includes the known frequency range used to define the HCLPF by comparing the required response spectrum (RRS) and test response spectrum (TRS). The test response spectra are chosen so as to demonstrate that no more than one percent rate of failure is expected when the equipment is subjected to the applicable seismic margin ground motion for the equipment identified to be applicable in the seismic margin insights of the site-specific PRA.The range of frequency response that is required for the equipment with its structural support is defined.

2. Hardware enhancements that were determined in previous test programs and/or analysis programs will be implemented.

A review of the differences between the as-built plant and the design used as the basis for the AP1000 PRA and Table 19.59-18 will be completed prior to fuel load. The plant-specific PRA-based insight differences will be evaluated and the plant-specific PRA model modified as necessary to account for plant-specific design and any design changes or departures from the design certification PRA.

As discussed in Subsection 19.58.3, it has been confirmed that the Winds, Floods and Other External Events analysis documented in Section 19.58 is applicable to the site. The site-specific design has been evaluated and is consistent with the AP1000 PRA assumptions. Therefore, Section 19.58 is applicable to this design.

A review of the differences between the as-built plant and the design used as the basis for the AP1000 internal fire and internal flood analyses will be completed prior to fuel load. Plant specific internal fire and internal flood analyses will be evaluated and the analyses modified as necessary to account for the plant-specific design, and any design changes or departures from the certified design.

The AP1000 Severe Accident Management Guidance (SAMG) from APP-GW-GLR-070, Reference 19.59-1, is implemented on a site-specific basis. Key elements of the implementation include:

- SAMG based on APP-GW-GLR-070 is provided to Emergency Response Organization (ERO) personnel in assessing plant damage, planning and prioritizing response actions and implementing strategies that delineate actions inside and outside the control room.
- Severe accident management strategies and guidance are interfaced with the Emergency Operating Procedures (EOP's) and Emergency Plan.
- Responsibilities for authorizing and implementing accident management strategies are delineated as part of the Emergency Plan.
- SAMG training is provided for ERO personnel commensurate with their responsibilities defined in the Emergency Plan.

A thermal lag assessment of the as-built equipment required to mitigate severe accidents (hydrogen igniters and containment penetrations) will be performed to provide additional assurance that this equipment can perform its severe accident functions during environmental conditions resulting from hydrogen burns associated with severe accidents. This assessment will be performed prior to fuel load and is required only for equipment used for severe accident mitigation that has not been tested at severe accident conditions. The ability of the as-built equipment to perform during severe accident hydrogen burns will be assessed using the Environment Enveloping method or the Test Based Thermal Analysis method discussed in EPRI NP-4354 (Reference 19.59-3).

As discussed in Subsection 19.55.6.3, it has been confirmed that the Seismic Margin Analysis (SMA) documented in Section 19.55 is applicable to the site. The site-specific effects (i.e., soil-related failure modes, etc.) have been evaluated and it was concluded that the plant-specific plant-level HCLPF value is equal to or greater than 1.67 times the site-specific GMRS peak ground acceleration.

19.59.10.6 PRA Configuration Controls

PRA configuration controls contain the following key elements:

- A process for monitoring PRA inputs and collecting new information.
- A process that maintains and updates the PRA to be reasonably consistent with the as-built, as operated plant.
- A process that considers the cumulative impact of pending changes when applying the PRA.
- A process that evaluates the impact of changes on currently implemented risk-informed decisions that have used the PRA.
- A process that maintains configuration control of computer codes used to support PRA quantification.
- A process for upgrading the PRA to meet PRA standards that the NRC has endorsed.
- Documentation of the PRA.

PRA configuration controls are consistent with the regulatory positions on maintenance and upgrades in Regulatory Guide 1.200.

Schedule for Maintenance and Upgrades of the PRA

The PRA update process is a means to reasonably reflect the as designed and as operated plant configurations in the PRA models. The PRA upgrade process includes an update of the PRA plus a general review of the entire PRA model, and as applicable the application of new software that implements a different methodology, implementation of new modeling techniques, as well as a comprehensive documentation effort.

- During construction, the PRA is upgraded prior to fuel load to cover those initiating events and modes of operation contained in NRC-endorsed consensus standards on PRA in effect one year prior to the scheduled date of the initial fuel load for a Level 1 and Level 2 PRA.
- Prior to license renewal the PRA is upgraded to include all modes of operation.
- During operation, PRA updates are completed as part of the upgrade process at least once every four years.
- A screening process is used to determine whether a PRA update should be performed more frequently based upon the nature of the changes in design or procedures. The screening process considers whether the changes affect the PRA insights. Changes that do not meet the threshold for immediate update are tracked for the next regulatory scheduled update. If the screening process determines that the changes do warrant a PRA update, the update is made as soon as practicable consistent with the required change importance and the applications being used.

PRA upgrades are performed in accordance with 10 CFR 50.71(h).

Process for Maintenance and Upgrades of the PRA

Various information sources are monitored to determine changes or new information that affects the model assumptions or quantification. Plant specific design, procedure, and operational changes are reviewed for risk impact. Information sources include applicable operating experience, plant modifications, engineering calculation revisions, procedure changes, industry studies, and NRC information.

The PRA upgrade includes initiating events and modes of operation contained in NRC-endorsed consensus standards on PRA in effect one year prior to each required upgrade.

This PRA maintenance and update incorporates the appropriate new information including significant modeling errors discovered during routine use of the PRA.

Once the PRA model elements requiring change are identified, the PRA computer models are modified and appropriate documents revised. Documentation of modifications to the PRA model include the changes as well as the upgraded portions clearly indicating what has been changed. The impact on the risk insights is clearly indicated.

PRA Quality Assurance

Maintenance and upgrades of the PRA are subject to the following quality assurance provisions:

Procedures identify the qualifications of personnel who perform the maintenance and upgrade of the PRA.

Procedures provide for the control of PRA documentation, including revisions.

For updates of the PRA, procedures provide for independent review, or checking of the calculations and information.

Procedures provide for an independent review of the model after an upgrade is completed. Additionally, after the PRA is upgraded, the PRA is reviewed by outside PRA experts such as industry peer review teams and the comments incorporated to maintain the PRA current with industry practices. Peer review findings are entered into a tracking system. PRA upgrades receive a peer review for those aspects of the PRA that are upgraded.

PRA models and applications are documented in a manner that facilitates peer review as well as future updates and applications of the PRA by describing the processes that were used, and provide details of the assumptions made and their bases. PRA documentation is developed such that traceability and reproducibility is maintained. PRA documentation is maintained in accordance with Regulatory Position 1.3 of Regulatory Guide 1.200.

Procedures provide for appropriate attention or corrective actions if assumptions, analyses, or information used previously are changed or determined to be in error. Potential impacts to the PRA model (i.e., design change notices, calculations, and procedure changes) are tracked. Errors found in the PRA model between periodic updates are tracked using the site tracking system.

PRA-Related Input to Other Programs and Processes

The PRA provides input to various programs and processes, such as the Maintenance Rule implementation, reactor oversight process, the RAP, and the RTNSS program. The use of the PRA in these programs is discussed below, or cross-references to the appropriate FSAR sections are provided.

PRA Input to Design Programs and Processes

The PRA insights identified during the design development are discussed in Subsection 19.59.10.4 and summarized in Table 19.59-18. Section 14.3 summarizes the design material contained in AP1000 that has been incorporated into the Tier 1 information from the PRA. A discussion of the plant features important to reducing risk is provided in Subsection 19.59.9.

PRA Input to the Maintenance Rule Implementation

The PRA is used as an input in determining the safety significance classification and bases of in-scope SSCs. SSCs identified as risk-significant via the Reliability Assurance Program for the design phase (DRAP, Section 17.4) are included within the initial Maintenance Rule scope as high safety significance SSCs.

For risk-significant SSCs identified via DRAP, performance criteria are established, by the Maintenance Rule expert panel using input from the reliability and availability assumptions used in the PRA, to monitor the effectiveness of the maintenance performed on the SSCs.

The Maintenance Rule implementation is discussed in Section 17.6.

PRA Input to the Reactor Oversight Process

The mitigating systems performance indicators (MSPI) are evaluated based on the indicators and methodologies defined in NEI 99-02 (Reference 201).

The Significance Determination Process (SDP) uses risk insights, where appropriate, to determine the safety significance of inspection findings.

PRA Input to the Reliability Assurance Program

The PRA input to the Reliability Assurance Program is discussed in Subsection 19.59.10.1.

PRA Input to the Regulatory Treatment of Nonsafety-Related Systems Programs

The importance of nonsafety-related SSCs in the AP1000 has been evaluated using PRA insights to identify SSCs that are important in protecting the utility's investment and for preventing and mitigating severe accidents. These investment protection systems, structures and components are included in the D-RAP/MR Program (refer to Section 17.4), which provides confidence that availability and reliability are designed into the plant and that availability and reliability are maintained throughout plant life through the maintenance rule. Technical Specifications are not required for these SSCs because they do not meet the selection criteria applied to the AP1000 (refer to Subsection 16.1.1).

MOV Program

The MOV Program includes provisions to accommodate the use of risk-informed inservice testing of MOVs (Subsection 3.9.6).

19.59.11 References

19.59-1. APP-GW-GLR-070, "Development of Severe Accident Management Guidance," Westinghouse Electric Company LLC.

19.59-2. APP-GW-GL-027, "Framework for AP1000 Severe Accident Management Guidance," Westinghouse Electric Company LLC.

19.59-3. "Large Scale Hydrogen Burn Equipment Experiments," EPRI-NP-4354, December 1985.

19.59-4. APP-GW-GLR-101, "AP1000 Probabilistic Risk Assessment Site Specific Considerations," Westinghouse Electric Company LLC.

19.59-5. APP-GW-GLR-069, "Equipment Survivability Assessment," Westinghouse Electric Company LLC.

201. NEI 99-02 Nuclear Energy Institute, "Regulatory Assessment Performance Indicator Guideline," Technical Report NEI 99-02, Revision 5, July 2007.

Table 19.59-1
Contribution of Initiating Events to Core Damage

	Core Damage Contribution	Initiating Event Category	Percent Contribution	Initiating Event Frequency
1	9.50E-08	SAFETY INJECTION LINE BREAK INITIATING EVENT	39.4%	2.12E-04
2	4.50E-08	LARGE LOCA INITIATING EVENT	18.7%	5.00E-06
3	2.96E-08	SPURIOUS ADS INITIATING EVENT	12.3%	5.40E-05
4	1.81E-08	SMALL LOCA INITIATING EVENT	7.5%	5.00E-04
5	1.61E-08	MEDIUM LOCA INITIATING EVENT	6.7%	4.36E-04
6	1.00E-08	REACTOR VESSEL RUPTURE INITIATING EVENT	4.2%	1.00E-08
7	6.79E-09	STEAM GENERATOR TUBE RUPTURE INITIATING EVENT	2.8%	3.88E-03
8	3.68E-09	CMT LINE BREAK INITIATING EVENT	1.5%	9.31E-05
9	3.61E-09	ATWS PRECURSOR WITH NO MFW INITIATING EVENT	1.5%	4.81E-01(*)
10	3.08E-09	TRANSIENT WITH MFW INITIATING EVENT	1.3%	1.40E+00
11	1.71E-09	RCS LEAK INITIATING EVENT	0.7%	6.20E-03
12	1.66E-09	CORE POWER EXCURSION INITIATING EVENT	0.7%	4.50E-03
13	1.24E-09	LOSS OF CONDENSER INITIATING EVENT	0.5%	1.12E-01
14	9.58E-10	LOSS OF OFFSITE POWER INITIATING EVENT	0.4%	1.20E-01
15	8.70E-10	LOSS OF MAIN FEEDWATER INITIATING EVENT	0.4%	3.35E-01
16	7.12E-10	ATWS PRECURSOR WITH MFW AVAILABLE INITIATING EVENT	0.3%	1.17E+00(*)
17	6.72E-10	LOSS OF COMPRESSED AIR INITIATING EVENT	0.3%	3.48E-02
18	6.06E-10	MAIN STEAM LINE STUCK-OPEN SV INITIATING EVENT	0.3%	2.39E-3
19	5.02E-10	PASSIVE RHR TUBE RUPTURE INITIATING EVENT	0.2%	1.34E-04
20	4.53E-10	LOSS OF MFW TO ONE SG INITIATING EVENT	0.2%	1.92E-01
21	3.23E-10	LOSS OF CCW/SW INITIATING EVENT	0.1%	1.44E-01
22	1.31E-10	MAIN STEAM LINE BREAK UPSTREAM OF MSIV INITIATING EVENT	0.1%	3.72E-04
23	1.11E-10	ATWS PRECURSOR WITH SI SIGNAL INITIATING EVENT	0.1%	1.48E-02(*)
24	5.00E-11	INTERFACING SYSTEMS LOCA INITIATING EVENT	0.0%	5.00E-11
25	3.52E-11	LOSS OF RCS FLOW INITIATING EVENT	0.0%	1.80E-02
26	9.15E-12	MAIN STEAM LINE BREAK DOWNSTREAM OF MSIV INITIATING EVENT	0.0%	5.96E-04
	2.41E-07	Totals	100.0%	2.38(*)

(*) = Note that the ATWS precursor frequencies are not included in the total initiating event frequency, since they are already accounted for in the other categories.

Table 19.59-2
Conditional Core Damage Probability of Initiating Events

	Core Damage Contribution	Initiating Event Category	Initiating Event Frequency	Conditional CD Prob.
6	1.00E-08	REACTOR VESSEL RUPTURE INITIATING EVENT	1.00E-08	1.00E+00
24	5.00E-11	INTERFACING SYSTEMS LOCA INITIATING EVENT	5.00E-11	1.00E+00
2	4.50E-08	LARGE LOCA INITIATING EVENT	5.00E-06	8.99E-03
3	2.96E-08	SPURIOUS ADS INITIATING EVENT	5.40E-05	5.48E-04
1	9.50E-08	SAFETY INJECTION LINE BREAK INITIATING EVENT	2.12E-04	4.48E-04
8	3.68E-09	CMT LINE BREAK INITIATING EVENT	9.31E-05	3.95E-05
5	1.61E-08	MEDIUM LOCA INITIATING EVENT	4.36E-04	3.70E-05
4	1.81E-08	SMALL LOCA INITIATING EVENT	5.00E-04	3.62E-05
19	5.02E-10	PASSIVE RHR TUBE RUPTURE INITIATING EVENT	1.34E-04	3.74E-06
7	6.79E-09	STEAM GENERATOR TUBE RUPTURE INITIATING EVENT	3.88E-03	1.75E-06
18	6.06E-10	MAIN STEAM LINE STUCK-OPEN SV INITIATING EVENT	2.39E-03	2.54E-07
12	1.66E-09	CORE POWER EXCURSION INITIATING EVENT	4.50E-03	3.69E-07
22	1.31E-10	MAIN STEAM LINE BREAK UPSTREAM OF MSIV INITIATING EVENT	3.72E-04	3.51E-07
11	1.71E-09	RCS LEAK INITIATING EVENT	6.20E-03	2.75E-07
17	6.72E-10	LOSS OF COMPRESSED AIR INITIATING EVENT	3.48E-02	1.93E-08
26	9.15E-12	MAIN STEAM LINE BREAK DOWNSTREAM OF MSIV INITIATING EVENT	5.96E-04	1.54E-08
13	1.24E-09	LOSS OF CONDENSER INITIATING EVENT	1.12E-01	1.11E-08
14	9.58E-10	LOSS OF OFFSITE POWER INITIATING EVENT	1.20E-01	7.98E-09
9	3.61E-09	ATWS PRECURSOR WITH NO MFW INITIATING EVENT	4.81E-01	7.49E-09
23	1.11E-10	ATWS PRECURSOR WITH SI SIGNAL INITIATING EVENT	1.48E-02	7.48E-09
15	8.70E-10	LOSS OF MAIN FEEDWATER INITIATING EVENT	3.35E-01	2.60E-09
20	4.53E-10	LOSS OF MFW TO ONE SG INITIATING EVENT	1.92E-01	2.36E-09
21	3.23E-10	LOSS OF CCW/SW INITIATING EVENT	1.44E-01	2.24E-09
10	3.08E-09	TRANSIENT WITH MFW INITIATING EVENT	1.40E+00	2.20E-09
25	3.52E-11	LOSS OF RSC FLOW INITIATING EVENT	1.80E-02	1.96E-09
16	7.12E-10	ATWS PRECURSOR WITH MFW AVAILABLE INITIATING EVENT	1.17E+00	6.09E-10
	2.41E-07	Totals	2.38E+00	

Table 19.59-3 (Sheet 1 of 4)
Internal Initiating Events at Power Dominant Core Damage Sequences

	Sequence Frequency	Percent Contrib	Cumulative % Contrib	Sequence Identifier	Sequence Description
1	6.88E-08	28.52	28.52	2esil-07	SAFETY INJECTION LINE BREAK INITIATING EVENT OCCURS RCPS TRIP AND CMT INJECTION IS SUCCESSFUL – 1 OF 2 CMT TRAINS SUCCESS OF FULL ADS DEPRESSURIZATION FAILURE OF ONE OF ONE IRWST INJECTION LINE
2	4.26E-08	17.66	46.18	2rllo-09	LARGE LOCA INITIATING EVENT OCCURS ANY ONE OF TWO ACCUMULATOR TRAINS FAIL
3	2.13E-08	8.82	55.00	3dsad-08	SPURIOUS ADS INITIATING EVENT OCCURS SUCCESS OF 1/2 OR 2/2 ACCUMULATORS FAILURE OF ADS OR CMT
4	1.98E-08	8.23	63.23	3dsil-08	SAFETY INJECTION LINE BREAK INITIATING EVENT OCCURS RCPS TRIP AND CMT INJECTION IS SUCCESSFUL – 1 OF 2 CMT TRAINS FAILURE OF FULL ADS DEPRESSURIZATION
5	1.00E-08	4.15	67.38	3crvr-02	REACTOR VESSEL RUPTURE INITIATING EVENT OCCURS
6	8.44E-09	3.5	70.88	2lslo-05	SMALL LOCA INITIATING EVENT OCCURS SUCCESS OF CMT & RCP TRIP SUCCESS OF PASSIVE RHR SYSTEM SUCCESS OF FULL ADS DEPRESSURIZATION FAILURE OF NORMAL RHR IN INJECTION MODE SUCCESS OF TWO OF TWO IRWST INJECTION LINES SUCCESS OF CIS & PRE-EXISTING CONTAINMENT OPENING FAILURE OF RECIRCULATION

Table 19.59-3 (Sheet 2 of 4)
Internal Initiating Events at Power Dominant Core Damage Sequences

	Sequence Frequency	Percent Contrib	Cumulative % Contrib	Sequence Identifier	Sequence Description
7	7.35E-09	3.05	73.93	2lmlo-05	MEDIUM LOCA INITIATING EVENT OCCURS SUCCESS OF CMT & RCP TRIP SUCCESS OF FULL ADS DEPRESSURIZATION FAILURE OF NORMAL RHR IN INJECTION MODE SUCCESS OF TWO OF TWO IRWST INJECTION LINES SUCCESS OF CIS & PRE-EXISTING CONTAINMENT OPENING FAILURE OF RECIRCULATION
8	5.11E-09	2.12	76.05	3dslo-12	SMALL LOCA INITIATING EVENT OCCURS SUCCESS OF CMT & RCP TRIP SUCCESS OF PASSIVE RHR SYSTEM FAILURE OF FULL ADS DEPRESSURIZATION SUCCESS OF PARTIAL ADS DEPRESSURIZATION FAILURE OF NORMAL RHR IN INJECTION MODE
9	4.46E-09	1.85	77.90	3dmlo-12	MEDIUM LOCA INITIATING EVENT OCCURS SUCCESS OF CMT & RCP TRIP FAILURE OF FULL ADS DEPRESSURIZATION SUCCESS OF PARTIAL ADS DEPRESSURIZATION FAILURE OF NORMAL RHR IN INJECTION MODE
10	3.72E-09	1.54	79.44	2rsad-09	SPURIOUS ADS INITIATING EVENT OCCURS FAILURE OF 2/2 ACCUMULATORS
11	3.67E-09	1.52	80.96	2esad-07	SPURIOUS ADS INITIATING EVENT OCCURS SUCCESS OF 1/2 OR 2/2 ACCUMULATORS SUCCESS OF ADS & CMT FAILURE OF IRW OR CMT

Table 19.59-3 (Sheet 3 of 4)
Internal Initiating Events at Power Dominant Core Damage Sequences

	Sequence Frequency	Percent Contrib	Cumulative % Contrib	Sequence Identifier	Sequence Description
12	3.57E-09	1.48	82.44	2lsil-03	SAFETY INJECTION LINE BREAK INITIATING EVENT OCCURS RCPS TRIP AND CMT INJECTION IS SUCCESSFUL – 1 OF 2 CMT TRAINS SUCCESS OF FULL ADS DEPRESSURIZATION IRWST INJECTION IS SUCCESSFUL – 1 OF 1 TRAINS SUCCESS OF CIS & PRE-EXISTING CONTAINMENT OPENING FAILURE OF RECIRCULATION
13	3.55E-09	1.47	83.91	6esgt-41	SGTR EVENT SEQUENCE CONTINUES FAILURE OF CMT OR RCP TRIP SUCCESS OF PASSIVE RHR SYSTEM FAILURE OF FULL ADS DEPRESSURIZATION FAILURE OF PARTIAL ADS DEPRESSURIZATION
14	3.31E-09	1.37	85.28	3aatw-23	ATWS PRECURSOR WITH NO MFW EVENT SEQUENCE CONTINUES SUCCESS OF SFW OR PRHR SYSTEM SUCCESS OF MANUAL REACTOR TRIP FAILURE OF MANUAL BORATION BY CVS FAILURE OF CMT OR RCP TRIP
15	3.30E-09	1.37	86.65	2eslo-09	SMALL LOCA INITIATING EVENT OCCURS SUCCESS OF CMT & RCP TRIP SUCCESS OF PASSIVE RHR SYSTEM SUCCESS OF FULL ADS DEPRESSURIZATION FAILURE OF NORMAL RHR IN INJECTION MODE FAILURE OF TWO OF TWO IRWST INJECTION LINES

Table 19.59-3 (Sheet 4 of 4)
Internal Initiating Events at Power Dominant Core Damage Sequences

	Sequence Frequency	Percent Contrib	Cumulative % Contrib	Sequence Identifier	Sequence Description
16	2.88E-09	1.19	87.84	2emlo-09	MEDIUM LOCA INITIATING EVENT OCCURS SUCCESS OF CMT & RCP TRIP SUCCESS OF FULL ADS DEPRESSURIZATION FAILURE OF NORMAL RHR IN INJECTION MODE FAILURE OF TWO OF TWO IRWST INJECTION LINES
17	2.19E-09	0.91	88.75	6esgt-13	SGTR EVENT SEQUENCE CONTINUES SUCCESS OF CMT & RCP TRIP SUCCESS OF PASSIVE RHR SYSTEM FAILURE OF FULL ADS DEPRESSURIZATION FAILURE OF PARTIAL ADS DEPRESSURIZATION
18	1.97E-09	0.82	89.57	3dllo-08	LARGE LOCA INITIATING EVENT OCCURS ACCUMULATOR INJECTION IS SUCCESSFUL – 2 OF 2 TRAINS FAILURE OF ADS OR CMT
19	1.57E-09	0.65	90.22	2lcmt-05	CMT LINE BREAK INITIATING EVENT OCCURS RCPS TRIP AND CMT INJECTION IS SUCCESSFUL – 1 OF 2 CMT TRAINS SUCCESS OF FULL ADS DEPRESSURIZATION FAILURE OF NORMAL RHR IN INJECTION MODE SUCCESS OF TWO OF TWO IRWST INJECTION LINES SUCCESS OF CIS & PRE-EXISTING CONTAINMENT OPENING FAILURE OF RECIRCULATION

Table 19.59-4 (Sheet 1 of 3)
Sequence 1 – Safety Injection Line Break Dominant Cutsets (SI-LB-07)

NUMBER	CUTSET PROB.	PERCENTAGE	BASIC EVENT NAME		
1	5.09E-08	74.04	SAFETY INJECTION LINE BREAK INITIATING EVENT OCCURS IRWST DISCHARGE LINE “A” STRAINER PLUGGED	2.12E-04 2.40E-04	IEV-SI-LB IWA-PLUG
2	6.36E-09	9.25	SAFETY INJECTION LINE BREAK INITIATING EVENT OCCURS CCF OF 4 GRAVITY INJECTION CVs	2.12E-04 3.00E-05	IEV-SI-LB IWX-CV-AO
3	5.51E-09	8.01	SAFETY INJECTION LINE BREAK INITIATING EVENT OCCURS CCF OF 4 GRAVITY INJECTION & 2 RECIRCULATION SQUIB VALVES	2.12E-04 2.60E-05	IEV-SI-LB IWX-EV-SA
4	1.23E-09	1.79	SAFETY INJECTION LINE BREAK INITIATING EVENT OCCURS CCF OF 2 GRAVITY INJECTION SQUIB VALVES IN 1/1 LINES TO OPEN	2.12E-04 5.80E-06	IEV-SI-LB IWX-EV1-SA
5	6.49E-10	.94	SAFETY INJECTION LINE BREAK INITIATING EVENT OCCURS CHECK VALVE 122A FAILS TO OPEN CHECK VALVE 124A FAILS TO OPEN	2.12E-04 1.75E-03 1.75E-03	IEV-SI-LB IWACV122AO IWACV124AO
6	5.42E-10	.79	SAFETY INJECTION LINE BREAK INITIATING EVENT OCCURS CHECK VALVE 122A FAILS TO OPEN HARDWARE FAILURE OF VALVE 125A	2.12E-04 1.75E-03 1.46E-03	IEV-SI-LB IWACV122AO IRWMOD06
7	5.42E-10	.79	SAFETY INJECTION LINE BREAK INITIATING EVENT OCCURS HARDWARE FAILURE OF VALVE 123A CHECK VALVE 124A FAILS TO OPEN	2.12E-04 1.46E-03 1.75E-03	IEV-SI-LB IRWMOD05 IWACV124AO
8	4.52E-10	.66	SAFETY INJECTION LINE BREAK INITIATING EVENT OCCURS HARDWARE FAILURE OF VALVE 123A HARDWARE FAILURE OF VALVE 125A	2.12E-04 1.46E-03 1.46E-03	IEV-SI-LB IRWMOD05 IRWMOD06
9	3.25E-10	.47	SAFETY INJECTION LINE BREAK INITIATING EVENT OCCURS CHECK VALVE 122A FAILS TO OPEN RELAY FAILS TO OPERATE	2.12E-04 1.75E-03 8.76E-04	IEV-SI-LB IWACV122AO IWDRS125AFA
10	3.25E-10	.47	SAFETY INJECTION LINE BREAK INITIATING EVENT OCCURS CHECK VALVE 124A FAILS TO OPEN RELAY FAILS TO OPERATE	2.12E-04 1.75E-03 8.76E-04	IEV-SI-LB IWACV124AO IWBRS123AFA
11	2.71E-10	.39	SAFETY INJECTION LINE BREAK INITIATING EVENT OCCURS HARDWARE FAILURE OF VALVE 123A RELAY FAILS TO OPERATE	2.12E-04 1.46E-03 8.76E-04	IEV-SI-LB IRWMOD05 IWDRS125AFA

Table 19.59-4 (Sheet 2 of 3)
Sequence 1 – Safety Injection Line Break Dominant Cutsets (SI-LB-07)

NUMBER	CUTSET PROB.	PERCENTAGE	BASIC EVENT NAME		
12	2.71E-10	.39	SAFETY INJECTION LINE BREAK INITIATING EVENT OCCURS HARDWARE FAILURE OF VALVE 125A RELAY FAILS TO OPERATE	2.12E-04 1.46E-03 8.76E-04	IEV-SI-LB IRWMOD06 IWBRS123AFA
13	1.63E-10	.24	SAFETY INJECTION LINE BREAK INITIATING EVENT OCCURS RELAY FAILS TO OPERATE RELAY FAILS TO OPERATE	2.12E-04 8.76E-04 8.76E-04	IEV-SI-LB IWBRS123AFA IWDRS125AFA
14	1.14E-10	.17	SAFETY INJECTION LINE BREAK INITIATING EVENT OCCURS CCF OF GRAVITY INJECTION CVs IN 1/1 LINES TO OPEN	2.12E-04 5.40E-07	IEV-SI-LB IWX-CV1-AO
15	1.11E-10	.16	SAFETY INJECTION LINE BREAK INITIATING EVENT OCCURS CHECK VALVE 122A FAILS TO OPEN BUS UNAVAILABLE DUE TO TEST OR CORRECTIVE MAINTENANCE	2.12E-04 1.75E-03 3.00E-04	IEV-SI-LB IWACV122AO IDDBSDS1TM
16	1.11E-10	.16	SAFETY INJECTION LINE BREAK INITIATING EVENT OCCURS CHECK VALVE 122A FAILS TO OPEN BUS UNAVAILABLE DUE TO TEST OR CORRECTIVE MAINTENANCE	2.12E-04 1.75E-03 3.00E-04	IEV-SI-LB IWACV122AO IDDBSDD1TM
17	1.11E-10	.16	SAFETY INJECTION LINE BREAK INITIATING EVENT OCCURS CHECK VALVE 124A FAILS TO OPEN BUS UNAVAILABLE DUE TO TEST OR CORRECTIVE MAINTENANCE	2.12E-04 1.75E-03 3.00E-04	IEV-SI-LB IWACV124AO IDBBSDS1TM
18	1.11E-10	.16	SAFETY INJECTION LINE BREAK INITIATING EVENT OCCURS CHECK VALVE 124A FAILS TO OPEN BUS UNAVAILABLE DUE TO TEST OR CORRECTIVE MAINTENANCE	2.12E-04 1.75E-03 3.00E-04	IEV-SI-LB IWACV124AO IDBBSDD1TM
19	9.29E-11	.14	SAFETY INJECTION LINE BREAK INITIATING EVENT OCCURS HARDWARE FAILURE OF VALVE 123A BUS UNAVAILABLE DUE TO TEST OR CORRECTIVE MAINTENANCE	2.12E-04 1.46E-03 3.00E-04	IEV-SI-LB IRWMOD05 IDDBSDS1TM
20	9.29E-11	.14	SAFETY INJECTION LINE BREAK INITIATING EVENT OCCURS HARDWARE FAILURE OF VALVE 123A BUS UNAVAILABLE DUE TO TEST OR CORRECTIVE MAINTENANCE	2.12E-04 1.46E-03 3.00E-04	IEV-SI-LB IRWMOD05 IDDBSDD1TM
21	9.29E-11	.14	SAFETY INJECTION LINE BREAK INITIATING EVENT OCCURS HARDWARE FAILURE OF VALVE 125A BUS UNAVAILABLE DUE TO TEST OR CORRECTIVE MAINTENANCE	2.12E-04 1.46E-03 3.00E-04	IEV-SI-LB IRWMOD06 IDBBSDS1TM

Table 19.59-4 (Sheet 3 of 3)
Sequence 1 – Safety Injection Line Break Dominant Cutsets (SI-LB-07)

NUMBER	CUTSET PROB.	PERCENTAGE	BASIC EVENT NAME		
22	9.29E-11	.14	SAFETY INJECTION LINE BREAK INITIATING EVENT OCCURS HARDWARE FAILURE OF VALVE 125A BUS UNAVAILABLE DUE TO TEST OR CORRECTIVE MAINTENANCE	2.12E-04 1.46E-03 3.00E-04	IEV-SI-LB IRWMOD06 IDBBSDD1TM
23	5.57E-11	.08	SAFETY INJECTION LINE BREAK INITIATING EVENT OCCURS RELAY FAILS TO OPERATE BUS UNAVAILABLE DUE TO TEST OR CORRECTIVE MAINTENANCE	2.12E-04 8.76E-04 3.00E-04	IEV-SI-LB IWDRS125AFA IDBBSDS1TM
24	5.57E-11	.08	SAFETY INJECTION LINE BREAK INITIATING EVENT OCCURS RELAY FAILS TO OPERATE BUS UNAVAILABLE DUE TO TEST OR CORRECTIVE MAINTENANCE	2.12E-04 8.76E-04 3.00E-04	IEV-SI-LB IWDRS125AFA IDBBSDD1TM
25	5.57E-11	.08	SAFETY INJECTION LINE BREAK INITIATING EVENT OCCURS RELAY FAILS TO OPERATE BUS UNAVAILABLE DUE TO TEST OR CORRECTIVE MAINTENANCE	2.12E-04 8.76E-04 3.00E-04	IEV-SI-LB IWBRS123AFA IDDBSDS1TM

Table 19.59-5
Sequence 2 – Large LOCA Dominant Cutsets (LLOCA-09)

NUMBER	CUTSET PROB.	PERCENTAGE	BASIC EVENT NAME		
1	8.75E-09	20.55	LARGE LOCA INITIATING EVENT OCCURS CHECK VALVE 029A FAILS TO OPEN	5.00E-06 1.75E-03	IEV-LLOCA ACACV029GO
2	8.75E-09	20.55	LARGE LOCA INITIATING EVENT OCCURS CHECK VALVE 028A FAILS TO OPEN	5.00E-06 1.75E-03	IEV-LLOCA ACACV028GO
3	8.75E-09	20.55	LARGE LOCA INITIATING EVENT OCCURS CHECK VALVE 029B FAILS TO OPEN	5.00E-06 1.75E-03	IEV-LLOCA ACBCV029GO
4	8.75E-09	20.55	LARGE LOCA INITIATING EVENT OCCURS CHECK VALVE 028B FAILS TO OPEN	5.00E-06 1.75E-03	IEV-LLOCA ACBCV028GO
5	3.64E-09	8.55	LARGE LOCA INITIATING EVENT OCCURS FLOW TUNING ORIFICE PLUGS	5.00E-06 7.27E-04	IEV-LLOCA ACAOR001SP
6	3.64E-09	8.55	LARGE LOCA INITIATING EVENT OCCURS FLOW TUNING ORIFICE PLUGS	5.00E-06 7.27E-04	IEV-LLOCA ACBOR001SP
7	2.55E-10	.60	LARGE LOCA INITIATING EVENT OCCURS COMMON CAUSE FAILURE OF 2 ACCUMULATOR CHECK VALVES	5.00E-06 5.10E-05	IEV-LLOCA ACX-CV-GO
8	1.20E-11	.03	LARGE LOCA INITIATING EVENT OCCURS ACCUMULATOR TANK A (T001A) RUPTURES	5.00E-06 2.40E-06	IEV-LLOCA ACATK001AF
9	1.20E-11	.03	LARGE LOCA INITIATING EVENT OCCURS ACCUMULATOR TANK B (T001B) RUPTURES	5.00E-06 2.40E-06	IEV-LLOCA ACBTK001AF
10	3.60E-12	.01	LARGE LOCA INITIATING EVENT OCCURS FLOW TUNING ORIFICE RUPTURE	5.00E-06 7.20E-07	IEV-LLOCA ACAOR001EB
11	3.60E-12	.01	LARGE LOCA INITIATING EVENT OCCURS FLOW TUNING ORIFICE RUPTURE	5.00E-06 7.20E-07	IEV-LLOCA ACBOR001EB
12	6.00E-13	.00	LARGE LOCA INITIATING EVENT OCCURS COMMON CAUSE FAILURE OF ACCUMULATOR TANKS	5.00E-06 1.20E-07	IEV-LLOCA ACX-TK-AF

Table 19.59-6 (Sheet 1 of 3)
Sequence 3 – Spurious ADS Actuation Dominant Cutsets (SPADS-08)

NUMBER	CUTSET PROB.	PERCENTAGE	BASIC EVENT NAME		
1	5.56E-09	26.14	SPURIOUS ADS INITIATING EVENT OCCURS CCF OF ESF INPUT LOGIC (HARDWARE)	5.40E-05 1.03E-04	IEV-SPADS CCX-INPUT-LOGIC
2	3.35E-09	15.75	SPURIOUS ADS INITIATING EVENT OCCURS COMMON CAUSE FAILURE OF 4 AOVS TO OPEN	5.40E-05 6.20E-05	IEV-SPADS CCX-AV-LA
3	3.19E-09	15.00	SPURIOUS ADS INITIATING EVENT OCCURS CCF OF 2 SQUIB VALVES TO OPERATE	5.40E-05 5.90E-05	IEV-SPADS ADX-EV-SA2
4	2.75E-09	12.93	SPURIOUS ADS INITIATING EVENT OCCURS COMMON CAUSE FAILURE OF 4 CHECK VALVES TO OPEN	5.40E-05 5.10E-05	IEV-SPADS CMX-CV-GO
5	2.07E-09	9.73	SPURIOUS ADS INITIATING EVENT OCCURS CCF OF RTD LEVEL TRANSMITTERS	5.40E-05 3.84E-05	IEV-SPADS CMX-VS-FA
6	1.62E-09	7.62	SPURIOUS ADS INITIATING EVENT OCCURS DUE TO CCF OF 4TH STAGE ADS SQUIB VALVES TO OPERATE	5.40E-05 3.00E-05	IEV-SPADS ADX-EV-SA
7	5.94E-10	2.79	SPURIOUS ADS INITIATING EVENT OCCURS CCF OF ESF INPUT LOGIC SOFTWARE	5.40E-05 1.10E-05	IEV-SPADS CCX-IN-LOGIC-SW
8	5.94E-10	2.79	SPURIOUS ADS INITIATING EVENT OCCURS CCF OF PMS ESF ACTUATION LOGIC SOFTWARE	5.40E-05 1.10E-05	IEV-SPADS CCX-PMXMOD2-SW
9	5.94E-10	2.79	SPURIOUS ADS INITIATING EVENT OCCURS CCF OF PMS ESF OUTPUT LOGIC SOFTWARE	5.40E-05 1.10E-05	IEV-SPADS CCX-PMXMOD1-SW
10	4.65E-10	2.19	SPURIOUS ADS INITIATING EVENT OCCURS CCF OF EPO BOARDS IN PMS	5.40E-05 8.62E-06	IEV-SPADS CCX-EP-SAM
11	6.48E-11	.30	SPURIOUS ADS INITIATING EVENT OCCURS SOFTWARE CCF OF ALL CARDS	5.40E-05 1.20E-06	IEV-SPADS CCX-SFTW
12	2.85E-11	.13	SPURIOUS ADS INITIATING EVENT OCCURS FLOW TUNING ORIFICE PLUGS FLOW TUNING ORIFICE PLUGS	5.40E-05 7.27E-04 7.27E-04	IEV-SPADS CMA-PLUG CMB-PLUG
13	1.82E-11	.09	SPURIOUS ADS INITIATING EVENT OCCURS HARDWARE FAILURE OF ST. #4 LINE 3 HARDWARE FAILURE OF ST. #4 LINE 4	5.40E-05 5.80E-04 5.80E-04	IEV-SPADS AD4MOD09 AD4MOD10

Table 19.59-6 (Sheet 2 of 3)
Sequence 3 – Spurious ADS Actuation Dominant Cutsets (SPADS-08)

NUMBER	CUTSET PROB.	PERCENTAGE	BASIC EVENT NAME		
14	1.82E-11	.09	SPURIOUS ADS INITIATING EVENT OCCURS HARDWARE FAILURE OF ST. #4 LINE 2 HARDWARE FAILURE OF ST. #4 LINE 4	5.40E-05 5.80E-04 5.80E-04	IEV-SPADS AD4MOD08 AD4MOD10
15	1.82E-11	.09	SPURIOUS ADS INITIATING EVENT OCCURS HARDWARE FAILURE OF ST. #4 LINE 2 HARDWARE FAILURE OF ST. #4 LINE 3	5.40E-05 5.80E-04 5.80E-04	IEV-SPADS AD4MOD08 AD4MOD09
16	1.82E-11	.09	SPURIOUS ADS INITIATING EVENT OCCURS HARDWARE FAILURE OF ST. #4 LINE 1 HARDWARE FAILURE OF ST. #4 LINE 4	5.40E-05 5.80E-04 5.80E-04	IEV-SPADS AD4MOD07 AD4MOD10
17	1.82E-11	.09	SPURIOUS ADS INITIATING EVENT OCCURS HARDWARE FAILURE OF ST. #4 LINE 1 HARDWARE FAILURE OF ST. #4 LINE 3	5.40E-05 5.80E-04 5.80E-04	IEV-SPADS AD4MOD07 AD4MOD09
18	1.82E-11	.09	SPURIOUS ADS INITIATING EVENT OCCURS HARDWARE FAILURE OF ST. #4 LINE 1 HARDWARE FAILURE OF ST. #4 LINE 2	5.40E-05 5.80E-04 5.80E-04	IEV-SPADS AD4MOD07 AD4MOD08
19	6.85E-12	.03	SPURIOUS ADS INITIATING EVENT OCCURS COMMON CAUSE FAILURE OF THE BATTERIES IDSA-DB-1A/1B UNAVAILABILITY OF BUS ECS ES 2 DUE TO UNSCHEDULED MAINTENANCE	5.40E-05 4.70E-05 2.70E-03	IEV-SPADS CCX-BY-PN EC2BS002TM
20	6.85E-12	.03	SPURIOUS ADS INITIATING EVENT OCCURS COMMON CAUSE FAILURE OF THE BATTERIES IDSA-DB-1A/1B BUS UNAVAILABLE DUE TO UNSCHEDULED MAINTENANCE	5.40E-05 4.70E-05 2.70E-03	IEV-SPADS CCX-BY-PN EC2BS022TM
21	6.85E-12	.03	SPURIOUS ADS INITIATING EVENT OCCURS COMMON CAUSE FAILURE OF THE BATTERIES IDSA-DB-1A/1B BUS UNAVAILABLE DUE TO UNSCHEDULED MAINTENANCE	5.40E-05 4.70E-05 2.70E-03	IEV-SPADS CCX-BY-PN EC2BS221TM
22	6.85E-12	.03	SPURIOUS ADS INITIATING EVENT OCCURS COMMON CAUSE FAILURE OF THE BATTERIES IDSA-DB-1A/1B UNAVAILABILITY OF BUS ECS ES 1 DUE TO UNSCHEDULED MAINTENANCE	5.40E-05 4.70E-05 2.70E-03	IEV-SPADS CCX-BY-PN EC1BS001TM
23	6.85E-12	.03	SPURIOUS ADS INITIATING EVENT OCCURS COMMON CAUSE FAILURE OF THE BATTERIES IDSA-DB-1A/1B BUS UNAVAILABLE DUE TO UNSCHEDULED MAINTENANCE	5.40E-05 4.70E-05 2.70E-03	IEV-SPADS CCX-BY-PN EC1BS012TM

Table 19.59-6 (Sheet 3 of 3)
Sequence 3 – Spurious ADS Actuation Dominant Cutsets (SPADS-08)

NUMBER	CUTSET PROB.	PERCENTAGE	BASIC EVENT NAME		
24	6.85E-12	.03	SPURIOUS ADS INITIATING EVENT OCCURS COMMON CAUSE FAILURE OF THE BATTERIES IDSA-DB-1A/1B BUS UNAVAILABLE DUE TO UNSCHEDULED MAINTENANCE	5.40E-05 4.70E-05 2.70E-03	IEV-SPADS CCX-BY-PN EC1BS121TM
25	6.83E-12	.03	SPURIOUS ADS INITIATING EVENT OCCURS PMBMOD32 PMCMOD33 PMDMOD34	5.40E-05 5.02E-03 5.02E-03 5.02E-03	IEV-SPADS PMBMOD32 PMCMOD33 PMDMOD34

Table 19.59-7 (Sheet 1 of 3)
Sequence 4 – Safety Injection Line Break Dominant Cutsets (SI-LB-08)

NUMBER	CUTSET PROB.	PERCENTAGE	BASIC EVENT NAME		
1	1.25E-08	63.00	SAFETY INJECTION LINE BREAK INITIATING EVENT OCCURS CCF OF 2 SQUIB VALVES TO OPERATE	2.12E-04 5.90E-05	IEV-SI-LB ADX-EV-SA2
2	6.36E-09	32.06	SAFETY INJECTION LINE BREAK INITIATING EVENT OCCURS DUE TO CCF OF 4TH STAGE ADS SQUIB VALVES TO OPERATE	2.12E-04 3.00E-05	IEV-SI-LB ADX-EV-SA
3	7.13E-11	.36	SAFETY INJECTION LINE BREAK INITIATING EVENT OCCURS HARDWARE FAILURE OF ST. #4 LINE 3 HARDWARE FAILURE OF ST. #4 LINE 4	2.12E-04 5.80E-04 5.80E-04	IEV-SI-LB AD4MOD09 AD4MOD10
4	7.13E-11	.36	SAFETY INJECTION LINE BREAK INITIATING EVENT OCCURS HARDWARE FAILURE OF ST. #4 LINE 2 HARDWARE FAILURE OF ST. #4 LINE 4	2.12E-04 5.80E-04 5.80E-04	IEV-SI-LB AD4MOD08 AD4MOD10
5	7.13E-11	.36	SAFETY INJECTION LINE BREAK INITIATING EVENT OCCURS HARDWARE FAILURE OF ST. #4 LINE 2 HARDWARE FAILURE OF ST. #4 LINE 3	2.12E-04 5.80E-04 5.80E-04	IEV-SI-LB AD4MOD08 AD4MOD09
6	7.13E-11	.36	SAFETY INJECTION LINE BREAK INITIATING EVENT OCCURS HARDWARE FAILURE OF ST. #4 LINE 1 HARDWARE FAILURE OF ST. #4 LINE 4	2.12E-04 5.80E-04 5.80E-04	IEV-SI-LB AD4MOD07 AD4MOD10
7	7.13E-11	.36	SAFETY INJECTION LINE BREAK INITIATING EVENT OCCURS HARDWARE FAILURE OF ST. #4 LINE 1 HARDWARE FAILURE OF ST. #4 LINE 3	2.12E-04 5.80E-04 5.80E-04	IEV-SI-LB AD4MOD07 AD4MOD09
8	7.13E-11	.36	SAFETY INJECTION LINE BREAK INITIATING EVENT OCCURS HARDWARE FAILURE OF ST. #4 LINE 1 HARDWARE FAILURE OF ST. #4 LINE 2	2.12E-04 5.80E-04 5.80E-04	IEV-SI-LB AD4MOD07 AD4MOD08
9	3.65E-11	.18	SAFETY INJECTION LINE BREAK INITIATING EVENT OCCURS COND. PROB. OF REC-MANDAS (FAILURE OF MANUAL DAS AC OPER. FAILS TO RECOG. THE NEED FOR RCS DEPRESS. DURING MLOCA CCF OF ESF INPUT LOGIC (HARDWARE)	2.12E-04 5.06E-01 3.30E-03 1.03E-04	IEV-SI-LB REC-MANDASC LPM-MAN02 CCX-INPUT-LOGIC
10	3.34E-11	.17	SAFETY INJECTION LINE BREAK INITIATING EVENT OCCURS COND. PROB. OF REC-MANDAS (FAILURE OF MANUAL DAS AC OPER. FAILS TO FULFIL MANUAL ACTUATION OF ADS CCF OF ESF INPUT LOGIC (HARDWARE)	2.12E-04 5.06E-01 3.02E-03 1.03E-04	IEV-SI-LB REC-MANDASC ADN-MAN01 CCX-INPUT-LOGIC

Table 19.59-7 (Sheet 2 of 3)
Sequence 4 – Safety Injection Line Break Dominant Cutsets (SI-LB-08)

NUMBER	CUTSET PROB.	PERCENTAGE	BASIC EVENT NAME		
11	2.71E-11	.14	SAFETY INJECTION LINE BREAK INITIATING EVENT OCCURS FAILURE OF MANUAL DAS ACT. CCF OF PMS ESF OUTPUT LOGIC SOFTWARE	2.12E-04 1.16E-02 1.10E-05	IEV-SI-LB REC-MANDAS CCX-PMXMOD1-SW
12	2.69E-11	.14	SAFETY INJECTION LINE BREAK INITIATING EVENT OCCURS COMMON CAUSE FAILURE OF THE BATTERIES IDSA-DB-1A/1B UNAVAILABILITY OF BUS ECS ES 2 DUE TO UNSCHEDUL MAINTENANCE	2.12E-04 4.70E-05 2.70E-03	IEV-SI-LB CCX-BY-PN EC2BS002TM
13	2.69E-11	.14	SAFETY INJECTION LINE BREAK INITIATING EVENT OCCURS COMMON CAUSE FAILURE OF THE BATTERIES IDSA-DB-1A/1B BUS UNAVAILABLE DUE TO UNSCHEDULED MAINTENANCE	2.12E-04 4.70E-05 2.70E-03	IEV-SI-LB CCX-BY-PN EC2BS022TM
14	2.69E-11	.14	SAFETY INJECTION LINE BREAK INITIATING EVENT OCCURS COMMON CAUSE FAILURE OF THE BATTERIES IDSA-DB-1A/1B BUS UNAVAILABLE DUE TO UNSCHEDULED MAINTENANCE	2.12E-04 4.70E-05 2.70E-03	IEV-SI-LB CCX-BY-PN EC2BS221TM
15	2.69E-11	.14	SAFETY INJECTION LINE BREAK INITIATING EVENT OCCURS COMMON CAUSE FAILURE OF THE BATTERIES IDSA-DB-1A/1B UNAVAILABILITY OF BUS ECS ES 1 DUE TO UNSCHEDULED MAINTENANCE	2.12E-04 4.70E-05 2.70E-03	IEV-SI-LB CCX-BY-PN EC1BS001TM
16	2.69E-11	.14	SAFETY INJECTION LINE BREAK INITIATING EVENT OCCURS COMMON CAUSE FAILURE OF THE BATTERIES IDSA-DB-1A/1B BUS UNAVAILABLE DUE TO UNSCHEDULED MAINTENANCE	2.12E-04 4.70E-05 2.70E-03	IEV-SI-LB CCX-BY-PN EC1BS012TM
17	2.69E-11	.14	SAFETY INJECTION LINE BREAK INITIATING EVENT OCCURS COMMON CAUSE FAILURE OF THE BATTERIES IDSA-DB-1A/1B BUS UNAVAILABLE DUE TO UNSCHEDULED MAINTENANCE	2.12E-04 4.70E-05 2.70E-03	IEV-SI-LB CCX-BY-PN EC1BS121TM
18	2.33E-11	.12	SAFETY INJECTION LINE BREAK INITIATING EVENT OCCURS FAILURE OF MANUAL DAS REACTOR TRIP HARDWARE CCF OF PMS ESF OUTPUT LOGIC SOFTWARE	2.12E-04 1.00E-02 1.10E-05	IEV-SI-LB MDAS CCX-PMXMOD1-SW
19	2.12E-11	.11	SAFETY INJECTION LINE BREAK INITIATING EVENT OCCURS FAILURE OF MANUAL DAS ACT. CCF OF EPO BOARDS IN PMS	2.12E-04 1.16E-02 8.62E-06	IEV-SI-LB REC-MANDAS CCX-EP-SAM
20	1.91E-11	.10	SAFETY INJECTION LINE BREAK INITIATING EVENT OCCURS BUS UNAVAILABLE DUE TO TEST OR CORRECTIVE MAINTENANCE BUS UNAVAILABLE DUE TO TEST OR CORRECTIVE MAINTENANCE	2.12E-04 3.00E-04 3.00E-04	IEV-SI-LB IDDBSDS1TM IDBBSDS1TM

Table 19.59-7 (Sheet 3 of 3)
Sequence 4 – Safety Injection Line Break Dominant Cutsets (SI-LB-08)

NUMBER	CUTSET PROB.	PERCENTAGE	BASIC EVENT NAME		
21	1.91E-11	.10	SAFETY INJECTION LINE BREAK INITIATING EVENT OCCURS BUS UNAVAILABLE DUE TO TEST OR CORRECTIVE MAINTENANCE BUS UNAVAILABLE DUE TO TEST OR CORRECTIVE MAINTENANCE	2.12E-04 3.00E-04 3.00E-04	IEV-SI-LB IDDBSDS1TM IDBBSDD1TM
22	1.91E-11	.10	SAFETY INJECTION LINE BREAK INITIATING EVENT OCCURS BUS UNAVAILABLE DUE TO TEST OR CORRECTIVE MAINTENANCE BUS UNAVAILABLE DUE TO TEST OR CORRECTIVE MAINTENANCE	2.12E-04 3.00E-04 3.00E-04	IEV-SI-LB IDDBSDD1TM IDBBSDS1TM
23	1.91E-11	.10	SAFETY INJECTION LINE BREAK INITIATING EVENT OCCURS BUS UNAVAILABLE DUE TO TEST OR CORRECTIVE MAINTENANCE BUS UNAVAILABLE DUE TO TEST OR CORRECTIVE MAINTENANCE	2.12E-04 3.00E-04 3.00E-04	IEV-SI-LB IDDBSDD1TM IDBBSDD1TM
24	1.91E-11	.10	SAFETY INJECTION LINE BREAK INITIATING EVENT OCCURS BUS UNAVAILABLE DUE TO TEST OR CORRECTIVE MAINTENANCE BUS UNAVAILABLE DUE TO TEST OR CORRECTIVE MAINTENANCE	2.12E-04 3.00E-04 3.00E-04	IEV-SI-LB IDCBSDS1TM IDABSDS1TM
25	1.91E-11	.10	SAFETY INJECTION LINE BREAK INITIATING EVENT OCCURS BUS UNAVAILABLE DUE TO TEST OR CORRECTIVE MAINTENANCE BUS UNAVAILABLE DUE TO TEST OR CORRECTIVE MAINTENANCE	2.12E-04 3.00E-04 3.00E-04	IEV-SI-LB IDCBSDS1TM IDABSDD1TM

Table 19.59-8
Sequence 5 – Reactor Vessel Rupture Cutset (RV-RP-02)

NUMBER	CUTSET PROB.	PERCENTAGE	BASIC EVENT NAME		
1	1.00E-08	100.00	REACTOR VESSEL RUPTURE INITIATING EVENT OCCURS	1.00E-08	IEV-RV-RP

Table 19.59-9 (Sheet 1 of 3)
Sequence 6 – Small LOCA Dominant Cutsets (SLOCA-05)

NUMBER	CUTSET PROB.	PERCENTAGE	BASIC EVENT NAME		
1	6.00E-09	71.10	SMALL LOCA INITIATING EVENT OCCURS PLUGGING OF BOTH RECIRC LINES DUE TO CCF OF SUMP SCREENS	5.00E-04 1.20E-05	IEV-SLOCA REX-FL-GP
2	2.39E-09	28.32	SMALL LOCA INITIATING EVENT OCCURS CCF OF TANK LEVEL TRANSMITTERS OPER. FAILS TO ACT. SUMP RECIRC GIVEN IRW LEVEL SIGNAL FAILUR	5.00E-04 4.78E-04 1.00E-02	IEV-SLOCA IWX-XMTR REN-MAN04
3	2.88E-11	.34	SMALL LOCA INITIATING EVENT OCCURS SUMP SCREEN A PLUGS AND PREVENTS FLOW SUMP SCREEN B PLUGS AND PREVENTS FLOW	5.00E-04 2.40E-04 2.40E-04	IEV-SLOCA REA-PLUG REB-PLUG
4	9.18E-12	.11	SMALL LOCA INITIATING EVENT OCCURS CCF OF TANK LEVEL TRANSMITTERS CCF OF CMT LEVEL SWITCHES	5.00E-04 4.78E-04 3.84E-05	IEV-SLOCA IWX-XMTR CCX-VS-FA
5	2.63E-12	.03	SMALL LOCA INITIATING EVENT OCCURS CCF OF PMS ESF OUTPUT LOGIC SOFTWARE CCF OF TANK LEVEL TRANSMITTERS	5.00E-04 1.10E-05 4.78E-04	IEV-SLOCA CCX-PMXMOD1-SW IWX-XMTR
6	2.63E-12	.03	SMALL LOCA INITIATING EVENT OCCURS CCX-PMXMOD4-SW CCF OF TANK LEVEL TRANSMITTERS	5.00E-04 1.10E-05 4.78E-04	IEV-SLOCA CCX-PMXMOD4-SW IWX-XMTR
7	2.06E-12	.02	SMALL LOCA INITIATING EVENT OCCURS CCF OF EPO BOARDS IN PMS CCF OF TANK LEVEL TRANSMITTERS	5.00E-04 8.62E-06 4.78E-04	IEV-SLOCA CCX-EP-SAM IWX-XMTR
8	3.07E-13	.00	SMALL LOCA INITIATING EVENT OCCURS HARDWARE FAILURE CAUSE RECIRC. CV 119A FAILS TO OPEN SUMP SCREEN B PLUGS AND PREVENTS FLOW HARDWARE FAILURE OF SQUIB VALVE 118A	5.00E-04 1.75E-03 2.40E-04 1.46E-03	IEV-SLOCA REACV119GO REB-PLUG IRWMOD09
9	3.07E-13	.00	SMALL LOCA INITIATING EVENT OCCURS HARDWARE FAILURE CAUSE RECIRC. CV 119B FAILS TO OPEN SUMP SCREEN A PLUGS AND PREVENTS FLOW HARDWARE FAILURE OF SQUIB VALVE 118B	5.00E-04 1.75E-03 2.40E-04 1.46E-03	IEV-SLOCA REBCV119GO REA-PLUG IRWMOD11
10	2.87E-13	.00	SMALL LOCA INITIATING EVENT OCCURS SOFTWARE CCF OF ALL CARDS CCF OF TANK LEVEL TRANSMITTERS	5.00E-04 1.20E-06 4.78E-04	IEV-SLOCA CCX-SFTW IWX-XMTR

Table 19.59-9 (Sheet 2 of 3)
Sequence 6 – Small LOCA Dominant Cutsets (SLOCA-05)

NUMBER	CUTSET PROB.	PERCENTAGE	BASIC EVENT NAME		
11	2.56E-13	.00	SMALL LOCA INITIATING EVENT OCCURS	5.00E-04	IEV-SLOCA
			HARDWARE FAILURE OF SQUIB VALVE 120A	1.46E-03	IRWMOD10
			SUMP SCREEN B PLUGS AND PREVENTS FLOW	2.40E-04	REB-PLUG
			HARDWARE FAILURE OF SQUIB VALVE 118A	1.46E-03	IRWMOD09
12	2.56E-13	.00	SMALL LOCA INITIATING EVENT OCCURS	5.00E-04	IEV-SLOCA
			HARDWARE FAILURE OF SQUIB VALVE 120B	1.46E-03	IRWMOD12
			SUMP SCREEN A PLUGS AND PREVENTS FLOW	2.40E-04	REA-PLUG
			HARDWARE FAILURE OF SQUIB VALVE 118B	1.46E-03	IRWMOD11
13	2.39E-13	.00	SMALL LOCA INITIATING EVENT OCCURS	5.00E-04	IEV-SLOCA
			INDICATION FAILURE	1.00E-06	ALL-IND-FAIL
			CCF OF TANK LEVEL TRANSMITTERS	4.78E-04	IWX-XMTR
14	1.84E-13	.00	SMALL LOCA INITIATING EVENT OCCURS	5.00E-04	IEV-SLOCA
			HARDWARE FAILURE CAUSE RECIRC. CV 119A FAILS TO OPEN	1.75E-03	REACV119GO
			SUMP SCREEN B PLUGS AND PREVENTS FLOW	2.40E-04	REB-PLUG
			RELAY FAILS TO OPERATE	8.76E-04	IWBRS118AFA
15	1.84E-13	.00	SMALL LOCA INITIATING EVENT OCCURS	5.00E-04	IEV-SLOCA
			HARDWARE FAILURE CAUSE RECIRC. CV 119B FAILS TO OPEN	1.75E-03	REBCV119GO
			SUMP SCREEN A PLUGS AND PREVENTS FLOW	2.40E-04	REA-PLUG
			RELAY FAILS TO OPERATE	8.76E-04	IWARS118BFA
16	1.68E-13	.00	SMALL LOCA INITIATING EVENT OCCURS	5.00E-04	IEV-SLOCA
			CCF OF 2 OUT 2 LOW PRESSURE RECIRCULATION SQUIB VALVES	5.80E-05	IWX-EV4-SA
			CCF OF MOV 120A AND 120B	5.80E-06	IWX-EV2-SA
17	1.53E-13	.00	SMALL LOCA INITIATING EVENT OCCURS	5.00E-04	IEV-SLOCA
			HARDWARE FAILURE OF SQUIB VALVE 120A	1.46E-03	IRWMOD10
			SUMP SCREEN B PLUGS AND PREVENTS FLOW	2.40E-04	REB-PLUG
			RELAY FAILS TO OPERATE	8.76E-04	IWBRS118AFA
18	1.53E-13	.00	SMALL LOCA INITIATING EVENT OCCURS	5.00E-04	IEV-SLOCA
			HARDWARE FAILURE OF SQUIB VALVE 118A	1.46E-03	IRWMOD09
			SUMP SCREEN B PLUGS AND PREVENTS FLOW	2.40E-04	REB-PLUG
			RELAY FAILS TO OPERATE	8.76E-04	IWDRS120AFA

Table 19.59-9 (Sheet 3 of 3)
Sequence 6 – Small LOCA Dominant Cutsets (SLOCA-05)

NUMBER	CUTSET PROB.	PERCENTAGE	BASIC EVENT NAME		
19	1.53E-13	.00	SMALL LOCA INITIATING EVENT OCCURS	5.00E-04	IEV-SLOCA
			HARDWARE FAILURE OF SQUIB VALVE 120B	1.46E-03	IRWMOD12
			SUMP SCREEN A PLUGS AND PREVENTS FLOW	2.40E-04	REA-PLUG
			RELAY FAILS TO OPERATE	8.76E-04	IWARS118BFA
20	1.53E-13	.00	SMALL LOCA INITIATING EVENT OCCURS	5.00E-04	IEV-SLOCA
			HARDWARE FAILURE OF SQUIB VALVE 118B	1.46E-03	IRWMOD11
			SUMP SCREEN A PLUGS AND PREVENTS FLOW	2.40E-04	REA-PLUG
			RELAY FAILS TO OPERATE	8.76E-04	IWCRS120BFA
21	9.21E-14	.00	SMALL LOCA INITIATING EVENT OCCURS	5.00E-04	IEV-SLOCA
			RELAY FAILS TO OPERATE	8.76E-04	IWDRS120AFA
			SUMP SCREEN B PLUGS AND PREVENTS FLOW	2.40E-04	REB-PLUG
			RELAY FAILS TO OPERATE	8.76E-04	IWBRS118AFA
22	9.21E-14	.00	SMALL LOCA INITIATING EVENT OCCURS	5.00E-04	IEV-SLOCA
			RELAY FAILS TO OPERATE	8.76E-04	IWCRS120BFA
			SUMP SCREEN A PLUGS AND PREVENTS FLOW	2.40E-04	REA-PLUG
			RELAY FAILS TO OPERATE	8.76E-04	IWARS118BFA
23	8.88E-14	.00	SMALL LOCA INITIATING EVENT OCCURS	5.00E-04	IEV-SLOCA
			HARDWARE FAILURE CAUSE RECIRC. CV 119B FAILS TO OPEN	1.75E-03	REBCV119GO
			CCF OF 2 OUT 2 LOW PRESSURE RECIRCULATION SQUIB VALVES	5.80E-05	IWX-EV4-SA
			HARDWARE FAILURE CAUSE RECIRC. CV 119A FAILS TO OPEN	1.75E-03	REACV119GO
24	7.41E-14	.00	SMALL LOCA INITIATING EVENT OCCURS	5.00E-04	IEV-SLOCA
			HARDWARE FAILURE CAUSE RECIRC. CV 119B FAILS TO OPEN	1.75E-03	REBCV119GO
			CCF OF 2 OUT 2 LOW PRESSURE RECIRCULATION SQUIB VALVES	5.80E-05	IWX-EV4-SA
			HARDWARE FAILURE OF SQUIB VALVE 120A	1.46E-03	IRWMOD10
25	7.41E-14	.00	SMALL LOCA INITIATING EVENT OCCURS	5.00E-04	IEV-SLOCA
			HARDWARE FAILURE CAUSE RECIRC. CV 119A FAILS TO OPEN	1.75E-03	REACV119GO
			CCF OF 2 OUT 2 LOW PRESSURE RECIRCULATION SQUIB VALVES	5.80E-05	IWX-EV4-SA
			HARDWARE FAILURE OF SQUIB VALVE 120B	1.46E-03	IRWMOD12

Table 19.59-10 (Sheet 1 of 3)
Sequence 7 – Medium LOCA Dominant Cutsets (MLOCA-05)

NUMBER	CUTSET PROB.	PERCENTAGE	BASIC EVENT NAME		
1	5.23E-09	71.13	MEDIUM LOCA INITIATING EVENT OCCURS PLUGGING OF BOTH RECIRC LINES DUE TO CCF OF SUMP SCREENS	4.36E-04 1.20E-05	IEV-MLOCA REX-FL-GP
2	2.08E-09	28.29	MEDIUM LOCA INITIATING EVENT OCCURS CCF OF TANK LEVEL TRANSMITTERS OPER. FAILS TO ACT. SUMP RECIRC GIVEN IRW LEVEL SIGNAL FAILUR	4.36E-04 4.78E-04 1.00E-02	IEV-MLOCA IWX-XMTR REN-MAN04
3	2.51E-11	.34	MEDIUM LOCA INITIATING EVENT OCCURS SUMP SCREEN A PLUGS AND PREVENTS FLOW SUMP SCREEN B PLUGS AND PREVENTS FLOW	4.36E-04 2.40E-04 2.40E-04	IEV-MLOCA REA-PLUG REB-PLUG
4	8.00E-12	.11	MEDIUM LOCA INITIATING EVENT OCCURS CCF OF TANK LEVEL TRANSMITTERS CCX-VS-FA	4.36E-04 4.78E-04 3.84E-05	IEV-MLOCA IWX-XMTR CCX-VS-FA
5	2.29E-12	.03	MEDIUM LOCA INITIATING EVENT OCCURS CCF OF PMS ESF OUTPUT LOGIC SOFTWARE CCF OF TANK LEVEL TRANSMITTERS	4.36E-04 1.10E-05 4.78E-04	IEV-MLOCA CCX-PMXMOD1-SW IWX-XMTR
6	2.29E-12	.03	MEDIUM LOCA INITIATING EVENT OCCURS CCX-PMXMOD4-SW CCF OF TANK LEVEL TRANSMITTERS	4.36E-04 1.10E-05 4.78E-04	IEV-MLOCA CCX-PMXMOD4-SW IWX-XMTR
7	1.80E-12	.02	MEDIUM LOCA INITIATING EVENT OCCURS CCF OF EPO BOARDS IN PMS CCF OF TANK LEVEL TRANSMITTERS	4.36E-04 8.62E-06 4.78E-04	IEV-MLOCA CCX-EP-SAM IWX-XMTR
8	2.67E-13	.00	MEDIUM LOCA INITIATING EVENT OCCURS HARDWARE FAILURE CAUSE RECIRC. CV 119A FAILS TO OPEN SUMP SCREEN B PLUGS AND PREVENTS FLOW HARDWARE FAILURE OF SQUIB VALVE 118A	4.36E-04 1.75E-03 2.40E-04 1.46E-03	IEV-MLOCA REACV119GO REB-PLUG IRWMOD09
9	2.67E-13	.00	MEDIUM LOCA INITIATING EVENT OCCURS HARDWARE FAILURE CAUSE RECIRC. CV 119B FAILS TO OPEN SUMP SCREEN A PLUGS AND PREVENTS FLOW HARDWARE FAILURE OF SQUIB VALVE 118B	4.36E-04 1.75E-03 2.40E-04 1.46E-03	IEV-MLOCA REBCV119GO REA-PLUG IRWMOD11
10	2.50E-13	.00	MEDIUM LOCA INITIATING EVENT OCCURS SOFTWARE CCF OF ALL CARDS CCF OF TANK LEVEL TRANSMITTERS	4.36E-04 1.20E-06 4.78E-04	IEV-MLOCA CCX-SFTW IWX-XMTR

Table 19.59-10 (Sheet 2 of 3)
Sequence 7 – Medium LOCA Dominant Cutsets (MLOCA-05)

NUMBER	CUTSET PROB.	PERCENTAGE	BASIC EVENT NAME		
11	2.23E-13	.00	MEDIUM LOCA INITIATING EVENT OCCURS	4.36E-04	IEV-MLOCA
			HARDWARE FAILURE OF SQUIB VALVE 120A	1.46E-03	IRWMOD10
			SUMP SCREEN B PLUGS AND PREVENTS FLOW	2.40E-04	REB-PLUG
			HARDWARE FAILURE OF SQUIB VALVE 118A	1.46E-03	IRWMOD09
12	2.23E-13	.00	MEDIUM LOCA INITIATING EVENT OCCURS	4.36E-04	IEV-MLOCA
			HARDWARE FAILURE OF SQUIB VALVE 120B	1.46E-03	IRWMOD12
			SUMP SCREEN A PLUGS AND PREVENTS FLOW	2.40E-04	REA-PLUG
			HARDWARE FAILURE OF SQUIB VALVE 118B	1.46E-03	IRWMOD11
13	2.08E-13	.00	MEDIUM LOCA INITIATING EVENT OCCURS	4.36E-04	IEV-MLOCA
			INDICATION FAILURE	1.00E-06	ALL-IND-FAIL
			CCF OF TANK LEVEL TRANSMITTERS	4.78E-04	IWX-XMTR
14	1.60E-13	.00	MEDIUM LOCA INITIATING EVENT OCCURS	4.36E-04	IEV-MLOCA
			HARDWARE FAILURE CAUSE RECIRC. CV 119A FAILS TO OPEN	1.75E-03	REACV119GO
			SUMP SCREEN B PLUGS AND PREVENTS FLOW	2.40E-04	REB-PLUG
			RELAY FAILS TO OPERATE	8.76E-04	IWBRS118AFA
15	1.60E-13	.00	MEDIUM LOCA INITIATING EVENT OCCURS	4.36E-04	IEV-MLOCA
			HARDWARE FAILURE CAUSE RECIRC. CV 119B FAILS TO OPEN	1.75E-03	REBCV119GO
			SUMP SCREEN A PLUGS AND PREVENTS FLOW	2.40E-04	REA-PLUG
			RELAY FAILS TO OPERATE	8.76E-04	IWARS118BFA
16	1.47E-13	.00	MEDIUM LOCA INITIATING EVENT OCCURS	4.36E-04	IEV-MLOCA
			CCF OF 2 OUT 2 LOW PRESSURE RECIRCULATION SQUIB VALVES	5.80E-05	IWX-EV4-SA
			CCF OF MOV 120A AND 120B	5.80E-06	IWX-EV2-SA
17	1.34E-13	.00	MEDIUM LOCA INITIATING EVENT OCCURS	4.36E-04	IEV-MLOCA
			HARDWARE FAILURE OF SQUIB VALVE 120A	1.46E-03	IRWMOD10
			SUMP SCREEN B PLUGS AND PREVENTS FLOW	2.40E-04	REB-PLUG
			RELAY FAILS TO OPERATE	8.76E-04	IWBRS118AFA
18	1.34E-13	.00	MEDIUM LOCA INITIATING EVENT OCCURS	4.36E-04	IEV-MLOCA
			HARDWARE FAILURE OF SQUIB VALVE 118A	1.46E-03	IRWMOD09
			SUMP SCREEN B PLUGS AND PREVENTS FLOW	2.40E-04	REB-PLUG
			RELAY FAILS TO OPERATE	8.76E-04	IWDRS120AFA

Table 19.59-10 (Sheet 3 of 3)
Sequence 7 – Medium LOCA Dominant Cutsets (MLOCA-05)

NUMBER	CUTSET PROB.	PERCENTAGE	BASIC EVENT NAME		
19	1.34E-13	.00	MEDIUM LOCA INITIATING EVENT OCCURS	4.36E-04	IEV-MLOCA
			HARDWARE FAILURE OF SQUIB VALVE 120B	1.46E-03	IRWMOD12
			SUMP SCREEN A PLUGS AND PREVENTS FLOW	2.40E-04	REA-PLUG
			RELAY FAILS TO OPERATE	8.76E-04	IWARS118BFA
20	1.34E-13	.00	MEDIUM LOCA INITIATING EVENT OCCURS	4.36E-04	IEV-MLOCA
			HARDWARE FAILURE OF SQUIB VALVE 118B	1.46E-03	IRWMOD11
			SUMP SCREEN A PLUGS AND PREVENTS FLOW	2.40E-04	REA-PLUG
			RELAY FAILS TO OPERATE	8.76E-04	IWCRS120BFA
21	8.03E-14	.00	MEDIUM LOCA INITIATING EVENT OCCURS	4.36E-04	IEV-MLOCA
			RELAY FAILS TO OPERATE	8.76E-04	IWDRS120AFA
			SUMP SCREEN B PLUGS AND PREVENTS FLOW	2.40E-04	REB-PLUG
			RELAY FAILS TO OPERATE	8.76E-04	IWBRS118AFA
22	8.03E-14	.00	MEDIUM LOCA INITIATING EVENT OCCURS	4.36E-04	IEV-MLOCA
			RELAY FAILS TO OPERATE	8.76E-04	IWCRS120BFA
			SUMP SCREEN A PLUGS AND PREVENTS FLOW	2.40E-04	REA-PLUG
			RELAY FAILS TO OPERATE	8.76E-04	IWARS118BFA
23	7.74E-14	.00	MEDIUM LOCA INITIATING EVENT OCCURS	4.36E-04	IEV-MLOCA
			HARDWARE FAILURE CAUSE RECIRC. CV 119B FAILS TO OPEN	1.75E-03	REBCV119GO
			CCF OF 2 OUT 2 LOW PRESSURE RECIRCULATION SQUIB VALVES	5.80E-05	IWX-EV4-SA
			HARDWARE FAILURE CAUSE RECIRC. CV 119A FAILS TO OPEN	1.75E-03	REACV119GO
24	6.46E-14	.00	MEDIUM LOCA INITIATING EVENT OCCURS	4.36E-04	IEV-MLOCA
			HARDWARE FAILURE CAUSE RECIRC. CV 119B FAILS TO OPEN	1.75E-03	REBCV119GO
			CCF OF 2 OUT 2 LOW PRESSURE RECIRCULATION SQUIB VALVES	5.80E-05	IWX-EV4-SA
			HARDWARE FAILURE OF SQUIB VALVE 120A	1.46E-03	IRWMOD10
25	6.46E-14	.00	MEDIUM LOCA INITIATING EVENT OCCURS	4.36E-04	IEV-MLOCA
			HARDWARE FAILURE CAUSE RECIRC. CV 119A FAILS TO OPEN	1.75E-03	REACV119GO
			CCF OF 2 OUT 2 LOW PRESSURE RECIRCULATION SQUIB VALVES	5.80E-05	IWX-EV4-SA
			HARDWARE FAILURE OF SQUIB VALVE 120B	1.46E-03	IRWMOD12

Table 19.59-11 (Sheet 1 of 3)
Sequence 8 – Small LOCA Dominant Cutsets (SLOCA-12)

NUMBER	CUTSET PROB.	PERCENTAGE	BASIC EVENT NAME		
1	4.16E-10	8.14	SMALL LOCA INITIATING EVENT OCCURS CCF OF 2 SQUIB VALVES TO OPERATE MECHANICAL FAILURE OF RNS MOV V055	5.00E-04 5.90E-05 1.41E-02	IEV-SLOCA ADX-EV-SA2 RN55MOD1
2	4.16E-10	8.14	SMALL LOCA INITIATING EVENT OCCURS CCF OF 2 SQUIB VALVES TO OPERATE HARDWARE FAILURE OF ISOLATION MOV 011	5.00E-04 5.90E-05 1.41E-02	IEV-SLOCA ADX-EV-SA2 RN11MOD3
3	4.16E-10	8.14	SMALL LOCA INITIATING EVENT OCCURS CCF OF 2 SQUIB VALVES TO OPERATE HARDWARE FAILS TO OPEN MOV V022/CB FTC/RELAY FTC	5.00E-04 5.90E-05 1.41E-02	IEV-SLOCA ADX-EV-SA2 RN22MOD4
4	4.16E-10	8.14	SMALL LOCA INITIATING EVENT OCCURS CCF OF 2 SQUIB VALVES TO OPERATE HARDWARE FAILS TO OPEN MOV V023/CB FTC/RELAY FTC	5.00E-04 5.90E-05 1.41E-02	IEV-SLOCA ADX-EV-SA2 RN23MOD5
5	2.95E-10	5.77	SMALL LOCA INITIATING EVENT OCCURS CCF OF 2 SQUIB VALVES TO OPERATE CASK LOADING PIT UNAVAILABLE DUE TO FUEL UNLOADING OPERATIONS	5.00E-04 5.90E-05 1.00E-02	IEV-SLOCA ADX-EV-SA2 CLP-UNAVAILABLE
6	2.11E-10	4.13	SMALL LOCA INITIATING EVENT OCCURS DUE TO CCF OF 4TH STAGE ADS SQUIB VALVES TO OPERATE MECHANICAL FAILURE OF RNS MOV V055	5.00E-04 3.00E-05 1.41E-02	IEV-SLOCA ADX-EV-SA RN55MOD1
7	2.11E-10	4.13	SMALL LOCA INITIATING EVENT OCCURS DUE TO CCF OF 4TH STAGE ADS SQUIB VALVES TO OPERATE HARDWARE FAILURE OF ISOLATION MOV 011	5.00E-04 3.00E-05 1.41E-02	IEV-SLOCA ADX-EV-SA RN11MOD3
8	2.11E-10	4.13	SMALL LOCA INITIATING EVENT OCCURS DUE TO CCF OF 4TH STAGE ADS SQUIB VALVES TO OPERATE HARDWARE FAILS TO OPEN MOV V022/CB FTC/RELAY FTC	5.00E-04 3.00E-05 1.41E-02	IEV-SLOCA ADX-EV-SA RN22MOD4
9	2.11E-10	4.13	SMALL LOCA INITIATING EVENT OCCURS DUE TO CCF OF 4TH STAGE ADS SQUIB VALVES TO OPERATE HARDWARE FAILS TO OPEN MOV V023/CB FTC/RELAY FTC	5.00E-04 3.00E-05 1.41E-02	IEV-SLOCA ADX-EV-SA RN23MOD5
10	1.50E-10	2.93	SMALL LOCA INITIATING EVENT OCCURS DUE TO CCF OF 4TH STAGE ADS SQUIB VALVES TO OPERATE CASK LOADING PIT UNAVAILABLE DUE TO FUEL UNLOADING OPERATIONS	5.00E-04 3.00E-05 1.00E-02	IEV-SLOCA ADX-EV-SA CLP-UNAVAILABLE

Table 19.59-11 (Sheet 2 of 3)
Sequence 8 – Small LOCA Dominant Cutsets (SLOCA-12)

NUMBER	CUTSET PROB.	PERCENTAGE	BASIC EVENT NAME		
11	1.45E-10	2.84	SMALL LOCA INITIATING EVENT OCCURS CCF OF 2 SQUIB VALVES TO OPERATE CCF OF STOP CHECK VALVES V015A/B TO OPEN	5.00E-04 5.90E-05 4.90E-03	IEV-SLOCA ADX-EV-SA2 RNX-KV1-GO
12	8.55E-11	1.67	SMALL LOCA INITIATING EVENT OCCURS CCF OF 2 SQUIB VALVES TO OPERATE OPERATOR FAILS TO ALIGN AND ACTUATE THE RNS	5.00E-04 5.90E-05 2.90E-03	IEV-SLOCA ADX-EV-SA2 RHN-MAN01
13	7.97E-11	1.56	SMALL LOCA INITIATING EVENT OCCURS CCF OF 2 SQUIB VALVES TO OPERATE UNAVAILABILITY OF BUS ECS ES 1 DUE TO UNSCHEDUL MAINTENANCE	5.00E-04 5.90E-05 2.70E-03	IEV-SLOCA ADX-EV-SA2 EC1BS001TM
14	7.97E-11	1.56	SMALL LOCA INITIATING EVENT OCCURS CCF OF 2 SQUIB VALVES TO OPERATE BUS UNAVAILABLE DUE TO UNSCHEDULED MAINTENANCE	5.00E-04 5.90E-05 2.70E-03	IEV-SLOCA ADX-EV-SA2 EC1BS012TM
15	7.97E-11	1.56	SMALL LOCA INITIATING EVENT OCCURS CCF OF 2 SQUIB VALVES TO OPERATE BUS UNAVAILABLE DUE TO UNSCHEDULED MAINTENANCE	5.00E-04 5.90E-05 2.70E-03	IEV-SLOCA ADX-EV-SA2 EC1BS122TM
16	7.58E-11	1.48	SMALL LOCA INITIATING EVENT OCCURS CCF OF 2 SQUIB VALVES TO OPERATE HARDWARE FAILURE OF VALVES ON DVI LINE A (V015A & 017 HARDWARE FAILURE OF VALVES ON DVI LINE B (V015B & 017	5.00E-04 5.90E-05 5.07E-02 5.07E-02	IEV-SLOCA ADX-EV-SA2 RNAMOD09 RNBMOD10
17	7.35E-11	1.44	SMALL LOCA INITIATING EVENT OCCURS DUE TO CCF OF 4TH STAGE ADS SQUIB VALVES TO OPERATE CCF OF STOP CHECK VALVES V015A/B TO OPEN	5.00E-04 3.00E-05 4.90E-03	IEV-SLOCA ADX-EV-SA RNX-KV1-GO
18	6.35E-11	1.24	SMALL LOCA INITIATING EVENT OCCURS COMMON CAUSE FAILURE OF THE BATTERIES IDSA-DB-1A/1B UNAVAILABILITY OF BUS ECS ES 2 DUE TO UNSCHEDULED MAINTENANCE	5.00E-04 4.70E-05 2.70E-03	IEV-SLOCA CCX-BY-PN EC2BS002TM
19	6.35E-11	1.24	SMALL LOCA INITIATING EVENT OCCURS COMMON CAUSE FAILURE OF THE BATTERIES IDSA-DB-1A/1B BUS UNAVAILABLE DUE TO UNSCHEDULED MAINTENANCE	5.00E-04 4.70E-05 2.70E-03	IEV-SLOCA CCX-BY-PN EC2BS022TM
20	6.35E-11	1.24	SMALL LOCA INITIATING EVENT OCCURS COMMON CAUSE FAILURE OF THE BATTERIES IDSA-DB-1A/1B BUS UNAVAILABLE DUE TO UNSCHEDULED MAINTENANCE	5.00E-04 4.70E-05 2.70E-03	IEV-SLOCA CCX-BY-PN EC2BS221TM

Table 19.59-11 (Sheet 3 of 3)
Sequence 8 – Small LOCA Dominant Cutsets (SLOCA-12)

NUMBER	CUTSET PROB.	PERCENTAGE	BASIC EVENT NAME		
21	6.35E-11	1.24	SMALL LOCA INITIATING EVENT OCCURS COMMON CAUSE FAILURE OF THE BATTERIES IDSA-DB-1A/1B UNAVAILABILITY OF BUS ECS ES 1 DUE TO UNSCHEDULED MAINTENANCE	5.00E-04 4.70E-05 2.70E-03	IEV-SLOCA CCX-BY-PN EC1BS001TM
22	6.35E-11	1.24	SMALL LOCA INITIATING EVENT OCCURS COMMON CAUSE FAILURE OF THE BATTERIES IDSA-DB-1A/1B BUS UNAVAILABLE DUE TO UNSCHEDULED MAINTENANCE	5.00E-04 4.70E-05 2.70E-03	IEV-SLOCA CCX-BY-PN EC1BS012TM
23	6.35E-11	1.24	SMALL LOCA INITIATING EVENT OCCURS COMMON CAUSE FAILURE OF THE BATTERIES IDSA-DB-1A/1B BUS UNAVAILABLE DUE TO UNSCHEDULED MAINTENANCE	5.00E-04 4.70E-05 2.70E-03	IEV-SLOCA CCX-BY-PN EC1BS121TM
24	5.16E-11	1.01	SMALL LOCA INITIATING EVENT OCCURS CCF OF 2 SQUIB VALVES TO OPERATE CHECK VALVE V013 FAILURE TO OPEN	5.00E-04 5.90E-05 1.75E-03	IEV-SLOCA ADX-EV-SA2 RNNCV013GO
25	4.50E-11	.88	SMALL LOCA INITIATING EVENT OCCURS BUS UNAVAILABLE DUE TO TEST OR CORRECTIVE MAINTENANCE BUS UNAVAILABLE DUE TO TEST OR CORRECTIVE MAINTENANCE	5.00E-04 3.00E-04 3.00E-04	IEV-SLOCA IDBBSDS1TM IDDBSDS1TM

Table 19.59-12 (Sheet 1 of 3)
Sequence 9 – Medium LOCA Dominant Cutsets (MLOCA-12)

NUMBER	CUTSET PROB.	PERCENTAGE	BASIC EVENT NAME		
1	3.63E-10	8.14	MEDIUM LOCA INITIATING EVENT OCCURS CCF OF 2 SQUIB VALVES TO OPERATE MECHANICAL FAILURE OF RNS MOV V055	4.36E-04 5.90E-05 1.41E-02	IEV-MLOCA ADX-EV-SA2 RN55MOD1
2	3.63E-10	8.14	MEDIUM LOCA INITIATING EVENT OCCURS CCF OF 2 SQUIB VALVES TO OPERATE HARDWARE FAILURE OF ISOLATION MOV 011	4.36E-04 5.90E-05 1.41E-02	IEV-MLOCA ADX-EV-SA2 RN11MOD3
3	3.63E-10	8.14	MEDIUM LOCA INITIATING EVENT OCCURS CCF OF 2 SQUIB VALVES TO OPERATE HARDWARE FAILS TO OPEN MOV V022/CB FTC/RELAY FTC	4.36E-04 5.90E-05 1.41E-02	IEV-MLOCA ADX-EV-SA2 RN22MOD4
4	3.63E-10	8.14	MEDIUM LOCA INITIATING EVENT OCCURS CCF OF 2 SQUIB VALVES TO OPERATE HARDWARE FAILS TO OPEN MOV V023/CB FTC/RELAY FTC	4.36E-04 5.90E-05 1.41E-02	IEV-MLOCA ADX-EV-SA2 RN23MOD5
5	2.57E-10	5.77	MEDIUM LOCA INITIATING EVENT OCCURS CCF OF 2 SQUIB VALVES TO OPERATE CASK LOADING PIT UNAVAILABLE DUE TO FUEL UNLOADING OPERATIONS	4.36E-04 5.90E-05 1.00E-02	IEV-MLOCA ADX-EV-SA2 CLP-UNAVAILABLE
6	1.84E-10	4.13	MEDIUM LOCA INITIATING EVENT OCCURS DUE TO CCF OF 4TH STAGE ADS SQUIB VALVES TO OPERATE MECHANICAL FAILURE OF RNS MOV V055	4.36E-04 3.00E-05 1.41E-02	IEV-MLOCA ADX-EV-SA RN55MOD1
7	1.84E-10	4.13	MEDIUM LOCA INITIATING EVENT OCCURS DUE TO CCF OF 4TH STAGE ADS SQUIB VALVES TO OPERATE HARDWARE FAILURE OF ISOLATION MOV 011	4.36E-04 3.00E-05 1.41E-02	IEV-MLOCA ADX-EV-SA RN11MOD3
8	1.84E-10	4.13	MEDIUM LOCA INITIATING EVENT OCCURS DUE TO CCF OF 4TH STAGE ADS SQUIB VALVES TO OPERATE HARDWARE FAILS TO OPEN MOV V022/CB FTC/RELAY FTC	4.36E-04 3.00E-05 1.41E-02	IEV-MLOCA ADX-EV-SA RN22MOD4
9	1.84E-10	4.13	MEDIUM LOCA INITIATING EVENT OCCURS DUE TO CCF OF 4TH STAGE ADS SQUIB VALVES TO OPERATE HARDWARE FAILS TO OPEN MOV V023/CB FTC/RELAY FTC	4.36E-04 3.00E-05 1.41E-02	IEV-MLOCA ADX-EV-SA RN23MOD5
10	1.31E-10	2.94	MEDIUM LOCA INITIATING EVENT OCCURS DUE TO CCF OF 4TH STAGE ADS SQUIB VALVES TO OPERATE CASK LOADING PIT UNAVAILABLE DUE TO FUEL UNLOADING OPERATIONS	4.36E-04 3.00E-05 1.00E-02	IEV-MLOCA ADX-EV-SA CLP-UNAVAILABLE

Table 19.59-12 (Sheet 2 of 3)
Sequence 9 – Medium LOCA Dominant Cutsets (MLOCA-12)

NUMBER	CUTSET PROB.	PERCENTAGE	BASIC EVENT NAME		
11	1.26E-10	2.83	MEDIUM LOCA INITIATING EVENT OCCURS CCF OF 2 SQUIB VALVES TO OPERATE CCF OF STOP CHECK VALVES V015A/B TO OPEN	4.36E-04 5.90E-05 4.90E-03	IEV-MLOCA ADX-EV-SA2 RNX-KV1-GO
12	7.46E-11	1.67	MEDIUM LOCA INITIATING EVENT OCCURS CCF OF 2 SQUIB VALVES TO OPERATE OPERATOR FAILS TO ALIGN AND ACTUATE THE RNS	4.36E-04 5.90E-05 2.90E-03	IEV-MLOCA ADX-EV-SA2 RHN-MAN01
13	6.95E-11	1.56	MEDIUM LOCA INITIATING EVENT OCCURS CCF OF 2 SQUIB VALVES TO OPERATE UNAVAILABILITY OF BUS ECS ES 1 DUE TO UNSCHEDULED MAINTENANCE	4.36E-04 5.90E-05 2.70E-03	IEV-MLOCA ADX-EV-SA2 EC1BS001TM
14	6.95E-11	1.56	MEDIUM LOCA INITIATING EVENT OCCURS CCF OF 2 SQUIB VALVES TO OPERATE BUS UNAVAILABLE DUE TO UNSCHEDULED MAINTENANCE	4.36E-04 5.90E-05 2.70E-03	IEV-MLOCA ADX-EV-SA2 EC1BS012TM
15	6.95E-11	1.56	MEDIUM LOCA INITIATING EVENT OCCURS CCF OF 2 SQUIB VALVES TO OPERATE BUS UNAVAILABLE DUE TO UNSCHEDULED MAINTENANCE	4.36E-04 5.90E-05 2.70E-03	IEV-MLOCA ADX-EV-SA2 EC1BS122TM
16	6.61E-11	1.48	MEDIUM LOCA INITIATING EVENT OCCURS CCF OF 2 SQUIB VALVES TO OPERATE HARDWARE FAILURE OF VALVES ON DVI LINE A (V015A & 017) HARDWARE FAILURE OF VALVES ON DVI LINE B (V015B & 017)	4.36E-04 5.90E-05 5.07E-02 5.07E-02	IEV-MLOCA ADX-EV-SA2 RNAMOD09 RNBMOD10
17	6.41E-11	1.44	MEDIUM LOCA INITIATING EVENT OCCURS DUE TO CCF OF 4TH STAGE ADS SQUIB VALVES TO OPERATE CCF OF STOP CHECK VALVES V015A/B TO OPEN	4.36E-04 3.00E-05 4.90E-03	IEV-MLOCA ADX-EV-SA RNX-KV1-GO
18	5.53E-11	1.24	MEDIUM LOCA INITIATING EVENT OCCURS COMMON CAUSE FAILURE OF THE BATTERIES IDSA-DB-1A/1B UNAVAILABILITY OF BUS ECS ES 2 DUE TO UNSCHEDULED MAINTENANCE	4.36E-04 4.70E-05 2.70E-03	IEV-MLOCA CCX-BY-PN EC2BS002TM
19	5.53E-11	1.24	MEDIUM LOCA INITIATING EVENT OCCURS COMMON CAUSE FAILURE OF THE BATTERIES IDSA-DB-1A/1B BUS UNAVAILABLE DUE TO UNSCHEDULED MAINTENANCE	4.36E-04 4.70E-05 2.70E-03	IEV-MLOCA CCX-BY-PN EC2BS022TM

Table 19.59-12 (Sheet 3 of 3)
Sequence 9 – Medium LOCA Dominant Cutsets (MLOCA-12)

NUMBER	CUTSET PROB.	PERCENTAGE	BASIC EVENT NAME		
20	5.53E-11	1.24	MEDIUM LOCA INITIATING EVENT OCCURS COMMON CAUSE FAILURE OF THE BATTERIES IDSA-DB-1A/1B BUS UNAVAILABLE DUE TO UNSCHEDULED MAINTENANCE	4.36E-04 4.70E-05 2.70E-03	IEV-MLOCA CCX-BY-PN EC2BS221TM
21	5.53E-11	1.24	MEDIUM LOCA INITIATING EVENT OCCURS COMMON CAUSE FAILURE OF THE BATTERIES IDSA-DB-1A/1B UNAVAILABILITY OF BUS ECS ES 1 DUE TO UNSCHEDULED MAINTENANCE	4.36E-04 4.70E-05 2.70E-03	IEV-MLOCA CCX-BY-PN EC1BS001TM
22	5.53E-11	1.24	MEDIUM LOCA INITIATING EVENT OCCURS COMMON CAUSE FAILURE OF THE BATTERIES IDSA-DB-1A/1B BUS UNAVAILABLE DUE TO UNSCHEDULED MAINTENANCE	4.36E-04 4.70E-05 2.70E-03	IEV-MLOCA CCX-BY-PN EC1BS012TM
23	5.53E-11	1.24	MEDIUM LOCA INITIATING EVENT OCCURS COMMON CAUSE FAILURE OF THE BATTERIES IDSA-DB-1A/1B BUS UNAVAILABLE DUE TO UNSCHEDULED MAINTENANCE	4.36E-04 4.70E-05 2.70E-03	IEV-MLOCA CCX-BY-PN EC1BS121TM
24	4.50E-11	1.01	MEDIUM LOCA INITIATING EVENT OCCURS CCF OF 2 SQUIB VALVES TO OPERATE CHECK VALVE V013 FAILURE TO OPEN	4.36E-04 5.90E-05 1.75E-03	IEV-MLOCA ADX-EV-SA2 RNNCV013GO
25	3.92E-11	.88	MEDIUM LOCA INITIATING EVENT OCCURS BUS UNAVAILABLE DUE TO TEST OR CORRECTIVE MAINTENANCE BUS UNAVAILABLE DUE TO TEST OR CORRECTIVE MAINTENANCE	4.36E-04 3.00E-04 3.00E-04	IEV-MLOCA IDDBSDS1TM IDBBSDS1TM

Table 19.59-13 (Sheet 1 of 3)
Sequence 10 – Spurious ADS Actuation Dominant Cutsets (SPADS-09)

NUMBER	CUTSET PROB.	PERCENTAGE	BASIC EVENT NAME		
1	2.75E-09	73.90	SPURIOUS ADS INITIATING EVENT OCCURS COMMON CAUSE FAILURE OF 2 ACCUMULATOR CHECK VALVES	5.40E-05 5.10E-05	IEV-SPADS ACX-CV-GO
2	1.65E-10	4.43	SPURIOUS ADS INITIATING EVENT OCCURS CHECK VALVE 029B FAILS TO OPEN CHECK VALVE 029A FAILS TO OPEN	5.40E-05 1.75E-03 1.75E-03	IEV-SPADS ACBCV029GO ACACV029GO
3	1.65E-10	4.43	SPURIOUS ADS INITIATING EVENT OCCURS CHECK VALVE 029B FAILS TO OPEN CHECK VALVE 028A FAILS TO OPEN	5.40E-05 1.75E-03 1.75E-03	IEV-SPADS ACBCV029GO ACACV028GO
4	1.65E-10	4.43	SPURIOUS ADS INITIATING EVENT OCCURS CHECK VALVE 028B FAILS TO OPEN CHECK VALVE 029A FAILS TO OPEN	5.40E-05 1.75E-03 1.75E-03	IEV-SPADS ACBCV028GO ACACV029GO
5	1.65E-10	4.43	SPURIOUS ADS INITIATING EVENT OCCURS CHECK VALVE 028B FAILS TO OPEN CHECK VALVE 028A FAILS TO OPEN	5.40E-05 1.75E-03 1.75E-03	IEV-SPADS ACBCV028GO ACACV028GO
6	6.87E-11	1.85	SPURIOUS ADS INITIATING EVENT OCCURS FLOW TUNING ORIFICE PLUGS CHECK VALVE 029A FAILS TO OPEN	5.40E-05 7.27E-04 1.75E-03	IEV-SPADS ACBOR001SP ACACV029GO
7	6.87E-11	1.85	SPURIOUS ADS INITIATING EVENT OCCURS FLOW TUNING ORIFICE PLUGS CHECK VALVE 028A FAILS TO OPEN	5.40E-05 7.27E-04 1.75E-03	IEV-SPADS ACBOR001SP ACACV028GO
8	6.87E-11	1.85	SPURIOUS ADS INITIATING EVENT OCCURS CHECK VALVE 029B FAILS TO OPEN FLOW TUNING ORIFICE PLUGS	5.40E-05 1.75E-03 7.27E-04	IEV-SPADS ACBCV029GO ACAOR001SP
9	6.87E-11	1.85	SPURIOUS ADS INITIATING EVENT OCCURS CHECK VALVE 028B FAILS TO OPEN FLOW TUNING ORIFICE PLUGS	5.40E-05 1.75E-03 7.27E-04	IEV-SPADS ACBCV028GO ACAOR001SP
10	2.85E-11	.77	SPURIOUS ADS INITIATING EVENT OCCURS FLOW TUNING ORIFICE PLUGS FLOW TUNING ORIFICE PLUGS	5.40E-05 7.27E-04 7.27E-04	IEV-SPADS ACBOR001SP ACAOR001SP

Table 19.59-13 (Sheet 2 of 3)
Sequence 10 – Spurious ADS Actuation Dominant Cutsets (SPADS-09)

NUMBER	CUTSET PROB.	PERCENTAGE	BASIC EVENT NAME		
11	6.48E-12	.17	SPURIOUS ADS INITIATING EVENT OCCURS COMMON CAUSE FAILURE OF ACCUMULATOR TANKS	5.40E-05 1.20E-07	IEV-SPADS ACX-TK-AF
12	2.27E-13	.01	SPURIOUS ADS INITIATING EVENT OCCURS ACCUMULATOR TANK B (T001B) RUPTURES CHECK VALVE 029A FAILS TO OPEN	5.40E-05 2.40E-06 1.75E-03	IEV-SPADS ACBTK001AF ACACV029GO
13	2.27E-13	.01	SPURIOUS ADS INITIATING EVENT OCCURS ACCUMULATOR TANK B (T001B) RUPTURES CHECK VALVE 028A FAILS TO OPEN	5.40E-05 2.40E-06 1.75E-03	IEV-SPADS ACBTK001AF ACACV028GO
14	2.27E-13	.01	SPURIOUS ADS INITIATING EVENT OCCURS CHECK VALVE 029B FAILS TO OPEN ACCUMULATOR TANK A (T001A) RUPTURES	5.40E-05 1.75E-03 2.40E-06	IEV-SPADS ACBCV029GO ACATK001AF
15	2.27E-13	.01	SPURIOUS ADS INITIATING EVENT OCCURS CHECK VALVE 028B FAILS TO OPEN ACCUMULATOR TANK A (T001A) RUPTURES	5.40E-05 1.75E-03 2.40E-06	IEV-SPADS ACBCV028GO ACATK001AF
16	9.42E-14	.00	SPURIOUS ADS INITIATING EVENT OCCURS ACCUMULATOR TANK B (T001B) RUPTURES FLOW TUNING ORIFICE PLUGS	5.40E-05 2.40E-06 7.27E-04	IEV-SPADS ACBTK001AF ACAOR001SP
17	9.42E-14	.00	SPURIOUS ADS INITIATING EVENT OCCURS FLOW TUNING ORIFICE PLUGS ACCUMULATOR TANK A (T001A) RUPTURES	5.40E-05 7.27E-04 2.40E-06	IEV-SPADS ACBOR001SP ACATK001AF
18	6.80E-14	.00	SPURIOUS ADS INITIATING EVENT OCCURS FLOW TUNING ORIFICE RUPTURE CHECK VALVE 029A FAILS TO OPEN	5.40E-05 7.20E-07 1.75E-03	IEV-SPADS ACBOR001EB ACACV029GO
19	6.80E-14	.00	SPURIOUS ADS INITIATING EVENT OCCURS FLOW TUNING ORIFICE RUPTURE CHECK VALVE 028A FAILS TO OPEN	5.40E-05 7.20E-07 1.75E-03	IEV-SPADS ACBOR001EB ACACV028GO
20	6.80E-14	.00	SPURIOUS ADS INITIATING EVENT OCCURS CHECK VALVE 029B FAILS TO OPEN FLOW TUNING ORIFICE RUPTURE	5.40E-05 1.75E-03 7.20E-07	IEV-SPADS ACBCV029GO ACAOR001EB

Table 19.59-13 (Sheet 3 of 3)
Sequence 10 – Spurious ADS Actuation Dominant Cutsets (SPADS-09)

NUMBER	CUTSET PROB.	PERCENTAGE	BASIC EVENT NAME		
21	6.80E-14	.00	SPURIOUS ADS INITIATING EVENT OCCURS CHECK VALVE 028B FAILS TO OPEN FLOW TUNING ORIFICE RUPTURE	5.40E-05 1.75E-03 7.20E-07	IEV-SPADS ACBCV028GO ACAOR001EB
22	2.83E-14	.00	SPURIOUS ADS INITIATING EVENT OCCURS FLOW TUNING ORIFICE RUPTURE FLOW TUNING ORIFICE PLUGS	5.40E-05 7.20E-07 7.27E-04	IEV-SPADS ACBOR001EB ACAOR001SP
23	2.83E-14	.00	SPURIOUS ADS INITIATING EVENT OCCURS FLOW TUNING ORIFICE PLUGS FLOW TUNING ORIFICE RUPTURE	5.40E-05 7.27E-04 7.20E-07	IEV-SPADS ACBOR001SP ACAOR001EB

Table 19.59-14
Typical System Failure Probabilities, Showing Higher Reliabilities for Safety Systems

Failure System/Function	Probability	Fault Tree Name	
CMT Valve Signal	5.7E-07	CMT-IC11	(one train; auto and manual actuation)
PRHR Valve Signal	1.1E-06	RHR-IC01	(one train; auto and manual actuation)
Passive Cont. Cool.	1.8E-06	PCT	
Reactor Trip by PMS	1.2E-05	RTPMS	(including operator actions)
Accumulators	6.9E-05	AC2AB	
IRWST Inj.	6.9E-05	IW2AB	
ADS	9.3E-05	ADS	(including operator actions)
Passive PRHR	2.0E-04	PRT	
Core Makeup Tanks	1.1E-04	CM2SL	
250 Vdc 1E Bus	3.1E-04	IDADS1	(one bus only)
DC Bus (Non-1E)	3.4E-04	ED1DS1	(one bus only)
RC Pump Trip	5.9E-04	RCT	
Hydrogen Control	1.0E-01	VLH	
Chilled Water	1.4E-03	VWH	
Containment Isol.	1.6E-03	CIC	
Reactor Trip by DAS	1.7E-03	DAS	(including operator action; excluding MGSET failure)
6900 Vac Bus	3.2E-03	ECES1	(one bus only)
CVS	3.4E-03	CVS1	
480 Vac Bus	5.9E-03	ECEK11	(one bus only)
Service Water	6.2E-03	SWT	
Comp. Cooling Water	6.3E-03	CCT	
Diesel Generators	1.0E-02	DGEN	
Startup Feedwater	1.7E-02	SFWT	
Compressed Air	1.3E-02	CAIR	
Condenser	2.4E-02	CDS	
Main Feedwater	2.8E-02	FWT	(including condenser)
RNS	9.1E-02	RNR	
Hydrogen Control	1.0E-01	VLH	

Table 19.59-15
Summary of AP1000 PRA Results

Events	Core Damage Frequency (per year)		Large Release Frequency (per year)	
	At-Power	Shutdown	At-Power	Shutdown
Internal Events	2.41E-07	1.03E-07	1.95E-08	1.72E-08
Internal Flood	8.82E-10	3.22E-09	7.14E-11	5.37E-10
Internal Fire	5.61E-08	8.5E-08(1)	4.54E-09	1.43E-08
Sum =	2.97E-07	1.91E-07	2.41E-08	3.20E-08

Note:

1. Internal fire during shutdown is evaluated quantitatively as a response to an NRC question and is not reported elsewhere in this document.

Table 19.59-16 not used.

Table 19.59-17
Comparison of AP1000 PRA Results to Risk Goals

Plant/Goal	Core Damage Frequency	Large Release Frequency	Containment Success Probability
Current PWR(1)	6.7E-05	5.3E-06	92%
NRC Safety Goal	1E-04	1E-06	90%
AP600	1.7E-07	1.8E-08	89%
AP1000	2.41E-07	1.95E-08	92%

Note:

1. Selected IPE result (two-loop Westinghouse PWR – internal at-power events and at-power flooding only). Note that there is no shutdown PRA requirement for currently operating plants.

Table 19.59-18 (Sheet 1 of 25)
AP1000 PRA-Based Insights

Insight	Disposition
1. The passive core cooling system (PXS) is composed of the following: – Accumulator subsystem – Core makeup tank (CMT) subsystem – In-containment refueling water storage tank (IRWST) subsystem – Passive residual heat removal (PRHR) subsystem. The automatic depressurization system (ADS), which is part of the reactor coolant system (RCS), also supports passive core cooling functions.	
1a. The accumulators provide a safety-related means of safety injection of borated water to the RCS.	6.3.2
The following are some important aspects of the accumulator subsystem as represented in the PRA:	
– There are two accumulators, each with an injection line to the reactor vessel/direct vessel injection (DVI) nozzle. Each injection line has two check valves in series.	Tier 1 Information
– The reliability of the accumulator subsystem is important. The accumulator subsystem is included in the D-RAP.	17.4
– Diversity between the accumulator check valves and the CMT check valves minimizes the potential for common cause failures.	6.3.2
1b. ADS provides a safety-related means of depressurizing the RCS.	Tier 1 Information
The following are some important aspects of ADS as represented in the PRA:	
ADS has four stages. Each stage is arranged into two separate groups of valves and lines.	Tier 1 Information
– Stages 1, 2, and 3 discharge from the top of the pressurizer to the IRWST	
– Stage 4 discharges from the hot leg to the RCS loop compartment.	
Each stage 1, 2, and 3 line contains two motor-operated valves (MOVs).	Tier 1 Information
Each stage 4 line contains an MOV valve and a squib valve.	Tier 1 Information
The valve arrangement and positioning for each stage is designed to reduce spurious actuation of ADS.	6.3.2 & 7.3
– Stage 1, 2, and 3 MOVs are normally closed and have separate controls.	
– Each stage 4 squib valve actuation requires signals from two separate PMS cabinets.	
– Stage 4 is blocked from opening at high RCS pressures.	

Table 19.59-18 (Sheet 2 of 25)
AP1000 PRA-Based Insights

Insight	Disposition
1b. (cont.)	
The ADS valves are automatically and manually actuated via the protection and safety monitoring system (PMS), and manually actuated via the diverse actuation system (DAS).	Tier 1 Information
The ADS valves are powered from Class 1E power.	Tier 1 Information
The ADS valve positions are indicated and alarmed in the control room.	6.3.7
Stage 1, 2, and 3 valves are stroke-tested every cold shutdown. Stage 4 squib valve actuators are tested every 2 years for 20% of the valves.	3.9.6
Because of the potential for counter-current flow limitation in the surgeline, it is essential to establish and maintain venting capability with ADS Stage 4 for gravity injection and containment recirculation following an extended loss of RNS when the RCS is open during shutdown operations.	6.3.3.4.3
ADS 4th stage squib valves receive a signal to open during shutdown conditions using PMS low hot leg level logic.	6.3.3.4.3
The reliability of the ADS is important. The ADS is included in the D-RAP.	17.4
ADS is required by the Technical Specifications to be available in Modes 1 through 6 without the cavity flooded.	16.1
Stages 1, 2, and 3, connected to the top of the pressurizer, provide a vent path to preclude pressurization of the RCS during shutdown conditions if decay heat removal is lost.	16.1
Depressurization of the RCS through ADS minimizes the potential for high-pressure melt ejection events.	
– Procedures will be provided for use of the ADS for depressurization of the RCS after core uncovery.	Emergency Response Guidelines
The ADS mitigates high pressure core damage events which can produce challenges to containment integrity due to the following severe accident phenomena:	19.36
– High pressure melt ejection	
– Direct containment heating	
– Induced steam generator tube rupture	
– Induced RCS piping rupture and rapid hydrogen release to containment	

Table 19.59-18 (Sheet 3 of 25)
AP1000 PRA-Based Insights

Insight	Disposition
1c. The CMTs provide safety-related means of high-pressure safety injection of borated water to the RCS.	6.3.1
The following are some important aspects of CMT subsystem as represented in the PRA:	
There are two CMTs, each with an injection line to the reactor vessel/DVI nozzle.	6.3.2
– Each CMT has a normally open pressure balance line from an RCS cold leg.	
– Each injection line is isolated with a parallel set of air-operated valves (AOVs).	
– These AOVs open on loss of Class 1E dc power, loss of air, or loss of the signal from the PMS.	
– The injection line for each CMT also has two normally open check valves in series.	
The CMT AOVs are automatically and manually actuated from PMS and DAS.	Tier 1 Information
CMT level instrumentation provides an actuation signal to initiate automatic ADS and provides the actuation signal for the IRWST squib valves to open.	6.3.1 & 7.3.1
The CMT AOV positions are indicated and alarmed in the control room.	6.3.7
CMT AOVs are stroke-tested quarterly.	3.9.6
The CMTs are risk-important for power conditions because the level indicators in the CMTs provide an open signal to ADS and to the IRWST squib valves as the CMTs empty.	
– The CMT subsystem is included in the D-RAP.	17.4
CMT is required by the Technical Specifications to be available in Modes 1 through 5 with RCS pressure boundary intact.	16.1

Table 19.59-18 (Sheet 4 of 25)
AP1000 PRA-Based Insights

Insight	Disposition
1d. IRWST subsystem provides a safety-related means of performing the following functions:	6.3
– Low-pressure safety injection following ADS actuation	
– Long-term core cooling via containment recirculation	
– Reactor vessel cooling through the flooding of the reactor cavity by draining the IRWST into the containment.	
The following are some important aspects of the IRWST subsystem as represented in the PRA:	
IRWST subsystem has the following flowpaths:	Tier 1 Information
– Two (redundant) injection lines from IRWST to reactor vessel/DVI nozzle. Each line is isolated with a parallel set of valves; each set with a check valve in series with a squib valve.	
– Two (redundant) recirculation lines from the containment to the reactor vessel/DVI injection line. Each recirculation line has two paths: one path contains a squib valve and a MOV, the other path contains a squib valve and a check valve.	
– The two MOV/squib valve lines also provide the capability to flood the reactor cavity.	
There are screens for each IRWST injection line and recirculation line.	Tier 1 Information
Squib valves provide the pressure boundary and prevent the check valves from normally seeing a high delta-P.	6.3.3
Squib valves and MOVs are powered by Class 1E power.	Tier 1 Information
The squib valves and MOVs for injection and recirculation are automatically and manually actuated via PMS, and manually actuated via DAS.	Tier 1 Information
The squib valves and MOVs for reactor cavity flooding are manually actuated via PMS and DAS from the control room.	Tier 1 Information
The injection squib valves and the recirculation squib valves in series with check valves are diverse from the other recirculation squib valves in order to minimize the potential for common cause failure between injection and recirculation/reactor cavity flooding.	6.3.2
Automatic IRWST injection at shutdown conditions is provided using PMS low hot leg level logic.	6.3.3.4.3 & 7.3.1

Table 19.59-18 (Sheet 5 of 25)
AP1000 PRA-Based Insights

Insight	Disposition
1d. (cont.)	
The positions of the squib valves and MOVs are indicated and alarmed in the control room.	6.3.7
IRWST injection and recirculation check valves are exercised at each refueling. IRWST injection and recirculation squib valve actuators are tested every 2 years for 20% of the valves (This does not require valve actuation). IRWST recirculation MOVs are stroke-tested quarterly.	3.9.6
The reliability of the IRWST subsystem is important. The IRWST subsystem is included in the D-RAP.	17.4
IRWST injection and recirculation are required by Technical Specifications to be available in Modes 1 through 6 without the cavity flooded.	16.1
The operator action to flood the reactor cavity is determined in Emergency Response Guideline AFR-C.1, which instructs the operator to flood the reactor cavity when the core-exit thermocouples reach 1200°F.	Emergency Response Guidelines
PXS recirculation valves are automatically actuated by a low IRWST level signal or manually from the control room, if automatic actuation fails.	6.3
1e. Passive residual heat removal (PRHR) provides a safety-related means of performing the following functions:	6.3.1 & 6.3.3
– Removes core decay heat during accidents	
– Allows automatic termination of RCS leak during a steam generator tube rupture (SGTR) without ADS	
– Allows plant to ride out an ATWS event without rod insertion.	PRA App. A4
The following are some important aspects of the PRHR subsystem as represented in the PRA:	
– PRHR is actuated by opening redundant parallel air-operated valves. These air-operated valves open on loss of Class 1E power, loss of air, or loss of the signal from PMS.	6.3.2
– The PRHR air-operated valves are automatically actuated and manually actuated from the control room by either PMS or DAS.	Tier 1 Information
– Diversity of the PRHR air-operated valves from the CMT air-operated valves minimizes the probability for common cause failure of both PRHR and CMT air-operated valves.	6.3.2

Table 19.59-18 (Sheet 6 of 25)
AP1000 PRA-Based Insights

Insight	Disposition
1e. (cont.)	
Long-term cooling of PRHR will result in steaming to the containment. The steam will normally condense on the containment shell and return to the IRWST by safety-related features. Connections are provided to IRWST from the spent fuel system (SFS) and chemical and volume control system (CVS) to extend PRHR operation. A safety-related makeup connection is also provided from outside the containment through the normal residual heat removal system (RNS) to the IRWST.	6.3.1 & system drawings
Capability exists and guidance is provided for the control room operator to identify a leak in the PRHR HX of 500 gpd. This limit is based on the assumption that a single crack leaking this amount would not lead to a PRHR HX tube rupture under the stress conditions involving the pressure and temperature gradients expected during design basis accidents, which the PRHR HX is designed to mitigate.	6.3.3 & 16.1
The positions of the inlet and outlet PRHR valves are indicated and alarmed in the control room.	6.3.7
PRHR air-operated valves are stroke-tested quarterly. The PRHR HX is tested to detect system performance degradation every 10 years.	3.9.6
PRHR is required by Technical Specifications to be available from Modes 1 through 5 with RCS pressure boundary intact.	16.1
The PRHR HX, in conjunction with the PCS, can provide core cooling for an indefinite period of time. After the IRWST water reaches its saturation temperature, the process of steaming to the containment initiates. Condensation occurs on the steel containment vessel, and the condensate is collected in a safety-related gutter arrangement, which returns the condensate to the IRWST. The gutter normally drains to the containment sump, but when the PRHR HX actuates, safety-related isolation valves in the gutter drain line shut and the gutter overflow returns directly to the IRWST. The following design features provide proper re-alignment for the gutter system valves to direct water to the IRWST:	6.3.2.1.1 & 6.3.7.6
– IRWST gutter and its drain isolation valves are safety-related	
– These isolation valves are designed to fail closed on loss of compressed air, loss of Class 1E dc power, or loss of the PMS signal	
– These isolation valves are actuated automatically by PMS and DAS.	7.3.1.2.7
The PRHR subsystem provides a safety-related means of removing decay heat following loss of RNS cooling during shutdown conditions with the RCS intact.	16.1

Table 19.59-18 (Sheet 7 of 25)
AP1000 PRA-Based Insights

Insight	Disposition
2. The protection and safety monitoring system (PMS) provides a safety-related means of performing the following functions: – Initiates automatic and manual reactor trip – Automatic and manual actuation of engineered safety features (ESF).	Tier 1 Information
PMS monitors the safety-related functions during and following an accident as required by Regulatory Guide 1.97.	7.1.1
PMS initiates an automatic reactor trip and an automatic actuation of ESF. PMS provides manual initiation of reactor trip. PMS 2-out-of-4 initiation logic reverts to a 2-out-of-3 coincidence logic if one of the 4 channels is bypassed. PMS does not allow simultaneous bypass of 2 redundant channels.	Tier 1 Information
PMS has redundant divisions of safety-related post-accident parameter display.	7.5.2.2.1 & 7.5.4
Each PMS division is powered from its respective Class 1E dc and UPS division.	Tier 1 Information
PMS provides fixed position controls in the control room.	Tier 1 Information
Reliability of the PMS is provided by the following:	
– The reactor trip functions are divided into two subsystems.	7.1.2.1.1
– The ESF functions are processed by two microprocessor-based subsystems that are functionally identical in both hardware and software.	7.1.2.2
Four sensors normally monitor variables used for an ESF actuation. These sensors may monitor the same variable for a reactor trip function.	7.3.1
Continuous automatic PMS system monitoring and failure detection/alarm is provided.	7.1.2
PMS equipment is designed to accommodate a loss of the normal heating, ventilation, and air conditioning (HVAC). PMS equipment is protected by the passive heat sinks upon failure or degradation of the active HVAC.	3.11 & 6.4
The reliability of the PMS is important. The PMS is included in the D-RAP.	17.4
The PMS software is designed, tested, and maintained to be reliable under a controlled verification and validation program written in accordance with IEEE 7-4.3.2 (1993) that has been endorsed by Regulatory Guide 1.152. Elements that contribute to a reliable software design include: – A formalized development, modification, and acceptance process in accordance with an approved software QA plan (paraphrased from IEEE standard, Section 5.3, “Quality”)	App 1A (Compliance with Reg. Guide 1.152)

Table 19.59-18 (Sheet 8 of 25)
AP1000 PRA-Based Insights

Insight	Disposition
2. (cont.) – A verification and validation program prepared to confirm the design implemented will function as required (IEEE standard, Subsection 5.3.4, “Verification and Validation”) – Equipment qualification testing performed to demonstrate that the system will function as required in the environment it is intended to be installed in (IEEE standard, Section 5.4, “Equipment Qualification”) – Design for system integrity (performing its intended safety function) when subjected to all conditions, external or internal, that have significant potential for defeating the safety function (abnormal conditions and events) (IEEE standard, Section 5.5, “System Integrity”) – Software configuration management process (IEEE standard, Subsection 5.3.5, “Software Configuration Management”).	
3. The diverse actuation system (DAS) provides a nonsafety-related means of performing the following functions: – Initiates automatic and manual reactor trip – Automatic and manual actuation of selected engineered safety features.	Tier 1 Information
Diversity is assumed in the PRA that eliminates the potential for common cause failures between PMS and DAS. – The DAS automatic actuation signals are generated in a functionally diverse manner from the PMS signals. Diversity between DAS and PMS is achieved by the use of different architectures, different hardware implementations, and different software, if any. – Software diversity between the DAS and PMS will be achieved through the use of different algorithms, logic, program architecture, executable operating system, and executable software/logic.	Tier 1 Information
DAS provides control room displays and fixed position controls to allow the operators to take manual actions.	7.7.1
DAS actuates using 2-out-of-2 logic. Actuation signals are output to the loads in the form of normally de-energized, energize-to-actuate signals. The normally de-energized output state, along with the dual 2-out-of-2 redundancy, reduces the probability of inadvertent actuation.	7.7.1.11
The actuation devices of DAS and PMS are capable of independent operation that is not affected by the operation of the other. The DAS is designed to actuate components only in a manner that initiates the safety function.	7.7.1.11

Table 19.59-18 (Sheet 9 of 25)
AP1000 PRA-Based Insights

Insight	Disposition
3. (cont.)	
The DAS reactor trip function is to trip the control rods by deenergizing the motor-generator set.	7.7.1.11
In the PRA it is assumed the following eliminates the potential for common cause failures between automatic and manual DAS functions.	
– DAS manual initiation functions are implemented in a manner that bypasses the signal processing equipment of the DAS automatic logic.	Tier 1 Information
The DAS, including the M-G set field breakers, is included in the D-RAP.	17.4
The DAS manual actuation cables are located within the nuclear island and, therefore, are protected from external hazards, such as high winds.	
4. The plant control system (PLS) provides a nonsafety-related means of controlling nonsafety-related equipment.	7.1.3 & 7.7.1
– Automatic and manual control of nonsafety-related functions, including “defense-in-depth” functions.	
– Provides control room indication for monitoring overall plant and nonsafety-related system performance.	
PLS has appropriate redundancy to minimize plant transients.	7.1.3 & 7.7.1.12
PLS provides capability for both automatic control and manual control.	7.1.3
Signal selector algorithms provide the PLS with the ability to obtain inputs from the PMS. The signal selector algorithms select those protection system signals that represent the actual status of the plant and reject erroneous signals.	7.1.3.2
PLS control functions are distributed across multiple distributed controllers so that single failures within a controller do not degrade the performance of control functions performed by other controllers.	7.1.3.1
5. The onsite power system consists of the main ac power system and the dc power system. The main ac power system is a non-Class 1E system. The dc power system consists of two independent systems: the Class 1E dc system and the non-Class 1E dc system.	
5a. The onsite main ac power system is a non-Class 1E system comprised of a normal, preferred, and standby power supplies.	8.3.1.1
The main ac power system distributes power to the reactor, turbine, and balance of plant auxiliary electrical loads for startup, normal operation, and normal/emergency shutdown.	8.3.1.1.1

Table 19.59-18 (Sheet 10 of 25)
AP1000 PRA-Based Insights

Insight	Disposition
5a. (cont.)	
The arrangement of the buses permits feeding functionally redundant pumps or groups of loads from separate buses and enhances the plant operational reliability.	8.3.1.1.1
During power generation mode, the turbine generator normally supplies electric power to the plant auxiliary loads through the unit auxiliary transformers. During plant startup, shutdown, and maintenance, the main ac power is provided from the high-voltage switchyard. The onsite standby power system powered by the two onsite standby diesel generators supplies power to selected loads in the event of loss of normal and preferred ac power supplies.	8.3.1.1.1
Two onsite standby diesel generator units, each furnished with its own support subsystems, provide power to the selected plant nonsafety-related ac loads.	8.3.1.1.2.1
On loss of power to a 6900 V diesel-backed bus, the associated diesel generator automatically starts and produces ac power. The normal source circuit breaker and bus load circuit breakers are opened, and the generator is connected to the bus. Each generator has an automatic load sequencer to enable controlled loading on the associated buses.	Tier 1 Information
5b. The Class 1E dc and uninterruptible power supply (UPS) system (IDS) provides reliable power for the safety-related equipment required for the plant instrumentation, control, monitoring, and other vital functions needed for shutdown of the plant.	8.3.2.1
There are four independent, Class 1E 250 Vdc divisions. Divisions A and D each consists of one battery bank, one switchboard, and one battery charger. Divisions B and C are each composed of two battery banks, two switchboards, and two battery chargers. The first battery bank in the four divisions is designated as the 24-hour battery bank. The second battery bank in Divisions B and C is designated as the 72-hour battery bank.	Tier 1 Information
The 24-hour battery banks provide power to the loads required for the first 24 hours following an event of loss of all ac power sources concurrent with a design basis accident. The 72-hour battery banks provide power to those loads requiring power for 72 hours following the same event.	Tier 1 Information
Battery chargers are connected to dc switchboard buses. The input ac power for the Class 1E dc battery chargers is supplied from non-Class 1E 480 Vac diesel-generator-backed motor control centers.	8.3.2.1.1.1
The 24-hour and the 72-hour battery banks are housed in ventilated rooms apart from chargers and distribution equipment.	8.3.2.1.3
Each of the four divisions of dc systems are electrically isolated and physically separated to prevent an event from causing the loss of more than one division.	8.3.2.1.3

Table 19.59-18 (Sheet 11 of 25)
AP1000 PRA-Based Insights

Insight	Disposition
5b. (cont.) The Class 1E batteries are included in the D-RAP.	17.4
5c. The non-Class 1E dc and UPS system (EDS) consists of the electric power supply and distribution equipment that provide dc and uninterruptible ac power to nonsafety-related loads.	Tier 1 Information
The non-Class 1E dc and UPS system consists of two subsystems representing two separate power supply trains.	8.3.2.1.2
EDS load groups 1, 2, 3, and 4 provide 125 Vdc power to the associated inverter units that supply the ac power to the non-Class 1E uninterruptible power supply ac system.	Tier 1 Information
The onsite standby diesel-generator-backed 480 Vac distribution system provides the normal ac power to the battery chargers.	Tier 1 Information
The batteries are sized to supply the system loads for a period of at least two hours after loss of all ac power sources.	8.3.2.1.2
6. The normal residual heat removal system (RNS) provides a safety-related means of performing the following functions: – Containment isolation for the RNS lines that penetrate the containment. – Isolation of the reactor coolant system at the RNS suction and discharge lines. – Pathway for long-term, post-accident makeup of containment inventory.	Tier 1 Information
RNS provides a nonsafety-related means of core cooling through: – RCS recirculation cooling during shutdown conditions. – Low pressure pumped makeup flow from the SFS cask loading pit and long-term recirculation from the IRWST and the containment. – Heat removal from IRWST during PRHR operation.	5.4.7
The RNS has redundant pumps and heat exchangers. The pumps are powered by non-Class 1E power with backup connections from the diesel generators.	5.4.7 & 8.3
RNS is manually aligned from the control room to perform its core cooling functions. The performance of the RNS is indicated in the control room.	5.4.7
The RNS containment isolation and pressure boundary valves are safety-related. The motor-operated valves are powered by Class 1E dc power.	Tier 1 Information
The RNS containment isolation MOVs are automatically and manually actuated via PMS.	7.3.1.2.20

Table 19.59-18 (Sheet 12 of 25)
AP1000 PRA-Based Insights

Insight	Disposition
6. (cont.)	
Interfacing system loss-of-coolant accident (LOCA) between the RNS and the RCS is prevented by:	5.4.7.2.2
– Each RNS line is isolated by at least three valves.	
– The RNS equipment outside containment is capable of withstanding the operating pressure of the RCS.	
– The RCS isolation valves are interlocked to prevent their opening at RCS pressures above its design pressure.	
CCS provides cooling to the RNS heat exchanger.	Tier 1 Information
Planned maintenance affecting the RNS cooling function and its support systems CCS and SWS should be performed in modes 1, 2, and 3, when the RNS is not normally operating.	16.3
Recognizing the increased vulnerability to risk with the plant in a “drained” condition, when the refueling cavity is not full and PRHR HXs are not available, entry into this condition and time spent in this condition during anticipation of a potentially severe high wind event will be minimized.	13.5
7. The component cooling water system (CCS) is a nonsafety-related system that removes heat from various components and transfers the heat to the service water system.	Tier 1 Information
The CCS has redundant pumps and heat exchanger.	Tier 1 Information
During normal operation, one CCS pump is operating. The standby pump is aligned to automatically start in case of a failure of the operating CCS pump.	9.2.2.4.2
The CCS pumps are automatically loaded on the standby diesel generator in the event of a loss of normal ac power. The CCS, therefore, continues to provide cooling of required components if normal ac power is lost.	9.2.2.4.5.4
8. The service water system (SWS) is a nonsafety-related system that transfers heat from the component cooling water heat exchangers to the atmosphere.	Tier 1 Information
The SWS has redundant pumps, strainers, and cooling tower cells.	9.2.1.2.1
During normal operation, one SWS train of equipment is operating. The standby train is aligned to automatically start in case of a failure of the operating SWS pump.	9.2.1.2.3.3
The SWS pumps and cooling tower fans are automatically loaded onto their associated diesel bus in the event of a loss of normal ac power. Both pumps and cooling tower fans automatically start after power from the diesel generator is available.	9.2.1.2.3.6

Table 19.59-18 (Sheet 13 of 25)
AP1000 PRA-Based Insights

Insight	Disposition
9. The chemical and volume control system (CVS) provides a safety-related means to terminate inadvertent RCS boron dilution and to preserve containment integrity by isolation of the CVS lines penetrating the containment.	Tier 1 Information
The CVS provides a nonsafety-related means to perform the following functions:	Tier 1 Information
– Makeup water to the RCS during normal plant operation.	
– Boration following a failure of reactor trip	
– Makeup water to the pressurizer auxiliary spray line.	
Two makeup pumps are provided. Each pump provides capability for normal makeup.	9.3.6.3.1
Two safety-related air-operated valves provide isolation of normal CVS letdown during shutdown operation on low hot leg level.	9.3.6.7
10. The operation of RNS and its support systems (CCS, SWS, main ac power and onsite power) is RTNSS-important for shutdown decay heat removal during reduced RCS inventory operations.	16.3
– These systems are included in the D-RAP.	17.4
Short-term availability controls for the RNS during at-power conditions reduce PRA uncertainties.	16.3
11. The information used regarding critical human actions (if any) and risk-important tasks from the PRA, as presented in Chapter 18 on human factors engineering, is important in developing and implementing procedures, training, and other human reliability related programs.	18
12. Sufficient instrumentation and control is provided at the remote shutdown workstation to bring the plant to safe shutdown conditions in case the control room must be evacuated.	7.4.3
There are no differences between the main control room and remote shutdown workstation controls and monitoring that would be expected to affect safety system redundancy and reliability.	7.4.3.1.1
13. Separation or protection of the equipment and cabling among the divisions of safety-related equipment and separation of safety-related from nonsafety-related equipment minimizes the probability that a fire or flood would affect more than one safety-related system or train, except in some areas inside containment where equipment will be capable of achieving safe shutdown prior to damage.	3.4.1.1.2 & 9.5.1.1.1, 9.5.1.2.1.1 & 9A
Although the containment is a single fire area, adequate design features exist for separation (structural or space), suppression, lack of combustibles, or operator action to ensure the plant can achieve safe shutdown.	9A

Table 19.59-18 (Sheet 14 of 25)
AP1000 PRA-Based Insights

Insight	Disposition
13. (cont.) To prevent flooding in a radiologically controlled area (RCA) in the Auxiliary Building from propagating to non-radiologically controlled areas, the non-RCAs are separated from the RCAs by 2 and 3-foot walls and floor slabs. In addition, electrical penetrations between RCAs and non-RCAs in the Auxiliary Building are located above the maximum flood level.	3.4.1.2.2.2
14. The following minimizes the probability for fire and flood propagation from one area to another and helps limit risk from internal fires and floods: – Fire barriers are sealed, to the extent possible (i.e., doors). – Structural barriers which function as flood barriers are watertight below the maximum flood level. – Administrative controls are established to maintain the performance of the fire protection system.	 9.5.1.2.1.1 3.4.1.1.2 Table 9.5.1-1, Item 29
15. Fire detection and suppression capability is provided in the design. Flooding control features and sump level indication are provided in the design. Administrative controls are established to maintain the performance of the fire protection system.	3.4.1, 9.5.1.2.1.2, & 9.5.1.8 Table 9.5.1-1, Item 29
16. AP1000 main control room fire ignition frequency is limited as a result of the use of low-voltage, low-current equipment and fiber optic cables. There is no cable spreading room in the AP1000 design.	7.1.2 & 7.1.3 Table 9.5.1-1
17. Redundancy in control room operations is provided within the control room itself for fires in which control room evacuation is not required.	9.5.1.2.1.1
18. The remote shutdown workstation provides redundancy of control and monitoring for safe shutdown functions in the event that main control room evacuation is required. The remote shutdown workstation is in a fire and flood area separate from the main control room.	7.4.3 & 9.5 3.4.1.2.2.2, 7.1.2, 7.4.3.1.1. & 9A.3.1.2.5
19. Although a main control room fire may defeat manual actuation of equipment from the main control room, it will not affect the automatic functioning of safe shutdown equipment via PMS or manual operation from the remote shutdown workstation. This is because the PMS cabinets, in which the automatic functions are housed, are located in fire areas separate from the main control room.	7.1.2.7 & 9A.3

Table 19.59-18 (Sheet 15 of 25)
AP1000 PRA-Based Insights

Insight	Disposition
20. The main control room has its own ventilation system, and is pressurized. This prevents smoke, hot gases, or fire suppressants originating in areas outside the control room from entering the control room via the ventilation system.	9.4.1
There are separate ventilation systems for safety-related equipment divisions (A & C and B & D). This prevents smoke, hot gases, or fire suppressants originating from one fire area to another to the extent that they could adversely affect safe shutdown capabilities.	9.4.1 9.5.1.1.1
The ventilation system for the remote shutdown room is independent of the ventilation system for the main control room.	9.4.1
21. AP1000 does not rely on ac power sources for safe shutdown capability since the safety-related passive systems do not require ac power sources for operation. Individual fires resulting in loss of offsite power or affecting onsite standby diesel generator operability do not affect safe shutdown capability.	8.1.4.2
22. Containment isolation functions are not compromised by internal fire or flood. Redundant containment isolation valves in a given line are located in separate fire and flood areas or zones and, if powered, are served by different control and electrical divisions.	6.2.3
One isolation component in a given line is located inside containment, while the other is located outside containment, and the containment wall is a fire/flood barrier.	6.2.3, 9.5 & 9A
23. The AP1000 design minimizes potential flooding sources in safety-related equipment areas, to the extent possible. The design also minimizes the number of penetrations through enclosure or barrier walls below the probable maximum flood level. Walls, floors, and penetrations are designed to withstand the maximum anticipated hydrodynamic loads.	3.4.1
24. Differences between the as-built plant and the basis for the AP1000 seismic margin analysis are reviewed.	19.59.10.5
25. The depressurization of the reactor coolant system below 150 psi facilitates in-vessel retention of molten core debris.	19.36
26. The reflective reactor vessel insulation provides an engineered flow path to allow the ingression of water and venting of steam for externally cooling the vessel in the event of a severe accident involving core relocation to the lower plenum.	19.39, 5.3.5 & Tier 1 Information
The reflective insulation panels and support members can withstand pressure differential loading due to the IVR boiling phenomena.	
Water inlets and steam vents are provided at the entrance and exit of the insulation boundary.	
The reactor vessel insulation is included in the D-RAP.	17.4

Table 19.59-18 (Sheet 16 of 25)
AP1000 PRA-Based Insights

Insight	Disposition
27. The reactor cavity design provides a reasonable balance between the regulatory requirements for sufficient ex-vessel debris spreading area and the need to quickly submerge the reactor vessel for the in-vessel retention of core debris.	19.39 & Appendix 19B
28. The design can withstand a best-estimate ex-vessel steam explosion without failing the containment integrity.	Appendix 19B
29. The containment design incorporates defense-in-depth for mitigating direct containment heating by providing no significant direct flow path for the transport of particulated molten debris from the reactor cavity to the upper containment regions.	Appendix 19B
30. The hydrogen control system is comprised of passive autocatalytic recombiners (PARs) and hydrogen igniters to limit the concentration of hydrogen in the containment during accidents and beyond design basis accidents, respectively. Operability of the hydrogen igniters is addressed by short-term availability controls during modes 1, 2, 5 (with RCS pressure boundary open), and 6 (with upper internals in place or cavity levels less than full). The operator action to activate the igniters is the first step in ERG AFR.C-1 to ensure that the igniter activation occurs prior to rapid cladding oxidation.	Tier 1 Information 16.3 Emergency Response Guidelines
31. Mitigation of the effects of a diffusion flames on the containment shell are addressed by the following containment layout features: – Vents from the PXS and CVS compartments (where hydrogen releases can be postulated) to the CMT room are located well away from the containment shell and containment penetrations. The access hatch to the PXS-B compartment is located near the containment wall and is normally closed to address severe accident considerations. The access hatch to the PXS-B compartment is accessible from Room 11300 on elevation 107′-2″. – IRWST vents are designed so that those located away from the containment wall open to vent hydrogen releases. In this situation IRWST vents located close to the containment wall would not open because flow of hydrogen through the other vents would not result in a IRWST pressure sufficient to open them.	1.2, General Arrangement Drawings 3.4.1.2.2.1 & 19.41.7 6.2.4.5.1
32. The containment structure can withstand the pressurization from a LOCA and the global combustion of hydrogen released in-vessel (10 CFR 50.44).	19.41
33. The steam generator should not be depressurized to cool down the RCS if water is not available to the secondary side. This action protects the tubes from large pressure differential and minimizes the potential for creep rupture. Severe accident management guidance is developed and implemented using the suggested framework provided in APP-GW-GL-027.	19.59.10

Table 19.59-18 (Sheet 17 of 25)
AP1000 PRA-Based Insights

Insight	Disposition
34. Depressurizing the RCS and maintaining a water level covering the SG tubes on the secondary side can mitigate fission product releases from a steam generator tube rupture accident. Severe accident management guidance is developed and implemented using the suggested framework provided in APP-GW-GL-027.	19.59.10
35. Loss of ac power does not contribute significantly to the core damage frequency. – Nonsafety-related containment spray does not need to be ac independent.	19.59
36. AP1000 has a nonsafety-related containment spray system.	6.5.2
Containment spray is not credited in the PRA. Failure of the nonsafety-related containment spray does not prevent the plant achieving the safety goals.	19.59
Severe accident management guidance for operation of the nonsafety-related containment spray system is developed and implemented using the suggested framework provided in APP-GW-GL-027.	19.59.10
37. Passive containment can withstand severe accidents without PCS water cooling the containment shell. Air cooling alone is sufficient to maintain containment pressure below failure pressure with high probability.	19.40
38. Operation of ADS stage 4 provides a vent path for the severe accident hydrogen to the steam generator compartments, bypassing the IRWST, and mitigating the conditions required to produce a diffusion flame near the containment wall.	19.41
39. Containment isolation valves controlled by DAS are important in limiting offsite releases following core melt accidents. These valves are identified as being risk-significant SSCs and are included in the D-RAP.	17.4
Operability of DAS for selected containment isolation actuations is addressed by short-term availability controls.	16.3
40. Reflooding the reactor pressure vessel through the break can have a significant effect on a severe accident by quenching core debris, achieving a controlled stable state, and producing hydrogen.	19.38 & 19.41
41. The type of concrete used in the basemat is not important.	Appendix 19B
The reactor cavity design incorporates features that extend the time to basemat melt-through in the event of RPV failure. The cavity design includes: – A minimum floor area of 48 m^2 available for spreading of the molten core debris – A minimum thickness of concrete above the embedded containment liner of 0.85 m	Appendix 19B

Table 19.59-18 (Sheet 18 of 25)
AP1000 PRA-Based Insights

Insight	Disposition
41. (cont.) – There is no piping buried in the concrete beneath the reactor cavity; sump drain lines are not enclosed in either of the reactor cavity floor or reactor cavity sump concrete. Thus, there is no direct pathway from the reactor cavity to outside the containment in the event of core-concrete interactions. – The openings between the reactor cavity and cavity sump are small diameter openings in which core debris in the cavity will solidify. Thus, there is no direct pathway for core debris to enter the sump, except in the case where it might spill over the sump curbing.	
42. No safety-related equipment is located outside the Nuclear Island.	1.2 & 3.4.1
43. Capability exists to vent the containment. Severe accident management guidance for venting containment is developed and implemented using the suggested framework provided in APP-GW-GL-027.	Appendix 19D 19.59.10
44. A list of risk-important systems, structures, and components (SSCs) has been provided in the D-RAP. The risk-significant SSCs are included in the D-RAP.	17.4 17.4
45. Differences between the as-built plant and the design used as the basis for the AP1000 PRA and Table 59-18 are reviewed. If the effects of the differences are shown, by a screening analysis, to potentially result in a significant increase in core damage frequency or large release frequency, the PRA will be updated to reflect these differences. Based on site-specific information, the qualitative screening of external events (PRA Section 58.1) is evaluated. If any site-specific susceptibilities are found, the PRA should be updated to include the applicable external event.	19.59.10
46. There are no watertight doors used for flood protection in the AP1000 design. Plugging of the drain headers is minimized by designing them large enough to accommodate more than the design flow and by making the flow path as straight as possible.	3.4.1.1.2 9.3.5.1.2
47. The maintenance guidelines as described in the Shutdown Evaluation Report (WCAP-14837) should be considered when developing the plant specific operations procedures.	13.5.1
48. Procedures to control transient combustibles are established.	Table 9.5.1-1, Items 77-83

Table 19.59-18 (Sheet 19 of 25)
AP1000 PRA-Based Insights

Insight	Disposition
49. There are two compartments inside containment (PXS-A and PXS-B) containing safe shutdown equipment that normally do not flood although they are below the maximum flood height. Each of these two compartments contains redundant and essentially identical equipment (one accumulator with associated isolation valves as well as isolation valves for one CMT, one IRWST injection line, and one containment recirculation line). A pipe break in one of these compartments can cause that room to flood. These two compartments are physically separated to ensure that a flood in one compartment does not propagate to the other. Drain lines from the PXS-A and PXS-B compartments to the reactor vessel cavity and steam generator compartment are protected from backflow by redundant backflow preventers.	3.4.1.2.2.1
50. There are seven automatically actuated containment isolation valves inside containment subject to flooding. These seven normally closed containment isolation valves would not fail open as a result of the compartment flooding. Also, there is a redundant, normally closed, containment isolation valve located outside containment in series with each of these valves.	3.4.1.2.2.1
51. The passive containment cooling system (PCS) cooling water not evaporated from the vessel wall flows down to the bottom of the containment annulus. Two 100-percent drain openings, located in the side wall of the Shield Building, are always open with screens provided to prevent entry of small animals into the drains.	19.40
52. The major rooms housing divisional cabling and equipment (the battery rooms, dc equipment rooms, I&C rooms, and penetration rooms) are separated by 3-hour fire rated walls. Separate ventilation subsystems are provided for A and C and for B and D division rooms. In order for a fire to propagate from one divisional room to another, it must move past a 3-hour barrier (e.g., a door) into a common corridor and enter the other room through another 3-hour barrier (e.g., another door).	9.5.1 & 9A.3
53. An access bay in the turbine building is provided to protect the north end of the Auxiliary Building, from potential debris produced by a postulated seismic damage of the adjacent Turbine Building.	1.2
54. There are no normally open connections to sources of “unlimited” quantity of water in the electrical and I&C portions of the Auxiliary Building such as that it could affect safe shutdown capabilities.	Figure 9.5.1-1
55. To prevent flooding in a radiologically controlled area (RCA) in the Auxiliary Building from propagating to non-RCAs, the non-RCAs are separated from the RCAs by 2- and 3-foot walls and floor slabs. In addition, electrical penetrations between RCAs and non-RCAs in the Auxiliary Building are located above the maximum flood level.	3.4.1.2.2.2
56. The two 72-hour rated Class 1E division B and C batteries are located above the maximum flood height in the Auxiliary Building considering all possible flooding sources.	3.4.1.2.2.2

Table 19.59-18 (Sheet 20 of 25)
AP1000 PRA-Based Insights

Insight	Disposition
57. Flood water in the Turbine Building drains to the yard and does not affect the Auxiliary Building. The presence of watertight walls and floor of the Auxiliary Building valve/ penetration room prevents flooding from propagating beyond this area.	3.4.1.2.2.2
58. The mechanical equipment and electrical equipment in the Auxiliary Building are separated to prevent propagation of leaks from the piping and mechanical equipment areas to the Class 1E equipment and Class 1E I&C equipment rooms.	3.4.1.2.2.2
59. Connections to sources of “large” quantity of water are located in the Turbine Building. They are the service water system, which interfaces with the component cooling water system, and the circulating water system, which interfaces with the Turbine Building closed cooling system and the condenser. Features that minimize the flood propagation to other buildings are: – Flow from any postulated ruptures above grade level (elevation 100') in the Turbine Building flows down to grade level via floor grating and stairwells. This grating in the floors also prevents any significant propagation of water to the Auxiliary Building via flow under the doors. – A relief panel in the Turbine Building west wall at grade level directs the water outside the building to the yard and limits the maximum flood level in the Turbine Building to less than 6 inches. Flooding propagation to areas of the adjacent Auxiliary Building, via flow under doors or backflow through the drains, is possible but is bounded by a postulated break in those areas.	3.4.1.2.2.3
60. Flood water in the Annex Building grade level is directed by the sloped floor to drains and to the yard area through the door of the Annex Building. Flow from postulated ruptures above grade level in the Annex Building is directed by floor drains to the Annex Building sump, which discharges to the Turbine Building drain tank. Alternate paths include flow to the Turbine Building via flow under access doors and down to grade level via stairwells and elevator shaft. The floors of the Annex Building are sloped away from the access doors to the Auxiliary Building in the vicinity of the access doors to prevent migration of flood water to the non-RCAs of the Nuclear Island where all safety-related equipment is located.	3.4.1.2.2.3
61. There are no connections to sources of “unlimited” quantity of water, except for fire protection, in the Annex Building.	Figure 9.5.1-1

Table 19.59-18 (Sheet 21 of 25)
AP1000 PRA-Based Insights

Insight	Disposition
62. To prevent overdraining, the RCS hot and cold legs are vertically offset, which permits draining of the steam generators for nozzle dam insertion with a hot leg level much higher than traditional designs.	7.2.1
To lower the RCS hot leg level at which a vortex occurs in the RNS suction line, a step nozzle connection between the RCS hot leg and the RNS suction line is used.	5.4.7.2.1 & Figure 5.1-5
Should vortexing occur, air entrainment into the RNS pump suction is limited.	5.4.7.2.1
There are two safety-related RCS hot leg level channels, one located in each hot leg. These level instruments are independent and do not share instrument lines. These level indicators are provided primarily to monitor RCS level during midloop operations. One level tap is at the bottom of the hot leg, and the other tap is on the top of the hot leg close to the steam generator.	Tier 1 Information Figure 5.1-5 19E.2.1.1
Wide range pressurizer level indication (cold calibrated) is provided that can measure RCS level to the bottom of the hot legs. This nonsafety-related pressurizer level indication can be used as an alternative way of monitoring level and can be used to identify inconsistencies in the safety-related hot leg level instrumentation.	Tier 1 Information Figure 5.1-5 19E.2.1.1
The RNS pump suction line is sloped continuously upward from the pump to the reactor coolant system hot leg with no local high points. This design eliminates potential problems in refilling the pump suction line if an RNS pump is stopped when cavitating due to excessive air entrainment. This self-venting suction line allows the RNS pumps to be immediately restarted once an adequate level in the hot leg is re-established.	5.4.7.2.1
It is important to maximize the availability of the nonsafety-related wide range pressurizer level indication during RCS draining operations during cold shutdown. Procedures and training must be developed to encompass this item.	13.5
63. Solid-state switching devices and electro-mechanical relays resistant to relay chatter will be used in the AP1000 safety-related I&C system.	19.55.2.3
64. The annulus drains will have the same or higher HCLPF value as the Shield Building so that the drain system will not fail at lower acceleration levels causing water blocking of the PCS air baffle.	19.59.10
65. The ability to close containment hatches and penetrations during Modes 5 & 6 prior to steaming to containment is important. Procedures and training must be developed to encompass this item.	13.5 & 16.1
66. Spurious actuation of squib valves is prevented by the use of a squib valve controller circuit which requires multiple hot shorts for actuation, physical separation of potential hot short locations (e.g., routing of ADS cables in low voltage cable trays, and, in the case of PMS, the use of arm and fire signals from separate PMS cabinets), and provisions for operator action to remove power from the fire zone.	9A.2.7.1

Table 19.59-18 (Sheet 22 of 25)
AP1000 PRA-Based Insights

Insight	Disposition
67. For long-term recirculation operation, the RNS pumps can take suction from one of the two sump recirculation lines. Unrestricted flow through both parallel paths is required for success of the sump recirculation function when both RNS pumps are running. If one of the two parallel paths fails to open, operator action is required to manually throttle the RNS discharge valve to prevent pump cavitation.	Emergency Response Guidelines
The containment isolation valves in the RNS piping automatically close via PMS with a high radiation signal. The actuation setpoint was established consistent with a DBA non-mechanistic source term associated with a large LOCA. The containment radiation level for other accidents is expected to be below the point that would cause the RNS MOVs to automatically close.	6.2.3 & 7.3.1.2.20
With the RNS pumps aligned either to the IRWST or the containment sump, the pumps' net positive suction head is adequate to prevent pump cavitation and failure even when the IRWST or sump inventory is saturated.	5.4.7
Emergency response guidelines are provided for aligning the RNS from the control room for RCS injection and recirculation.	Emergency Response Guidelines
The following are additional AP1000 features which contribute to the low likelihood of interfacing system LOCAs between the RNS and the RCS: – A relief valve located in the common RNS discharge line outside containment provides protection against excess pressure. – Two remotely operated MOVs connecting the suction and discharge headers to the IRWST are interlocked with the isolation valves connecting the RNS pumps to the hot leg. This prevents inadvertent opening of these two MOVs when the RNS is aligned for shutdown cooling and potential diversion and draining of reactor coolant system. – Power to the four isolation MOVs connecting the RNS pumps to the RCS hot leg is administratively blocked at their motor control centers during normal power operation.	5.4.7.2
Per the Shutdown Evaluation, operability of the RNS is tested, via connections to the IRWST, before its alignment to the RCS hot leg for shutdown cooling.	19E
Inadvertent opening of RNS valve V024 results in a draindown of RCS inventory to the IRWST and requires gravity injection from the IRWST. Administrative controls to ensure that inadvertent opening of this valve is unlikely must be developed.	13.5
The reliability of the IRWST suction isolation valve (V023) to open on demand is important. The IRWST suction isolation valve is included in the D-RAP.	17.4

Table 19.59-18 (Sheet 23 of 25)
AP1000 PRA-Based Insights

Insight	Disposition
68. The startup feedwater system pumps provide feedwater to the steam generator. This capability provides an alternate core cooling mechanism to the PRHR heat exchangers for non-LOCA or steam generator tube ruptures. The startup feedwater pumps are included in the D-RAP.	17.4
69. Capability is provided for on-line testing and calibration of the DAS channels, including sensors. Short-term availability controls of the DAS during at-power conditions reduce PRA uncertainties.	7.7.1.11 16.3
70. One CVS pump is configured to operate on demand while the other CVS pump is in standby. The operation of these pumps will alternate periodically. On a source range flux doubling signal, the PMS automatically closes two safety-related CVS makeup line isolation valves, closes two safety-related CVS demineralized water suction valves to the makeup pumps, and trips the makeup pumps. On a reactor trip or low input voltage to the Class 1E dc power system battery chargers, the PMS closes the two safety-related CVS demineralized water suction valves to the makeup pumps and aligns the makeup pump suction to the boric acid tank.	9.3.6.3.1 & 19.15 7.3.1.2.14
71. Procedures will be prepared to respond to low hot leg level alarms.	Emergency Response Guidelines
72. The containment recirculation screens are configured such that the chance of clogging is minimized during operation following accidents at power and at shutdown. The configuration features that reduce the chance of clogging include: – Redundant screens are provided and located in separate locations – Bottom of screens are located well above the lowest containment level as well as the floors around them – Top of screens are located well below the containment floodup level – Screens have protective plates that are located close to the top of the screens and extend out in front and to the side of the screens – Screens have conservative flow areas to account for plugging. Adequate PXS performance can be supported by one screen with at least 90% of its surface area completely blocked – During recirculation operation, the velocities approaching the screens are very low which limits the transport of debris.	6.3.2

Table 19.59-18 (Sheet 24 of 25)
AP1000 PRA-Based Insights

Insight	Disposition
73. A cleanliness program controls foreign debris from being introduced into the IRWST tank and into the containment during maintenance and inspection operations.	6.3.2.2.7.2, 6.3.2.2.7.3, & 6.3.8.1
74. For floor drains, from the reactor cavity PXS-A and PXS-B rooms, appropriate precautions such as check valves, back flow preventers, and siphon breaks are assumed to prevent back flow from a flooded space to a nonflooded space.	3.4.1.2.2
75. Plant ventilation systems include features to prevent smoke originating from one fire area to another to the extent that they could adversely affect safe shutdown capabilities.	9.4.2.2
76. An alternative gravity injection path is provided through RNS V-023 during cold shutdown and refueling conditions with the RCS open. Administrative controls to maximize the likelihood that RNS valve V-023 will be able to open if needed during Mode 5 when the RCS is open, and PRHR cannot be used for core cooling are established.	Emergency Response Guidelines 13.5
77. The IRWST suction isolation valve (V023) and the RCS pressure boundary isolation valves (V001A/B, V002A/B) are environmentally qualified to perform their safety functions.	Tier 1 Information
78. Following an extended loss of RNS during safe/cold shutdown with the RCS intact and PRHR unavailable, it is essential to establish and maintain venting capability with ADS Stage 4 for gravity injection and containment recirculation.	19.59.5
79. Generic open items and plant-specific action items resulting from NRC review of the I&C platform are resolved.	7.1.6
80. An analysis is provided that demonstrates that operator actions, which minimize the probability of the potential for spurious ADS actuation as a result of a fire, can be accomplished within 30 minutes following detection of the fire and the procedure for the manual actuation of the valve to allow fire water to reach the automatic fire system in the containment maintenance floor.	9.5.1.8
81. Procedures to minimize risk when fire areas are breached during maintenance are established. These procedures will address a fire watch for fire areas breached during maintenance.	9.5.1.8
82. It is important to maintain the low-temperature overpressure protection provided by the RNS relief valve to ensure that the reactor vessel pressure and temperature limits are not exceeded during shutdown conditions. Isolation of the RNS and its relief valve is permitted during shutdown conditions in case the hot legs empty due to a loss of RCS inventory; if the RNS is isolated, an alternate vent path would be opened, such as the ADS Stage 1, 2, and 3 valves.	16.1 (LCO Basis 3.4.14)

Table 19.59-18 (Sheet 25 of 25)
AP1000 PRA-Based Insights

Insight	Disposition
83. The passive cooling system louvers and screens cover openings located all around the containment, into an enclosed volume where the air inlet ducts are located. The screens are designed to help prevent foreign objects or debris from entering the air flow path. In the event of a snow or ice storm, some fraction of these air inlets can become blocked with snow or ice. The results of analysis, made available to the staff during the design certification of the AP1000, show that a considerable fraction of the inlet area can be blocked without a significant effect on the peak containment pressure for design basis events.	
Louvers are arranged within the air inlets to minimize the entrance of debris into the inlets. These louvers are fixed and, therefore, will not block the air flow path.	
The chimney outlet is designed to produce the necessary air flow in the event of an accident. The outlet contains two heavy grates to guard against missiles, and it is fully screened to prevent foreign objects from entering the containment annulus. The presence of a positive air flow during normal operation helps prevents ice and snow from entering the chimney.	6.2.2.2.4
Air-only cooling of the containment provides cooling necessary to maintain containment integrity with a high level of confidence for the first 24 hours following an accident in the event there is no water cooling from PCS.	
There is a surveillance requirement (SR 3.6.6.5) to verify every 24 months that the air flow path is unobstructed.	3.6.6
84. The AP1000 is protected against external floods up to the 100-foot level, which corresponds to the ground level at each plant. From this point, the ground is graded so that water naturally flows away from the plant structures.	
85. The plant is designed such that the 100-foot level is slightly above grade and the level of anticipated external flooding. Below grade is protected against flooding by a waterproofing system. Seismic Category I SSCs below grade are designed to withstand hydrostatic pressures.	RN-12-038
The seismic Category I SSCs below grade are protected against external flooding by a waterproofing system.	3.4.1.1.1
86. The vacuum relief system is important for the integrity of the containment during an event where a vacuum is developed inside containment. The vacuum relief system consists of redundant relief devices, and its function is to prevent differential pressure between the inside and outside of the containment from exceeding the design value.	

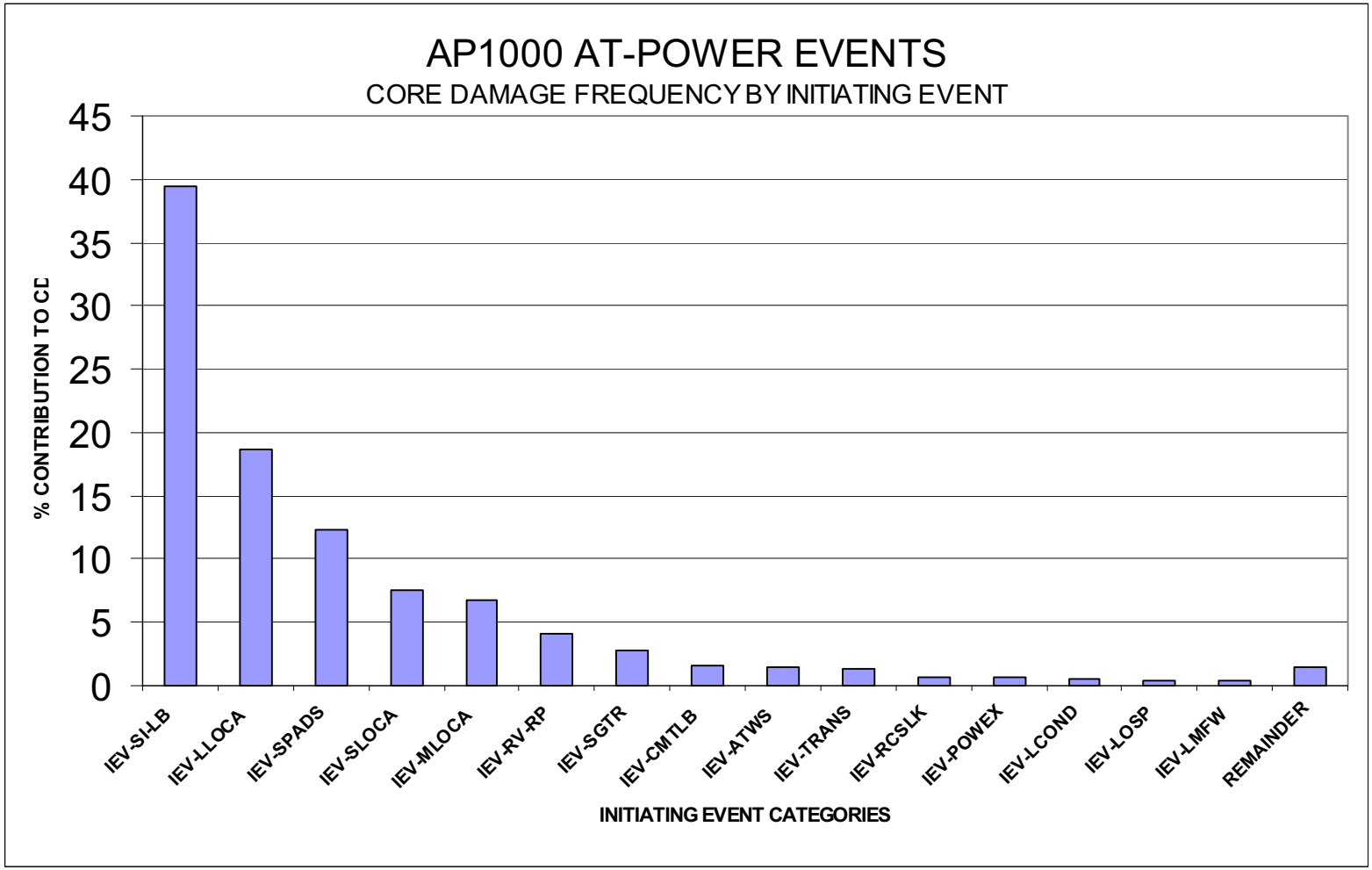

Figure 19.59-1 Contribution of Initiating Events to Core Damage

Figure 19.59-2 not used.

Appendix 19A Thermal Hydraulic Analysis to Support Success Criteria

The design certification of the AP1000 included consideration by the NRC of the topic referred to in this section.

Appendix 19B Ex-Vessel Severe Accident Phenomena

One of the key AP1000 severe accident design features is the capability to retain the core debris within the reactor vessel for a large number of severe accident sequences by flooding the reactor cavity and submerging the outer surface of the reactor vessel. The heat removal capability of the water on the external surface of the reactor vessel prevents the reactor vessel wall from reaching temperatures where failure of the reactor vessel could occur. This has been termed in-vessel retention (IVR) and is described in detail in Chapter 39 of the AP1000 Level 2 PRA. The primary benefit of in-vessel retention of the core is that ex-vessel severe accident phenomena associated with relocation of core debris to the containment, which can be a dominant containment failure mechanism, are physically prevented. Thus, retention of the core within the reactor vessel results in a significant reduction in the potential for large fission product releases to the environment for core damage accidents.

The probability of various levels of fission product releases (release categories) has been determined in the AP1000 Level 2 PRA, using a containment event tree which describes the various severe accident phenomena that can impact the fission product release quantities and probability of release. In the quantification of the AP1000 Level 2 PRA it was conservatively assumed that the containment would fail at the time of reactor vessel failure for all core damage sequences in which the core debris could not be retained within the reactor vessel. The two principle ways identified in the Level 2 PRA of retaining the core within the reactor vessel are reflooding the core with water before the core begins to relocate within the reactor vessel and submerging the outer surface of the reactor vessel to the reactor coolant loop nozzles. Using this approach, the regulatory and industry severe accident performance targets for the AP1000 design criteria were met. Therefore, it was considered unnecessary to investigate the consequences of reactor vessel failure on a realistic basis, including quantification of uncertainties.

The AP1000 design includes features to enhance the likelihood of retaining the core within the reactor vessel for severe accident sequences. These features include:

- Depressurization of the reactor coolant system (RCS) in the event of an accident by either automatic or manual actuation of the highly reliable automatic depressurization system (ADS)
- A containment layout wherein the water relieved from the reactor coolant system (either from the ADS discharge or a break in the RCS) accumulates in the reactor cavity region
- The capability to manually initiate flooding of the reactor cavity by gravity draining the in-containment refueling water storage tank (IRWST) into the reactor cavity
- The absence of in-core penetrations in the reactor vessel bottom head eliminates a possible reactor vessel failure mode
- The reactor cavity layout provides for rapid flooding of the reactor vessel to the reactor coolant loop nozzle elevation
- The reactor vessel insulation design promotes the two-phase natural circulation in the vessel cooling annulus
- The external reactor vessel surface treatment is bare metal

Some of the AP1000 design features to reduce the probability of a core damage accident and to enhance the likelihood of in-vessel retention of core debris in the event of a core damage accident are counter to the design philosophy that would be used to mitigate the consequences of ex-vessel severe accident phenomena. In particular, two of the design features are mutually exclusive between

preventing ex-vessel phenomena and mitigating the consequences of ex-vessel phenomena. On balance, the AP1000 severe accident risk profile is substantially reduced by the features that prevent ex-vessel severe accident phenomena. Two of the more noteworthy features are:

- The large mass of the AP1000 core provides for a slower accident progression, which enhances the capability to prevent a core damage accident (i.e., a reduced core damage frequency). The larger mass of core materials may result in more severe consequences from some of the potential ex-vessel phenomena such as core debris coolability and core concrete interactions.

- The small reactor cavity floor area reduces the amount of water required to completely submerge the reactor vessel. The small cavity floor area also provides for a more rapid flooding of the cavity if manual initiation of IRWST draining to the reactor cavity is required to submerge the reactor vessel. The small reactor cavity floor area may result in more severe consequences from some of the severe accident ex-vessel phenomena such as core debris coolability and core concrete interactions.

The purpose of this section is to provide the results of a limited number of deterministic investigations of the consequences of ex-vessel severe accident phenomena for the AP1000 design. The results of these deterministic investigations show that the challenges to the integrity of the containment posed by ex-vessel severe accident phenomena are generally within the structural capability of the containment. From these investigations, the conclusion is the capability to prevent large fission product releases to the environment does not depend on the ability to retain the core within the reactor vessel for core damage accident sequences.

The limited deterministic investigations of ex-vessel severe accident phenomena described in this section includes: ex-vessel steam explosions, direct containment heating and core concrete interactions. These ex-vessel phenomena are strongly dependent on the assumptions made concerning the mode of reactor vessel failure for the AP1000 design. Therefore, the reactor vessel failure mode is described first, followed by a description of the ex-vessel phenomena investigations.

19B.1 Reactor Vessel Failure

The AP1000 reactor vessel has a main cylindrical section approximately 4 meters in diameter and a hemispherical bottom head. The bottom head is approximately 15 cm (6 inches) thick and is made of carbon steel with an inner cladding of stainless steel to prevent contact between reactor coolant and carbon steel during normal plant operations. The bottom head of the reactor vessel does not contain any discontinuities or penetrations that could impact the mode of reactor vessel failure as the molten core material relocates to the bottom head.

Based on the similar vessel configurations of AP600 and AP1000, the possible failure modes for the AP600 reactor vessel, as documented in Reference 19B-1, are extended to the AP1000. The most likely failure mode is creep failure of the vessel wall due to heating of the vessel wall by the core debris that has relocated to the reactor vessel bottom head. Since creep failure is a strongly temperature-dependent phenomenon, the location of the failure is predicted to be at the upper surface of the core debris pool that has relocated to the reactor vessel bottom head. For most severe accident sequences, this location is near the junction of the hemispherical bottom head and the cylindrical portion of the vessel.

As described in Reference 19B-2, the presence of water on the external surface of the reactor vessel, as in the case of a flooded reactor cavity, does not alter the conclusion that the highest heat fluxes to the reactor vessel walls will be at a point near the top of the in-vessel molten core pool. This would correspond to the region of the reactor vessel most susceptible to creep failure. However,

reactor vessel failure will not occur for the case in which the reactor coolant system is depressurized and the reactor cavity is filled with water to the reactor coolant loop elevation.

For the case in which the outside of the reactor vessel is initially submerged but a sufficient in-flow of water to the reactor cavity cannot be maintained, the reactor vessel wall location experiencing the highest heat fluxes would uncover and lose its external cooling before other locations on the reactor vessel lower head. Thus, creep failure of the vessel would be expected to occur at the same location as the case with no water in the reactor cavity.

Two reactor vessel failure cases, as described below, are carried through the deterministic analyses of ex-vessel steam explosions and core concrete interactions. For the consideration of ex-vessel steam explosions and core concrete interactions, it is assumed that the reactor vessel is initially submerged in water but that gravity draining of water from the IRWST does not occur. As the water in the reactor cavity boils down, the outside of the reactor vessel at the elevation at the top of the in-vessel core pool will dry out and begin to heat up. As the vessel wall heats up, it undergoes thinning due to dissolution and melting until failure occurs. The manner in which the reactor vessel fails is treated in two separate scenarios described below.

In the first scenario, the formation of a localized opening occurs due to asymmetric heating around the circumference followed by the vessel tearing around nearly all of its circumference. This would result in the bottom part of the reactor vessel and the bottom head hinging such that the lower head swings downward and comes to rest on the cavity floor. This behavior is illustrated in Figure 19B-1. A hinging type of failure would result in an immediate pouring of core debris onto the cavity floor with metal flowing ahead of oxide. The relationship between the height of the reactor vessel above the floor is such that all but a minor part of the oxide melt would be free to flow immediately out of the head.

In the second scenario, the head and bottom part of the vessel do not hinge downward. In this scenario, the formation of a localized opening permits molten core debris to drain into the cavity lowering the in-vessel core debris depth and thereby decreasing the thermal load on the vessel wall formerly adjacent to the melt. This type of failure is illustrated in Figure 19B-2. In this case, the continued boildown of water level is followed by the release of the core debris located above the water level after a delay interval during which heatup, thinning, and localized failure of the wall will occur. Over time, the elevation of the failure location moves downward over the vessel wall and lower head. This type of failure gives rise to a very slow release rate with the core debris first relocating downward through the water before collecting and spreading on the cavity floor.

19B.2 Direct Containment Heating

Direct containment heating (DCH) is defined as the rapid energy addition to the containment atmosphere as a result of several physical and chemical processes that can occur if the core debris is forcibly ejected from the reactor vessel. The prerequisites for direct containment heating are vessel failure occurs at a location where a substantial portion of the core debris that has relocated to the lower head is ejected into the reactor cavity before the RCS gases are discharged from the RCS and the RCS is at a high pressure (sometimes called high pressure melt ejection or HPME).

To preclude the potential for high-pressure core melt ejection leading to containment failure via DCH, SECY-93-087 (Reference 19B-4) directs passive light water reactor (LWR) designs to:

- Provide a reliable depressurization system
- Provide cavity design features to decrease the amount of ejected core debris that reaches the upper compartment

The AP1000 design incorporated design features that prevent high-pressure core melt. These features include the passive residual heat removal (PRHR) system and the ADS, both subsystems of the passive core cooling system (PXS). Depressurization of the AP1000 RCS in the event of an accident is provided by automatic or manual actuation of the ADS. Redundancy and diversity are included within the ADS design to ensure a highly reliable depressurization system. The ADS consists of four different valve stages that open sequentially to reduce reactor coolant system pressure in a controlled fashion. All four-valve stages are arranged into two identical groups. Different valve types/sizes are utilized within the ADS stages to provide diversity. Based on these ADS design features, a highly reliable depressurization system is provided which precludes the potential for high-pressure core melt ejection in the AP1000 design. The AP1000 PRHR and ADS subsystems are described in additional detail in Chapters 8 and 11 of the AP1000 PRA and in Section 6.3 of this document.

Even though high-pressure core melt ejection is not a likely scenario for the AP1000, SECY-93-087 directs passive LWR designs to include cavity design features to decrease the amount of ejected core debris from reaching the upper compartment. The AP1000 design includes design features to retain and quench the core debris within the reactor cavity in the unlikely event of core debris relocation outside the reactor vessel. These features include:

- A containment layout wherein the water accumulates in the reactor cavity region
- The capability to manually initiate flooding of the reactor cavity by gravity draining the IRWST into the reactor cavity
- The reactor cavity geometry is arranged to provide a torturous pathway from the reactor cavity to the loop compartment and no direct pathway for the impingement of debris on the containment shell

19B.3 Ex-Vessel Steam Explosions

The first level of defense for ex-vessel steam explosion is the in-vessel retention of the molten core debris. If molten debris does not relocate from the vessel to the containment, there are no conditions for ex-vessel steam explosion. In the event that the reactor cavity is not flooded and the vessel fails, the PRA containment event tree assumes that the containment fails in the early time frame.

An analysis of the structural response of the reactor cavity was performed for the AP600 (Reference 19B-3). As in the in-vessel steam explosion analysis, the results of this AP600 ex-vessel steam explosion analysis are extended to the AP1000. The vessel failure modes for AP600 and AP1000 are the same. The initial debris mass participating in the interaction, superheat and composition are assumed to be the same as for AP600. The mass assumption is conservative since the AP1000 reactor vessel lower head is closer to the cavity floor resulting in less debris mass participating in the interaction. The reactor cavity geometry and water depth prior to vessel failure are the same as AP600. Therefore, the results of the AP600 ex-vessel steam explosion analysis are considered to be appropriate for the AP1000.

19B.4 Core Concrete Interactions

If the reactor vessel fails when the RCS is at a low pressure, the molten core debris will pour from the reactor vessel onto the reactor cavity floor. If a steam explosion does not occur, the pour will spread over the cavity floor and begin to transfer heat to the concrete floor of the reactor cavity. Due to the predicted mode of reactor vessel failure and the shape of the AP600 reactor cavity, analyses of the possible spreading of the core debris over the cavity floor were conducted. The results were used as input to the MAAP4 code for analysis of core concrete interactions for AP1000.

An investigation of the spreading of core debris that pours into the reactor cavity was conducted for reactor vessel failure that occurs at low RCS pressure. The investigation considered the vessel failure mode and location, as well as the recognition that the oxide and metal components of the in-vessel core debris are predicted to be separated. Since the oxide and metal components of the core debris have very different physical characteristics (e.g., viscosity or heat capacity), the separated in-vessel layers influence the spreading of the core debris in the reactor cavity. The melt spreading analysis was conducted for two reactor vessel failure modes, hinged and localized failures.

For the hinged vessel failure case, the analysis results show that the core debris is spread relatively uniformly over the reactor cavity floor. However, the distribution of the metal and oxide components of the core debris is not uniformly distributed over the reactor cavity floor. In the region directly under the reactor vessel, the core debris consists primarily of the oxide component. At the opposite end of the reactor cavity, the core debris consists mainly of the metal component of the core debris released from the reactor vessel. The core debris is still almost totally molten at the end of the spreading analysis.

A different behavior is predicted for the localized reactor vessel failure case. The analysis predicts that the core debris will accumulate at the reactor vessel end of the reactor cavity. The distribution of the metal and oxide components of the core debris is not uniformly distributed over the reactor cavity floor. In the region directly under the reactor vessel, the core debris consists primarily of the oxide component. At the opposite end of the reactor cavity, the core debris consists mainly of the metal component of the core debris released from the reactor vessel. The core debris is almost totally frozen at the end of the spreading analysis.

The core concrete interactions for the AP1000 design were analyzed for two concrete types: basaltic concrete and common limestone-sand concrete. The common limestone-sand concrete has a significantly higher noncondensable gas generation rate, compared to basaltic concrete and should therefore present a more severe containment pressurization transient. On the other hand, the basaltic concrete suffers higher ablation rate, due to its physical properties (mainly, its lower decomposition energy), and should therefore present a more severe basemat penetration failure mode, compared to common limestone-sand concrete. In all cases, a 3.5 m deep water pool is initially present in the cavity while debris is being released into it.

Based on analyses, it can be concluded that: a) the goal of protecting the containment fission product boundary during the first 24 hours of a core melt accident is met, b) it is not necessary to specify a concrete type for the containment basemat since credible containment basemat failure that could lead to fission product releases to the atmosphere are likely to occur at times well beyond 24 hours, and c) the reactor cavity sump is adequately protected such that it is not a weakness in containment basemat integrity during postulated accidents that lead to core concrete interactions.

19B.4.1 Containment Pressurization due to Core Concrete Interactions

The containment pressurization due to steam and noncondensable gas generation during the episodes of core concrete interactions described above was assessed to determine the effect of core concrete interactions on the containment integrity.

The indicator of a challenge to containment integrity for the containment pressurization due to the noncondensable gases produced from core concrete interactions is the Service Level “C” pressure, which is 91 psig (0.73 MPa). This is well below the 50 percent containment failure probability value of 135 psig (1.03 MPa).

The results also show that, in all cases the containment does not pressurize to Service Level “C” containment challenge indicator value prior to the time that the core debris completely penetrates the containment basemat. Thus, for these cases there is no potential challenge to containment integrity

due to overpressurization since: a) there is no longer a source of mass and energy input to the containment after the core debris penetrates the entire basemat, and b) basemat penetration assures that the containment will be depressurized through the basemat failure.

Based on these analyses, it can be concluded that it is not necessary to specify a concrete type for the containment basemat since containment overpressure failure due to non-condensable gas generation from core concrete interactions is not likely for any credible severe accident scenarios.

19B.5 Conclusions

The results of the limited deterministic analyses of ex-vessel severe accident phenomena presented in this section show that early containment failure is not a certainty if the reactor vessel fails. Based on the deterministic analyses, direct containment heating that might ensue from a high pressure melt ejection would not challenge the integrity of the containment. Ex-vessel steam explosions, assessed on a very conservative basis would not produce impulse loads that would challenge the integrity of the containment due to localized failures of the reactor cavity floor and walls. In addition, these analyses indicate that the ex-vessel steam explosion loads are not strong enough to displace the reactor vessel from its location inside the biological shield. Thus, there is no challenge to any containment penetrations connected to the reactor vessel or to the reactor coolant loops. In the case of a vessel failure at a low RCS pressure, the core concrete interactions analyses indicate that the containment integrity would not be challenged in the first 24 hours of the event and thus no significant releases of fission products are predicted in that time frame.

Thus, it is concluded that prevention of large fission product releases to the environment is not dependent on the integrity of the reactor vessel. If reactor vessel failure occurs, there may be challenges to the containment integrity, but these challenges are highly uncertain and the most likely challenge (containment failure by core penetration of the cavity basemat) would not occur in the first 24 hours of the accident. Thus, the AP1000 assumption that reactor vessel failure always leads to containment failure is a conservatism in the AP1000 risk profile.

19B.6 References

19B-1. “AP600 Phenomenological Evaluation Summaries,” WCAP-13388 (Proprietary) Rev. 0, June 1992 and WCAP-13389 (Nonproprietary), Rev. 1, 1994.

19B-2. Theofanous, T. G., et al., “In-Vessel Coolability and Retention of a Core Melt,” DOE/ID-10460, July 1995.

19B-3. “AP600 Probabilistic Risk Assessment,” GW-GL-022, August 1998.

19B-4. “Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Design,” SECY-93-087, dated April 2, 1993.

TABLE 19B-1 NOT USED.

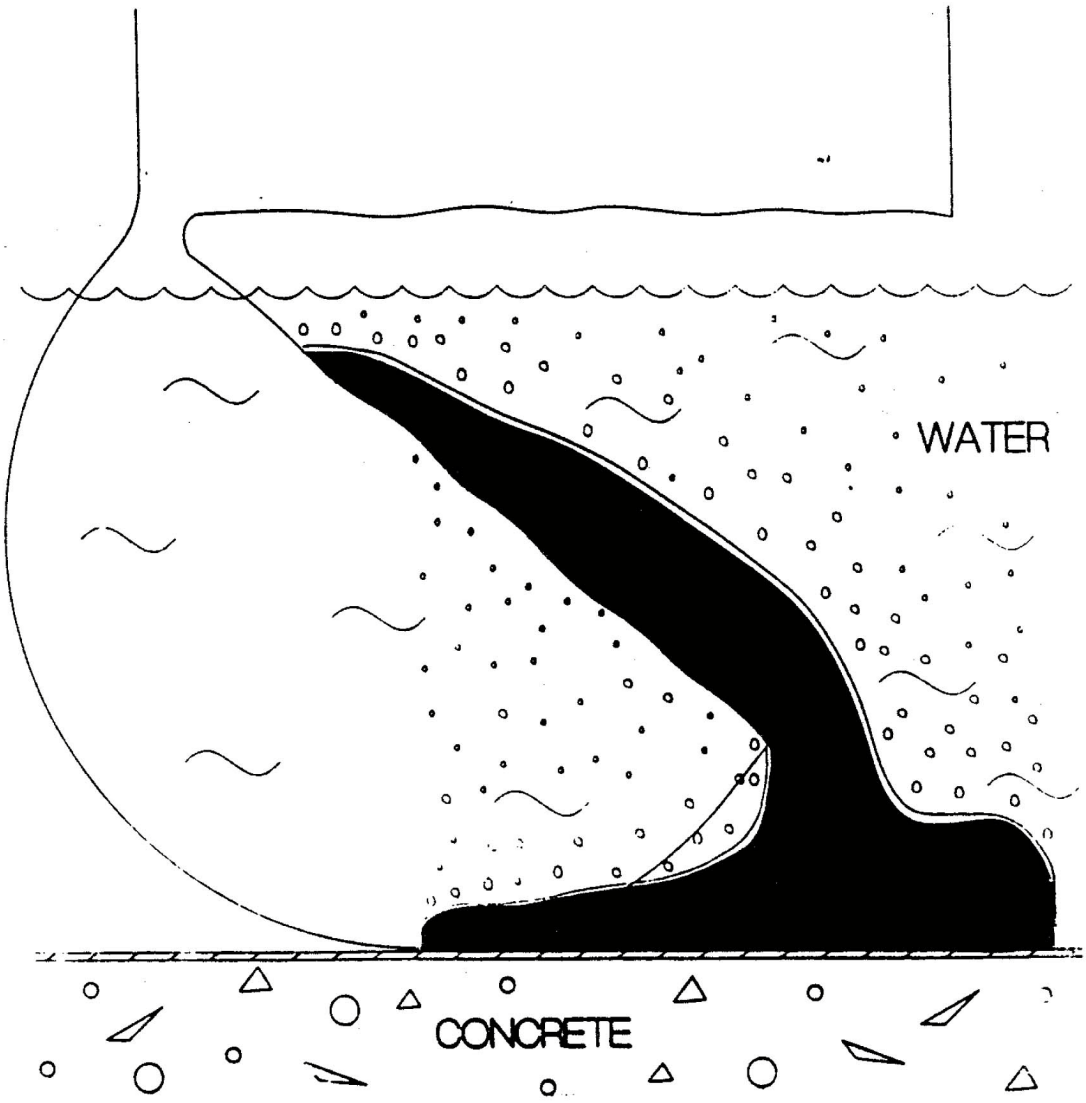

Figure 19B-1 Illustration of Hinging Type of Failure Resulting in Rapid Melt Release

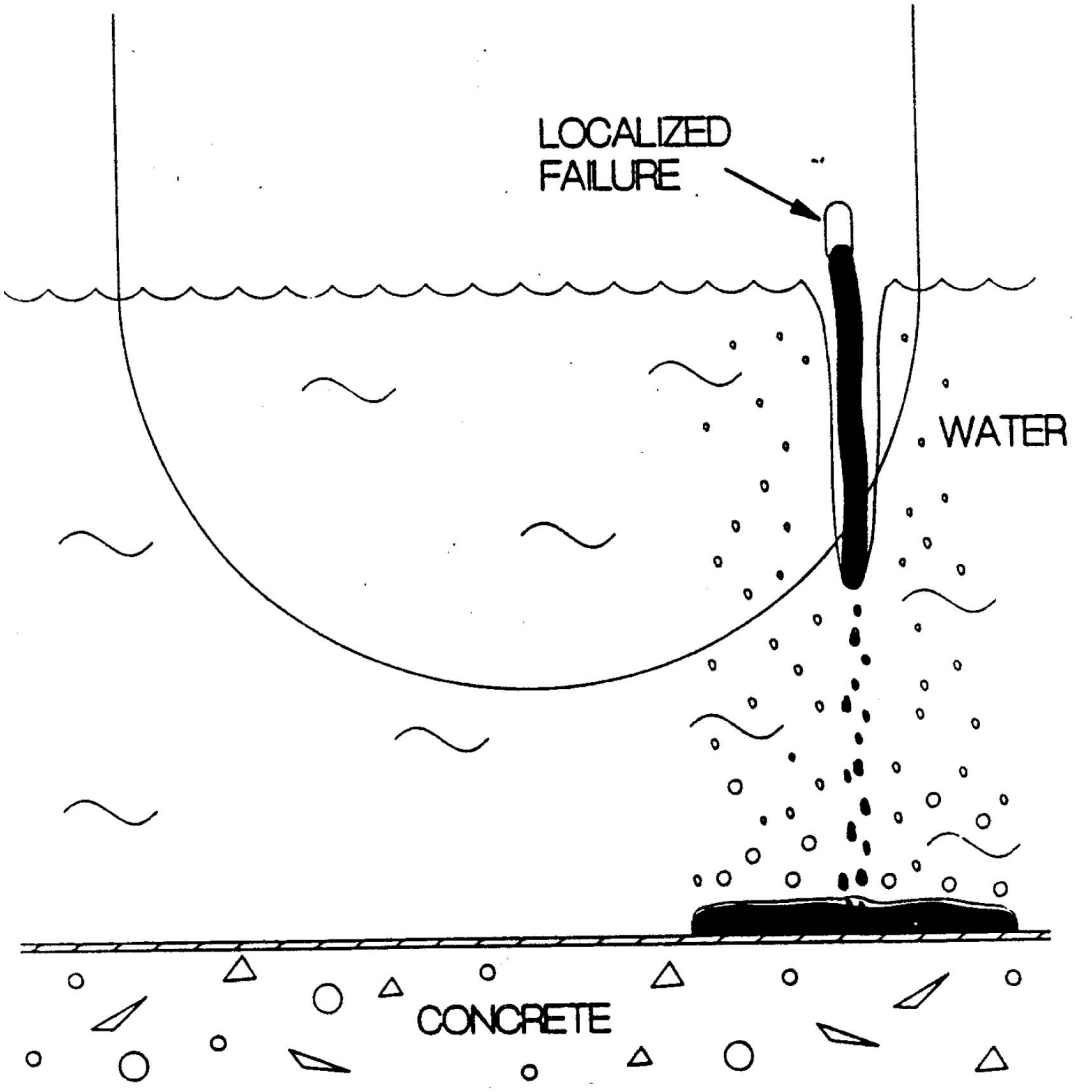

Figure 19B-2 Illustration of Localized Type of Failure Resulting in Slow Melt Release

FIGURES 19B-3 THROUGH 19B-8b NOT USED.

Appendix 19C Additional Assessment of AP1000 Design Features

The AP1000 PRA model, like many other conventional PRA models, is an evolving model. It is revised, as needed, to keep up with design changes and to implement revisions identified by various reviews, applications, and related analyses. Due to the iterative nature of the interface between the PRA analysts and the plant designers, it is not always possible to incorporate all differences identified between the plant design and the PRA model in a timely manner. This appendix is intended to summarize known differences between the two, and identify any future changes planned to the current PRA model to address these differences.

Planned Revisions to AP1000 PRA Model

Several changes to the PRA were previously considered by preliminary evaluations. These evaluations indicated the changes are of low importance to the PRA results. These changes are listed here for consideration and include the following:

1. Containment isolation event trees.

2. Correction of ADR fault tree top logic to reflect the success criteria (logic was conservative).

3. Success criteria for medium LOCA (including CMT and DVI line breaks) will be modified to credit the PRHR heat exchanger for those instances when the accumulators are assumed to fail. The impact on the overall PRA results for this change is not expected to be significant.

Preliminary quantification shows that the plant CDF is not affected by this revision. The large release frequency (LRF) is not expected to be affected either.

Appendix 19D Equipment Survivability Assessment

19D.1 Introduction

The purpose of the equipment survivability assessment is to evaluate the availability of equipment and instrumentation used during a severe accident to achieve a controlled, stable state after core damage under the unique containment environments. Severe accident phenomena may create harsh, high temperature and pressure containment environments with a significant concentration of combustible gases. Local or global burning of the gases may occur, presenting additional challenges to the equipment. Analyses demonstrate that there is reasonable assurance that equipment used to mitigate and monitor severe accident progression is available at the time it is called upon to perform.

The methodology used to demonstrate equipment survivability is:

- Identify the high level actions used to achieve a controlled, stable state
- Define the accident time frames for each high level action
- Determine the equipment and instruments used to diagnose, perform and verify high level actions in each time frame
- Determine the bounding environment within each time frame
- Demonstrate reasonable assurance that the equipment will survive to perform its function within the severe environment.

19D.2 Applicable Regulations and Criteria

Equipment that is classified as safety-related must perform its function within the environmental conditions associated with design-bases accidents. The level of assurance provided by equipment required for design-bases events is “equipment qualification.”

The environmental conditions resulting from beyond design basis events may be more limiting than conditions from design-bases events. The NRC has established criteria to provide a reasonable level of assurance that necessary equipment will function in the severe accident environment within the time span it is required. This criterion is referred to as “equipment survivability.”

The applicable criteria for equipment, both mechanical and electrical, required for recovery from in-vessel severe accidents are provided in 10 CFR 50.34(f):

- Part 50.34(f)(2)(ix)(c) states that equipment necessary for achieving and maintaining safe shutdown of the plant and maintaining containment integrity will perform its safety function during and after being exposed to the environmental conditions attendant with the release of hydrogen generated by the equivalent of a 100 percent fuel-clad metal-water reaction including the environmental conditions created by activation of the hydrogen control system.
- Part 50.34(f)(2)(xvii) requires instrumentation to measure containment pressure, containment water level, containment hydrogen concentration, containment radiation intensity, and noble gas effluent.
- Part 50.34(f)(2)(xix) requires instrumentation adequate for monitoring plant conditions following an accident that includes core damage.

- Part 50.44(c)(2) states that systems necessary to ensure containment integrity shall be demonstrated to perform their function under conditions associated with an accident that releases hydrogen generated from 100-percent fuel-clad metal-water reaction.

Part 50.44(c)(4) states that equipment must be provided for monitoring hydrogen in the containment that is functional, reliable, and capable of continuously measuring the concentration of hydrogen in the containment atmosphere following a significant beyond design-basis accident for accident management, including emergency planning. The applicable criteria for equipment, both electrical and mechanical, required to mitigate the consequences of ex-vessel severe accidents are discussed in Section III.F, “Equipment Survivability” of SECY-90-016. The NRC recommends in SECY-93-087 that equipment provided only for severe accident protection need not be subject to 10 CFR 50.49 equipment qualification requirements, the 10 CFR 50 Appendix B quality assurance requirements, or 10 CFR 50 Appendix A redundancy/diversity requirements. However, mitigation features must be designed to provide reasonable assurance they will operate in the severe accident environment for which they are intended and over the time span for which they are needed.

19D.3 Definition of Controlled, Stable State

The goal of accident management is to achieve a controlled, stable state following a beyond design basis accident. Establishment of a controlled, stable state protects the integrity of the containment pressure boundary. The conditions for a controlled, stable state are defined by APP-GW-GL-027, the “Framework for AP1000 Severe Accident Management Guidance” (SAMG) (Reference 19D-1).

For a controlled, stable core state:

- A process must be in place for transferring the energy being generated in the core to a long-term heat sink.
- The bulk core temperature must be well below the point where chemical or physical changes might occur.

For a controlled, stable containment state:

- A process must be in place for transferring the energy that is released to the containment to a long-term heat sink.
- The containment boundary must be protected.
- The containment and reactor coolant system conditions must be well below the point where chemical or physical processes (severe accident phenomena) might result in a dynamic change in containment conditions or a failure of the containment boundary.

19D.4 Definition of Equipment Survivability Time Frames

The purpose of the equipment survivability time frames is to identify the time span in the severe accident in which specific equipment is required to perform its function. The phenomena and environment associated with that phase of the accident defines the environment which challenges the equipment survivability. The equipment survivability time frame definitions are summarized in Table 19D-1.

19D.4.1 Time Frame 0 - Pre-Core Uncovery

Time Frame 0 is defined as the period of time in the accident sequence after the accident initiation and prior to core uncovery. The fuel rods are cooled by the water/steam mixture in the reactor vessel.

The accident has not yet progressed beyond the design basis of the plant, and hydrogen generation and the release of fission products from the core is negligible. Emergency Operating Procedures (EOPs) are designed to maintain or recover the borated water inventory and heat removal in the reactor coolant system to prevent core uncovery and establish a safe, stable state. Recovery within Time Frame 0 prevents the accident from becoming a severe accident. Equipment survivability in Time Frame 0 is covered under the design basis equipment qualification program for the primary accident management strategies.

19D.4.2 Time Frame 1 - Core Heatup

Time Frame 1 is defined as the period of time after core uncovery and prior to the onset of significant core damage as evidenced by the rapid zirconium-water reactions in the core. This is the transition period from design basis to severe accident environment. The overall core geometry is intact and the uncovered portion of the core is overheating due to the lack of decay heat removal. Hydrogen releases are limited to relatively minor cladding oxidation and some noble gas and volatile fission products may be released from the fuel-clad gap due to rupture of fuel rod cladding at these higher temperatures. As the core-exit gas temperature increases above 1200 degrees F, the EOPs transition to a red path indicating inadequate core cooling (FR-C.1). Upon entry into FR-C.1, the control room staff initiates actions to mitigate a severe accident by turning on the hydrogen igniters for hydrogen control and flooding the reactor cavity to prevent reactor pressure vessel failure. The operators attempt to reduce the core temperature by depressurizing the RCS and re-establish the borated water inventory in the reactor coolant system. Recovery in Time Frame 1 prevents the accident from becoming a core melt. In general, the containment conditions are expected to be within the design basis conditions while the reactor vessel and RCS conditions will be slightly above the design basis. Equipment survivability in Time Frame 1 is evaluated to demonstrate it is within the equipment qualification envelope except for components inside the RCS pressure boundary.

19D.4.3 Time Frame 2 - In-Vessel Severe Accident Phase

Time Frame 2 is the period of time in the severe accident after the accident progresses beyond the onset of rapid zirconium-water reactions and prior to the establishment of a controlled, stable state (end of in-vessel core relocation), or prior to reactor vessel failure. The onset of rapid zirconium-water reactions of the fuel rod cladding and hydrogen generation defines the beginning of Time Frame 2. The heat of the exothermic reaction accelerates the degradation, melting and relocation of the core. Fission products are released from the fuel-clad gap as the cladding bursts and from the fuel matrix as the UO_2 pellets melt. Over the period of Time Frame 2, the initial, intact geometry of the core is lost as it melts and relocates downward. Severe accident management strategies exercised during Time Frame 2 are designed to recover reactor coolant system inventory and heat removal, to maintain reactor vessel integrity and to maintain containment integrity. Recovery actions in Time Frame 2 may create containment environmental challenges by increasing the rate of hydrogen and steam generation.

19D.4.4 Time Frame 3 - Ex-Vessel Severe Accident Phase

Time Frame 3 is defined as the period of time after the reactor vessel fails until the establishment of a controlled, stable state. The AP1000 design and the AP1000 EOPs provide the capability to flood the reactor vessel and depressurize the RCS to prevent vessel failure in a severe accident. This severe accident Time Frame 3 is predicted to be a very low probability event. However, it is included in the SAMG to provide guidance in the event that reactor vessel failure occurs. Molten core debris is relocated from the reactor vessel onto the containment cavity floor which creates the potential for rapid steam generation, core-concrete interaction and non-condensable gas generation. Severe accident management strategies implemented in Time Frame 3 are designed to monitor the accident progression, attempt to re-establish a coolable core configuration on the containment floor, maintain containment integrity and mitigate fission product releases to the environment.

19D.5 Definition of Active Operation Time

Equipment only needs to survive long enough to perform its function to protect the containment fission product boundary. In the case of some items, such as valves or motor-operators, once the equipment performs its function, and changes state (e.g., opens), the function is completed. An exception to this is solenoid-operated valves that must maintain a position other than their design basis failure position (e.g., a fail closed AOV that must remain open for a strategy to remain effective). For other items, such as pumps, the equipment must operate continuously to perform its function. The time of active operation is the time during which the equipment must perform its function.

19D.6 Equipment and Instrumentation for Severe Accident Management

The AP1000 EOPs (Reference 19D-2) and severe accident management guidance (SAMG) framework (Reference 19D-1) define actions that accomplish the goals for achieving a controlled, stable state and terminating fission product releases in an accident. The high level actions from the accident management framework are summarized in Table 19D-2 and provide the basis for identifying equipment. This section discusses the EOP and SAMG actions within each of the time frames of the accident to determine the equipment and instrumentation and the active operation time in which they are needed to provide reasonable assurance of achieving a controlled, stable state.

The AP1000 SAMG (Reference 19D-3) provides the primary input to the selection of the instrumentation used for monitoring the actions. The instrument used to diagnose the need for the action and monitor the response are listed. Instruments to evaluate potential negative impacts are covered under other high level actions in the framework and therefore are also considered for survivability.

The equipment and instrumentation used in each time frame are summarized in Tables 19D-3 through 19D-5. Although the SAMG considers all possible paths for each high level action, only the primary method is listed in Tables 19D-4 and 19D-5 for the equipment survivability assessment.

19D.6.1 Time Frames 0 and 1 - Accident Initiation, Core Uncovery and Heatup

Time Frame 0 represents the accident time prior to core uncovery. Time Frame 1 represents the time following core uncovery, but prior to the rapid oxidation of the core. Aside from potential ballooning of the cladding, the core has not lost its initial intact geometry and coolability is assured by recovering the core with borated water.

During Time Frames 0 and 1, most of the equipment that is automatically actuated will receive a signal to start. However, given that the accident has progressed to core uncovery and heatup, some critical equipment has not actuated. From accident initiation until the time of core uncovery (Time Frame 0) the conditions are bounded by the design basis and covered under equipment qualification. During Time Frame 1, the containment environment is still within the design basis of the plant and the control room is operating within the Emergency Operating Procedures, but the conditions have degraded. Accident management to achieve a controlled, stable state, via the EOPs, is geared toward recovering the core cooling before the coolable geometry is lost.

19D.6.1.1 Injection into the RCS

Failure of RCS injection is likely to be the reason the accident has proceeded to core uncovery. Successful injection into the RCS removes the sensible and decay heat from the core. Prior to the onset of rapid oxidation of the cladding, successful RCS injection recovers the accident before it progresses to substantial damage and establishes a controlled, stable state. Failure to inject into the RCS at a sufficient rate allows the accident to proceed into Time Frame 2 and the SAMG.

The equipment and systems used to inject into the RCS during Time Frame 0 and 1 are the core makeup tanks, accumulators and IRWST (which are part of the passive core cooling system (PXS)), the chemical and volume control system (CVS) makeup pumps, and the normal residual heat removal (RNS) pumps. For non-LOCA and small LOCA sequences, depressurization of the RCS using the automatic depressurization system (ADS) is required for successful injection.

The plant response is monitored using the system flow rates, IRWST water level indication, RCS pressure, core-exit temperature, and RCS temperature.

19D.6.1.2 Injection into Containment

The operator is instructed via the EOPs to inject water into the containment to submerge the reactor vessel and cool the external surface if core overheating begins to occur. This action is performed later in Time Frame 1, but prior to entry into the SAMG. Successful cavity flooding, in conjunction with RCS depressurization, prevents vessel failure in the event of molten core relocation to the vessel lower head. Failure of cavity flooding allows the accident to proceed to vessel failure and molten core relocation into the containment (Time Frame 3) if timely injection into the reactor vessel cannot be established to cool the core and prevent substantial core relocation to the lower head.

The PXS motor-operated and squib recirculation valves are opened manually to drain the IRWST water into the containment in Time Frame 1.

The plant response is monitored by core-exit temperature, containment water level indication, and IRWST water level indication.

19D.6.1.3 Decay Heat Removal and Injection into the Steam Generators

In the event of non-LOCA or small LOCA sequences, the RCS pressure is elevated above the secondary pressure. In Time Frame 0, the SGs and PRHR are used for decay heat removal. Note that PRHR is effective only in Time Frame 0. Failure of the PRHR may be the reason that the event proceeds to core overheating. Recovery of the PRHR will provide decay heat removal. Failure of feedwater to the steam generators with the PRHR failed may also be a cause for core overheating and recovery of injection to the steam generators may be required. If the steam generators remain dry without PRHR recovery and the core is uncovered, the tube integrity or hot leg nozzle integrity may be threatened by creep rupture failure at the onset of rapid oxidation (entry into Time Frame 2) if the RCS is at a high pressure. Injecting to the steam generators provides a heat sink to the RCS by boiling water on the secondary side, and protects the tubes by cooling them. Successful steam generator injection can establish a controlled, stable state if the losses from the RCS can be recovered and mitigated. Failure to inject to the steam generator requires depressurization of the RCS to prevent creep rupture failure of the tubes and loss of the containment integrity at the onset of rapid oxidation in Time Frame 2.

For accident sequences initiated by steam generator tube rupture, the procedures instruct the control room to isolate feedwater to the faulted steam generator, and to use feedwater to the intact steam generator in conjunction with steam generator depressurization and PRHR initiation to cooldown the reactor coolant system and isolate the break. In Time Frame 1, PRHR initiation or feed to the intact steam generators may be used to re-establish a primary heat sink to cooldown the RCS and a controlled, stable state if the losses from the RCS can be recovered and mitigated. Failure to recover the PRHR or to feed the intact steam generator may lead to a continued loss of coolant to the faulted steam generator and progression to Time Frame 2.

The main feedwater and startup feedwater pumps are used to inject into a pressurized secondary system. The AP1000 plant design does not allow for use of low pressure systems (e.g., condensate, fire water, or service water) to feed the steam generators.

The plant response is monitored with the steam generator water level indication, steam line pressure, core-exit temperature, RCS temperature, IRWST temperature, and IRWST water level indication.

19D.6.1.4 Depressurize Reactor Coolant System

19D.6.1.4.1 Non-LOCA and Small LOCA Sequences

In Time Frame 0, RCS depressurization is not used for most accidents because the steam generators and PRHR are used to establish a controlled stable state.

In the event of non-LOCA or a small LOCA sequences, the RCS pressure will remain above the secondary pressure. If the steam generators are dry and the core is uncovered, the hot leg nozzle or tube integrity is threatened by creep rupture failure at the onset of rapid cladding oxidation (beginning of Time Frame 2). Timely depressurization (prior to significant cladding oxidation) of the RCS mitigates the threat to the tubes, allows injection of the accumulators and IRWST water, and provides a long-term heat sink to establish a controlled, stable state. Failure to depressurize can result in the failure of the tubes and a loss of containment integrity when oxidation begins.

For steam generator tube rupture (SGTR) initiated sequences, depressurization of the RCS can be used to isolate the faulted steam generator, and re-establish core cooling via injection.

The automatic depressurization system (ADS) is required to depressurize the RCS to allow the PXS systems to inject. However, the recovery of passive residual heat removal (PRHR) or feedwater to the steam generators will provide a substantial heat sink to depressurize the RCS and mitigate the threat to the tubes. The auxiliary pressurizer sprays are not evaluated for survivability since the inclusion of several other safety-related systems which perform the same function provides reasonable assurance of RCS depressurization in the event of a non-LOCA or small LOCA severe accident.

The RCS pressure, steam generator pressure, IRWST water level, and IRWST temperature can be used to monitor the plant response to the RCS depressurization.

19D.6.1.4.2 LOCA Sequences

In Time Frame 0, steam generators and PRHR are not effective due to low RCS pressure.

LOCA sequences (other than small LOCA sequences) by definition are depressurized below the secondary system pressure by the initiating event and therefore, are not a threat to steam generator tube integrity upon the onset of rapid oxidation. Depressurization may be required for injection to establish a long-term heat sink. Medium LOCAs require additional depressurization to allow the injection of RNS or PXS. Large LOCAs are fully depressurized by the initiating event.

In LOCA sequences, the ADS is effective in providing depressurization capability to allow injection to the RCS. While RCS cooldown and depressurization using the steam generators could be effective, it is not evaluated here for survivability for LOCA sequences. RCS cooldown using pressurizer sprays was determined to not be effective for the larger LOCA sequences because of the loss of communication between the RCS and the pressurizer for these sequences.

The RCS pressure can be used to monitor the plant response to the RCS depressurization.

19D.6.1.4.3 Prevent Reactor Vessel Failure

Depressurization of the RCS, along with injecting into the containment is an accident management strategy to prevent vessel failure. The depressurization of the RCS reduces the stresses on the

damaged vessel wall facilitating the in-vessel retention of core debris. To prevent reactor vessel failure, the RCS must be depressurized to nearly containment conditions.

The ADS is used to depressurize the RCS to prevent reactor vessel failure. The use of the steam generators to depressurize the RCS to prevent vessel failure was determined to not be effective because it cannot bring the RCS pressure down far enough in the time frame of interest for accidents that progress to Time Frame 1 (i.e., no water on primary side of steam generators).

The RCS pressure can be used to monitor the plant response to the RCS depressurization.

19D.6.1.5 Depressurize Steam Generators

The steam generators may be depressurized to depressurize the RCS in non-LOCA and small LOCA sequences. Injection to the steam generator must be available to depressurize the secondary system to prevent creep rupture failure of the tubes.

The steam generator PORV and main steam bypass valves are used for depressurizing the steam generators. The MSIV must be opened in order to use the main steam bypass valves.

Depressurization of the steam generators is used in the EOPs as a means to cool down and depressurize the RCS. Depressurization of the steam generators is called for in the EOPs and is appropriate only in Time Frame 1 as the RCS is depressurized in order to minimize the pressure differential across the steam generator tubes.

The steam line pressure, steam generator water level, and RCS pressure can be used to monitor the plant response.

19D.6.1.6 Containment Heat Removal

Containment heat removal is not explicitly listed as a high level action in the AP1000 SAMG Framework, but it is implicit in the high level action “Depressurize Containment.” Containment heat removal is provided by the passive containment cooling system (PCS). Water cooling of the shell is needed to establish a controlled, stable state with the containment depressurized. The actuation of PCS water is typically automatic in Time Frame 0.

PCS water is supplied to the external surface of the containment shell from the PCS water storage tank or the post-72 hour PCS ancillary water tank. Alternative water sources can be provided via separate connections outside containment.

The containment heat removal can be monitored with the containment pressure and the PCS water flowrate or PCS water and PCS ancillary water storage tank levels.

19D.6.1.7 Containment Isolation

Containment isolation is not explicitly listed as a high level action in the AP1000 SAMG Framework, but it is implicit as a requirement to protect the fission product barrier.

Containment isolation is provided by an intact containment shell and the containment isolation system which closes the isolation valve in lines penetrating the containment shell that may be open to either the RCS or containment atmosphere following an accident.

The containment isolation can be monitored by the containment pressure and the containment isolation system valve positions.

19D.6.1.8 Hydrogen Control

Maintaining the containment hydrogen concentration below a globally flammable limit is a requirement for a controlled, stable state. The containment can withstand the pressurization from a global deflagration. While hydrogen is not generated in a significant quantity until Time Frame 2, provisions are provided in the EOPs within Time Frame 1 to turn on the hydrogen igniters before hydrogen generation begins so that hydrogen can be burned as it is produced.

Severe accident hydrogen control in the AP1000 is provided by hydrogen igniters. The containment has passive auto-catalytic recombiners (PARs) as well, but they are not credited in the severe accidents assessments. The PARs are passive equipment that cannot be controlled by the operating staff from the control room.

The igniters are manually actuated from the control room in the EOPs on high core-exit temperature. The intention is to actuate the igniters prior to the onset of significant cladding oxidation (Time Frame 1). The containment hydrogen concentration is monitored prior to igniter actuation so that a globally flammable mixture is not unintentionally ignited by the hydrogen igniters.

The plant response to the igniter actuation can be monitored by containment hydrogen concentration using the hydrogen monitors or containment atmosphere sampling, which is part of the primary sampling system. The containment pressure response can also be used to indicate hydrogen burning, which creates a distinctive pressure global peak, but not continual hydrogen burning by the igniters because the energy release to containment is at a low rate and the containment pressure response cannot be distinguished from other heat generation processes.

19D.6.1.9 Accident Monitoring

Accident monitoring is a post-TMI requirement as outlined in 10 CFR 50.34(f). Aside from the accident management purposes outlined above, monitoring the progression of the accident and radioactive releases provides input to emergency response and emergency action levels.

Accident monitoring is provided by the in-containment monitors for pressure, hydrogen concentration, water levels, temperature and radiation, core-exit temperature, IRWST water level, RCS pressure, and steam generator radiation monitors.

19D.6.2 Time Frame 2 - In-Vessel Core Melting and Relocation

Time Frame 2 represents the period of core melting and relocation and the entry into the SAMG. The intact and coolable in-vessel core geometry is lost, and relocation of core debris into the lower head is likely. The in-vessel hydrogen generation and fission product releases from the fuel matrix occur during this time frame.

19D.6.2.1 Injection into the RCS

In Time Frame 2, the in-vessel core configuration loses its coolable geometry and it is likely that at least some of the core debris will migrate to the reactor vessel lower head. If the RCS is depressurized and the reactor vessel is submerged, the core debris will be retained in the reactor vessel. However, injection into the RCS to cover and cool the core debris is required to achieve a controlled, stable state. RCS injection is not required to protect the containment fission product boundary. Injection is successful if it is sufficient to quench the sensible heat from the core debris and refill the reactor vessel. Decay heat removal will then be accomplished by a combination of heat transfer to the water in the reactor vessel and heat transfer to the water on the exterior surface of the reactor vessel.

Severe accident studies for the AP1000 indicate that even with the reactor vessel refilled and the exterior surface of the reactor vessel submerged, the entire core debris may not return to low temperatures (e.g., less than 1200°F for a substantial period of time (e.g., months) if most of the core debris has relocated to the reactor vessel bottom head. This is due to the heat transfer rate through the outer shell of frozen core debris in relation to the heat generation in the central unfrozen core debris. However, this is an extreme case (i.e., no recovery of injection to the RCS until the entire core debris is in the reactor vessel bottom head).

Guidance for establishing RCS injection would be from the AP1000 SAMG (Reference 19D-3). Water can be injected into the RCS using the CVS or the RNS systems. The PXS (CMT, accumulator, IRWST) is not credited in Time Frame 2 in survivability assessments because automatic and manual activation of the system is attempted several times in Time Frame 0 and 1.

Post-core damage, the actions may be monitored with RCS pressure or temperature, containment pressure or CVS or RNS flow rates.

19D.6.2.2 Injection into Containment

The objective of injection to the containment prior to reactor vessel failure (Time Frame 3) is to cool the external surface of the reactor vessel to maintain the core debris in the vessel. Due to the lead time required to submerge the bottom head of the reactor vessel prior to core relocation of the bottom head, injecting to the containment for in-vessel retention is achieved by instructing the operator to drain the IRWST in the EOPs within Time Frame 1.

Since a long lead time is required to submerge the exterior surface of the RPV, the objective of injecting into containment in Time Frame 2 is to provide water in the containment if the accident progresses to RPV failure and Time Frame 3. Two methods are used to inject into containment during Time Frame 2; the containment spray and the addition of water to the IRWST to overflow into containment. There are three methods used to add makeup to the IRWST to overflow; RNS pumps, makeup pumps, and spent fuel system pumps. Draining the IRWST to containment is not credited in Time Frame 2 in survivability assessments because activation of the system is attempted several times in Time Frame 1, and diverse systems are credited to provide reasonable assurance of containment injection survivability in this time frame. If the vessel fails, the accident progresses to Time Frame 3.

Post-core damage, the actions may be monitored with containment water level indication or IRWST water level indication if IRWST overfill is used.

19D.6.2.3 Decay Heat Removal and Injection into the Steam Generators

In transients and small LOCAs, initiation of PRHR or injection into the steam generators is required to be recovered in Time Frame 1 to be successful. If the secondary side is dry and the RCS is not depressurized, the steam generator tubes can experience creep rupture due to circulation of hot gases when the cladding oxidation begins at the onset of Time Frame 2. Steam generator injection is not required for LOCAs which depressurize the RCS below the secondary system pressure.

Within Time Frame 2, steam generator injection can be utilized in unisolated SGTR sequences to maintain the water level on the secondary side for mitigation of fission product releases. Injecting into the steam generators, along with depressurization of the RCS, is an accident management action to isolate containment or scrub fission products. Failure to inject to the ruptured steam generator in Time Frame 2 can lead to continued breech of the containment fission product boundary and large offsite doses.

Steam generator feed for non-ruptured SGs is not credited in Time Frame 2 because it is attempted several times in Time Frame 0 and Time Frame 1. However, re-initiation of feedwater to the ruptured steam generator is not attempted until the SAMG, which is not used until Time Frame 2. Thus, re-initiation of feedwater is a Time Frame 2 activity.

The main feedwater and startup feedwater pumps are used to inject into a pressurized secondary system.

The plant response is monitored with the core-exit temperature, RCS temperature, steam generator water level and steam line pressure.

19D.6.2.4 Depressurize RCS

RCS depressurization is required within Time Frame 1 for facilitating in-vessel retention of core debris and for successfully preventing steam generator tube failure in high pressure severe accident sequences. The steam generator tubes or hot leg nozzles may fail due to creep rupture after the onset of rapid oxidation at the beginning of Time Frame 2. RCS depressurization facilitates in-vessel retention of core debris in conjunction with injection into the containment to give time to recover pumped injection sources to the RCS to establish a controlled, stable state. RCS depressurization is provided by instructing the operator to depressurize the system in the EOPs in Time Frame 1.

Three methods are used to depressurize the RCS during Time Frame 2: ADS, auxiliary pressurizer spray, and reactor vessel head vent. ADS and auxiliary pressurizer spray are not credited in Time Frame 2 in survivability assessments because activation of the system is attempted several times in Time Frame 1. Survivability of the reactor vessel head vent is assessed only in Time Frame 2.

19D.6.2.5 Depressurize Steam Generators

Active operation to depressurize a steam generator can be used to cooldown the RCS prior to Time Frame 2. After the onset of core melting and relocation, depressurizing steam generators could threaten steam generator tube integrity. Depressurizing the steam generator in Time Frame 2 does not facilitate the establishment of a controlled, stable state. Depressurization of the steam generators is called for in the EOPs and is appropriate only in Time Frame 1 if the RCS is depressurized in order to minimize the pressure differential across the steam generator tubes.

19D.6.2.6 Containment Heat Removal

Automatic actuation of PCS water occurs in Time Frame 0 or 1. In Time Frame 2, PCS flowrate and level are monitored to determine if additional water is needed to permit continuation of PCS flow. Alternate water sources can be provided by connections to the external PCS water tank which is outside the containment pressure boundary and not subjected to the harsh environment.

In addition to PCS water, a nonsafety-related containment spray system can provide heat removal from containment. The design basis purpose of containment spray is scrubbing fission products and containment spray is actuated on high containment radiation levels. This would most likely occur in Time Frame 2 when the fuel rods are overheated and melting. Manually actuating the containment spray system involves opening an air-operated valve inside the containment and actuating valves and a pump outside the containment. Once open, the active operation of the valve inside the containment is completed.

Post-core damage, the actions may be monitored with PCS flow rate and tank water level, containment water level, and containment pressure.

19D.6.2.7 Containment Isolation

Active operation of containment isolation valves is required in Time Frame 0 or 1 to establish the containment fission product barrier. Therefore, only the survivability of the containment pressure boundary, including penetrations, is required to maintain containment isolation after Time Frame 1.

19D.6.2.8 Hydrogen Control

The operator action to actuate the igniters occurs prior to the hydrogen generation at the onset of Time Frame 2. The igniters need to survive and receive power throughout the hydrogen release to maintain the hydrogen concentration below the lower flammability limit during the hydrogen generation in Time Frame 2.

If containment becomes steam inert in Time Frame 2, the igniters will become ineffective and hydrogen will accumulate in containment. The passive auto-catalytic recombiners (PARs) are also available to control hydrogen in containment and can be effective in a steam inert environment. The PARs are not credited in the design basis for severe accidents because they are passive equipment that cannot be controlled by the operating staff from the control room.

The plant response to the igniter actuation can be monitored by containment hydrogen concentration using the hydrogen monitors or containment atmosphere sampling, which is part of the primary sampling system. The containment pressure response can also be used to indicate hydrogen burning which creates a distinctive pressure global peak, but not continual hydrogen burning by the igniters because the energy release to containment is at a low rate and the containment pressure response cannot be distinguished from other heat generation processes.

19D.6.2.9 Control Fission Product Releases

A nonsafety-related containment spray system is provided in AP1000 to wash aerosol fission products from the containment atmosphere. The spray system is manually actuated from the SAMG which is entered at the onset of Time Frame 2. Operating the spray involves opening an air-operated valve inside the containment and actuating valves and a pump outside the containment. Once open, the active operation of the valve inside the containment is completed.

Post-core damage, this action may be monitored with containment water level.

19D.6.2.10 Accident Monitoring

During the initial core melting and relocation, containment hydrogen and radiation monitors are used for core damage assessment and verification of the hydrogen igniter operation. Steam generator radiation monitoring is used to determine steam generator tube integrity. In the longer term, containment atmosphere sampling can be used to monitor hydrogen and radiation. Containment pressure, temperature, and water level indication and RCS pressure need to be monitored throughout Time Frame 2.

During a severe accident, the instrumentation may be subjected to conditions well beyond its design basis. The SAMG does not automatically eliminate instrumentation based on its design basis in comparison to severe accident conditions. Instead, the AP1000 SAMG relies on all available instrumentation indications and instructs the user to constantly compare instrumentation readings to diverse sources to validate the instrumentation reading. It is also noteworthy that while target values are established for various plant parameters to indicate a controlled stable state, the trends of the parameters being monitored are equally as important in managing the accident. The parameter trends indicate whether strategies are effective and determine if additional strategies need to be considered.

19D.6.3 Time Frame 3 - Ex-Vessel Core Relocation

Time Frame 3 represents the phase of the accident after vessel failure. The core debris is in the reactor cavity, and the IRWST water is not injected into the containment.

19D.6.3.1 Injection into the RCS

The RCS is failed. Injection to the RCS is no longer needed in Time Frame 3. Note that the AP1000 SAMG considers RCS injection as a means to inject water into the reactor cavity in Time Frame 3.

19D.6.3.2 Injection into Containment

Water coverage to the ex-vessel debris bed is passively provided by the containment design to drain water from the RCS via the IRWST. Water condensing on the PCS shell is returned to the reactor cavity after filling the IRWST to the overflow. The addition of water to the IRWST from other sources to overflow into containment is also a method of injecting water into containment. Containment spray can also be used to inject water into containment in Time Frame 3. Draining the IRWST to containment is not credited in Time Frame 3 in survivability assessments because activation of the system is attempted several times in Time Frame 1, and diverse systems are credited to provide reasonable assurance of containment injection survivability in this time frame. Containment spray and overflowing the IRWST are also not credited in Time Frame 3 survivability assessments because these methods are already credited in Time Frame 2.

19D.6.3.3 Decay Heat Removal and Injection into the Steam Generators

The RCS is failed. PRHR activation or injection into the steam generators is no longer needed in Time Frame 3. Injection to the steam generator for SGTR fission product scrubbing is not required to maintain the water level.

19D.6.3.4 Depressurize RCS

The RCS is depressurized by the vessel failure in Time Frame 3.

19D.6.3.5 Depressurize Steam Generators

The RCS is failed. Steam generator depressurization is not needed in Time Frame 3.

19D.6.3.6 Containment Heat Removal

Active initiation of PCS water is completed prior to Time Frame 3. PCS flowrate and level are monitored for post-72 hour activities. Alternate water sources can be provided by connections to the external PCS water tank which is outside the containment pressure boundary and not subjected to the harsh environment.

In addition to PCS water, a nonsafety-related containment spray system can provide heat removal from containment. The design basis purpose of containment spray is scrubbing fission products and containment spray is actuated on high containment radiation levels. This would most likely occur in Time Frame 2 when the fuel rods are overheated and melting. Manually actuating the containment spray system involves opening an air-operated valve inside the containment and actuating valves and a pump outside the containment. Once open, the active operation of the valve inside the containment is completed.

Post-core damage, the actions may be monitored with PCS flowrate and tank water level, containment water level and containment pressure.

19D.6.3.7 Containment Isolation and Venting

Continued operation of the containment shell as a pressure boundary is needed to maintain containment isolation in Time Frame 3. Containment temperature needs to be monitored because prolonged exposure of organic materials (e.g., equipment and personnel hatch seals) to high temperatures (> 400°F) can degrade the material.

In the event of containment pressurization above design pressure due to core concrete interaction non-condensable gas generation, the containment can be vented. Venting protects containment isolation by preventing an uncontrolled containment failure airborne release pathway. The vent can be opened and closed as required to maintain pressure in the containment below its failure pressure. Containment venting does not prevent or mitigate containment basemat failure due to core concrete interaction. Containment venting to the spent fuel pool is available through RNS hot leg suction line MOVs.

19D.6.3.8 Combustible Gas Control

The hydrogen igniters are used to control combustible gases. Active operation of igniters continues to control the release of combustible gases (e.g., hydrogen and carbon monoxide) from the degradation of concrete in the reactor cavity.

If containment becomes steam inert in Time Frame 3, the igniters will become ineffective and hydrogen will accumulate in containment. The passive auto-catalytic recombiners (PARs) are also available to control hydrogen in containment and can be effective in a steam inert environment. The PARs are not credited in the design basis for severe accidents because they are passive equipment that cannot be controlled by the operating staff from the control room.

The plant response to the igniter actuation can be monitored by containment hydrogen concentration using the containment atmosphere sampling, which is part of the primary sampling system. The containment pressure response can also be used to indicate hydrogen burning which creates a distinctive pressure global peak, but not continual hydrogen burning by the igniters because the energy release to containment is at a low rate and the containment pressure response cannot be distinguished from other heat generation processes.

19D.6.3.9 Control Fission Product Releases

The nonsafety-related sprays are actuated in Time Frame 2. The operation of the nonsafety-related containment spray continues, possibly into Time Frame 3, until the water from the source tank is depleted.

Post-core damage, this action may be monitored with containment water level.

19D.6.3.10 Accident Monitoring

Containment pressure, temperature, water level and radiation, steam generator radiation and the containment hydrogen concentration are sufficient to monitor the accident in the long-term. Hydrogen concentration and radiation can be monitored with containment sampling functions. In both Time Frame 2 and Time Frame 3, auxiliary building radiation monitors, if properly correlated, could be used for containment radiation monitoring.

19D.6.4 Summary of Equipment and Instrumentation

The equipment and instrumentation used in achieving a controlled, stable state following a severe accident, and the time it operates are summarized in Tables 19D-3 through 19D-5.

19D.7 Severe Accident Environments

The design certification of the AP1000 included consideration by the NRC of the topic referred to in this section.

19D.8 Assessment of Equipment Survivability

Since severe accidents are very low probability events, the NRC recommends in SECY-93-087, that equipment desired to be available following a severe accident need not be subject to the qualification requirements of 10CFR50.49, the quality assurance requirements of 10CFR50 Appendix B, or the redundancy/diversity requirements of 10CFR50 Appendix A. It is satisfactory to provide reasonable assurance that the designated equipment will operate following a severe accident by comparing the AP1000 severe accident environments to design basis event/severe accident testing or by design practices.

19D.8.1 Approach to Equipment Survivability

The approach to survivability is by equipment type, equipment location, survival time required, and the use of design basis event qualification requirements and severe environment experimental data.

19D.8.1.1 Equipment Type

The various types of equipment needed to perform the activities discussed above are transmitters, thermocouples, resistance temperature detectors (RTDs), hydrogen and radiation monitors, valves, pumps, valve limit switches, containment penetration assemblies, igniters, and cables.

19D.8.1.2 Equipment Location

Some of the in-containment equipment, such as transmitters, has been deliberately located to avoid the most severe calculated environments. Other equipment is located outside containment. The performance of the equipment was judged based on the most severe postulated event for that location.

19D.8.1.3 Time Duration Required

Requirements are defined for each time frame, so the equipment evaluation only discusses performance during these periods. A limited amount of equipment has been designated for the long term (Time Frame 3) and these parameters can be monitored outside containment.

19D.8.1.4 Severe Environment Experiments

The primary source for performance expectations of similar equipment in severe accident environments is EPRI NP-4354, “Large Scale Hydrogen Burn Equipment Experiments.” This information is supplemented by NUREG/CR-5334, “Severe Accident Testing of Electrical Penetration Assemblies.” These programs tested equipment types that had previously been qualified for design basis event environmental conditions. The temperature in the chamber for the first program was in the 700°F - 800°F range for ten to twenty minutes during the continuous hydrogen injection tests. Although the conditions at the equipment would be somewhat less severe, the chamber conditions envelop all of the longer duration profiles indicated for the AP1000 events. The equipment in this program was also exposed to significant hydrogen burn spikes that are also postulated for the AP1000 plant. The same equipment was exposed to and survived several events, both pre-mixed and continuous hydrogen injection which provides confidence in its ability to survive a postulated severe accident. The second program tested containment penetrations to high temperatures for long durations. A penetration was tested under severe accident conditions simulated with steam up to

400°F and 75 psia for ten days. The results indicated that the electrical performance of the penetration would not lead to degraded equipment performance for the first four days. The mechanical performance did not degrade (no leaks) during the entire test.

19D.8.2 Equipment Located in Containment

The exposure to elevated temperatures as a direct result of the postulated severe accident or as a result of hydrogen burning is the primary parameter of interest. Pressure environments do not exceed the design basis event conditions for which the equipment has been qualified if PCS is operating as designed. Radiation environments also do not exceed the design basis event conditions throughout Time Frames 1 and 2.

19D.8.2.1 Differential Pressure and Pressure Transmitters

The functions defined for accident management that utilize in-containment transmitters are IRWST water level, reactor coolant system pressure, steam generator wide range water level, and containment pressure. Most of these transmitters that provide this information are located in rooms where the environment is limited to short duration temperature transients. These transients exceed ambient design basis temperature conditions but should not impact the transmitter performance since the internal transmitter temperature do not increase significantly above that experienced during design basis testing. EPRI NP-4354 documents transmitter performance during several temperature transients with acceptable results. The IRWST water level transmitters are located in the maintenance floor and are only required during Time Frames 1 and 2. The environment during Time Frames 1 and 2 does not exceed the design basis qualification parameters of the transmitters if PCS is operating as designed. Reactor system pressure and steam generator wide range water level are required through the second time frame. The only long term application is the containment pressure transmitter which may eventually be impacted by the severe accident radiation dose.

19D.8.2.2 Thermocouples

The functions defined for severe accident management that utilize thermocouples are core-exit temperatureand containment water level. The core-exit temperature is only required during Time Frame 1 and the containment water level is required through Time Frame 2. The temperatures to which the thermocouples are exposed during the defined time frames do not exceed the thermocouple design.

19D.8.2.3 Resistance Temperature Detectors (RTDs)

Both hot and cold leg temperatures are defined as parameters for severe accident management in Time Frame 1. RTDs are utilized for these measurements and will perform until their temperature range is exceeded. The hot leg RTDs could fail as the temperature increases well above the design conditions of the RTDs but the cold leg RTDs should perform throughout Time Frame 1. RTDs are also utilized through Time Frame 3 for the containment temperature measurement and are exposed to temperature transients that exceed design basis qualification conditions. EPRI NP-4354 documents RTD performance during several temperature transients with acceptable results.

19D.8.2.4 Hydrogen Monitors

Containment hydrogen is defined as a parameter to be monitored throughout the severe accident scenarios. Early in the accident, the hydrogen may be monitored by a device that operates on the basis of catalytic oxidation of hydrogen on a heated element. The hydrogen monitors are located in the main containment area. The design limits of this device may be exceeded after the first few hours of some of the postulated accidents and performance may be uncertain. If the device fails, post-

accident sampling of containment atmosphere using analysis of grab samples may be used to determine containment hydrogen concentrations.

19D.8.2.5 Radiation Monitors

Containment radiation is defined as a parameter to be monitored throughout the severe accident scenarios. The containment radiation monitors are located in the main containment area. Early in the accident, the design basis event qualified containment radiation monitor provides the necessary information until the environment exceeds the design limits of the monitor. If the device fails, containment radiation is determined through the containment atmosphere sampling function or by portable monitors located against the outside of the containment shell.

19D.8.2.6 Solenoid Valve

Qualified solenoid valves are used to vent air-operated valves (AOVs) to perform the function required. In Time Frame 1, the core makeup tank AOVs located in the accumulator room provide a path for RCS injection, the PRHR AOVs located in the maintenance floor provide a path for RCS heat removal and the containment is isolated by AOVs located in the maintenance floor and the PXS valve/accumulator room. The environment to which these solenoid valves may be exposed in Time Frame 1 is not significantly different than the design basis events to which the devices are qualified. In Time Frame 2, the RCS boundary AOV located in the maintenance floor is used for CVS injection into the RCS and the containment spray AOV located in the maintenance floor is used for control of fission product release. Also in Time Frame 2, the reactor vessel head vent AOVs provide a path for RCS depressurization. In addition, throughout Time Frame 3, access to the containment environment from the containment atmosphere sampling function is through solenoid valves located in the maintenance floor. During Time Frame 2 and Time Frame 3, these valves may be exposed to transient conditions due to hydrogen burns that exceed design basis event qualification. Solenoid valves in an energized condition were included in the hydrogen burn experiments (EPRI NP-4354) and survived many transients. Shielding provided by the location of the valves limits the severe accident radiation dose to the typical design basis qualification dose for these valves.

19D.8.2.7 Motor-Operated Valves

Motor-operated valves (MOVs) are utilized in several applications during the severe accident scenarios. MOVs in the accumulator and core makeup tank path are normally open and remain open. In Time Frame 1, the PXS recirculation MOVs located in the PXS valve/accumulator room are required for injection of water into the containment, MOVs for the first three stages of ADS located in a compartment above the pressurizer are required for RCS depressurization and the containment is isolated by MOVs located in the maintenance floor and the PXS valve/accumulator room. The environment to which these MOVs may be exposed in Time Frame 1 is not significantly different than the design basis events to which they are qualified. In Time Frame 2, the charging and injection MOV located in the maintenance floor provides a path from the CVS for RCS injection and an RNS MOV located in the PXS valve/accumulator room provides a path from the IRWST for RCS injection. In addition, throughout Time Frame 3, containment venting to the spent fuel pool is available through RNS hot leg suction line MOVs located in the RNS valve room. During Time Frames 2 and 3, these valves may be exposed to transient conditions due to hydrogen burns that exceed design basis event qualification. MOVs were included in the hydrogen burn experiments (EPRI NP-4354) and survived many transients. Shielding provided by the location of the valve limits the severe accident radiation dose to the typical design basis qualification dose for these valves.

19D.8.2.8 Squib Valves

Squib valves are only required in Time Frame 1 when the severe accident environment is not significantly different than the design basis environment for which these valves are qualified. IRWST

and PXS recirculation squib valves located in the accumulator room are used for injection into the RCS and containment, respectively. For RCS depressurization, the fourth stage ADS squib valves are located in steam generator compartments 1 and 2.

19D.8.2.9 Position Sensors

Position sensors are required to monitor the position of containment isolation valves that could lead directly to an atmospheric release. These isolation valves actuate early in the transient, so verification is only required during Time Frame 1. The position sensors are located in the maintenance floor and the environment in this time frame does not exceed the design basis event qualification environment of the position sensors.

19D.8.2.10 Hydrogen Igniters

The hydrogen igniters are distributed throughout the containment and are designed to perform in environments similar to those postulated for severe accidents. The igniters' transformers are located outside containment. The successful results of glow plug testing through several hydrogen burns is documented in EPRI NP-4354 and provides confidence in the performance of these devices.

19D.8.2.11 Electrical Containment Penetration Assemblies

The electrical containment penetrations are located in the lower compartment and are required to perform both electrically and mechanically throughout the severe accident. The hydrogen burn equipment experiments documented by EPRI NP-4354 included penetrations qualified for nuclear plants. Electrical testing on the penetration cables after all the pre-mixed and continuous injection tests concluded that most of the cables passed the electrical tests while submerged in water. These tests consisted of ac (at rated voltage) and dc (at three times rated voltage) withstand tests and insulation resistance tests at 500 volts. The penetrations were also tested under simulated severe accident conditions at 400°F and 75 psia for about 10 days (NUREG/CR-5334). The results indicated that some degradation in instrumentation connected to the penetration may occur in four days under these severe conditions. The maintenance floor may experience short temperature transients above 400°F but stable temperatures are significantly less, so it is expected that the electrical performance would be maintained throughout the event. The only long term measurement utilizing these penetrations is containment pressure and this can be measured outside containment if necessary. There was no degradation of mechanical performance of the electrical penetrations (maintaining the seal) in either test program.

19D.8.2.12 Cables

The hydrogen burn equipment experiments documented by EPRI NP-4354 included twenty-four different cable types qualified for nuclear plants. Electrical testing on these cables after all the pre-mixed and continuous injection tests concluded that all (fifty two samples) of the cables passed the electrical tests while submerged. These tests consisted of ac (at rated voltage) and dc (at three times rated voltage) withstand tests and insulation resistance tests at 500 volts. Due to the exposure to many events, some cable samples had extensive damage in the form of charring, cracking and bulging of the outer jackets and still performed satisfactorily. The cables tested are representative of cables specified for the AP1000 and are only exposed to short single temperature transients in their respective locations. Proper performance can be expected. The only long term measurement utilizing cables is containment pressure, which can be measured outside containment if necessary.

19D.8.2.13 Assessment of Equipment for Sustained Burning

The equipment necessary for equipment survivability in sustained burning environments is defined in Tables 19D-3 through 19D-5. The equipment in Table 19D-3 includes equipment and instrumentation

operation during Time Frame 1 - core uncovery and heatup, and is prior to the release of significant quantities of hydrogen. Therefore, it does not have to be qualified for sustained hydrogen burning. Table 19D-7 specifies the equipment and instrumentation used in Time Frames 2 and 3 to provide reasonable assurance of achieving a controlled stable state.

19D.8.3 Equipment Located Outside Containment

Other functions defined for severe accident management are performed outside containment and the equipment is not subjected to the harsh environment of the event. This equipment includes, but is not limited to:

- Steam line radiation monitor,
- Transmitters for monitoring steam line pressure,
- Passive containment cooling system flow and tank level,
- Containment atmosphere sampling function,
- Makeup pumps and flow measurement,
- RNS pumps and flow measurement,
- SFS pumps and flow measurement,
- RNS MOVs
- MFW pumps and valves,
- SFW pumps and valves,
- Steam generator PORVs and main steam bypass valves for depressurization,
- Recirculation pumps, PCS valves and fire water pumps and valves for containment heat removal,
- Containment isolation valves (outside containment),
- Auxiliary building radiation monitor,
- MOV and manual valve from RNS hot leg suction lines to the spent fuel pool and
- Fire water, fire pumps, valves and flow measurement used to provide containment spray and backup containment cooling.

19D.9 Conclusions of Equipment Survivability Assessment

The equipment defined for severe accident management was reviewed for performance during the environments postulated for these events. Survivability of the equipment was evaluated based on design basis event qualification testing, severe accident testing, and the survival time required following the initiation of the severe accident. The equipment that is qualified for design basis events has a high probability of surviving postulated severe accident events and performing satisfactorily for the time required.

This assessment provides reasonable assurance that equipment, both electrical and mechanical, used to mitigate the consequences of severe accidents and achieve a controlled, stable state can perform over the time span for which they are needed.

19D.10 References

19D-1. APP-GW-GL-027, “Framework for AP1000 Severe Accident Management Guidance,” Westinghouse Electric Company LLC.

19D-2. AP1000 Emergency Operating Procedures.

19D-3. APP-GW-GJR-400, “AP1000 Severe Accident Management Guidelines,” Westinghouse Electric Company LLC.

Table 19D-1
Definition of Equipment Survivability Time Frames

Time Frame	Beginning Time	Ending Time	Comments
0	Accident initiation	safe, stable state or core uncovery	• Bounded by design basis equipment qualification environment
1	Core uncovery	controlled, stable state or rapid cladding oxidation	• Core uncovery and heatup • Bounded by design basis equipment qualification environment
2	Rapid cladding oxidation	controlled, stable state or vessel failure	• In-vessel core melting and relocation • Entry into SAMG
3	Vessel failure	controlled, stable state or containment failure	• Ex-vessel core relocation

Table 19D-2
AP1000 High Level Actions Relative to Accident Management Goals

Goal	Element	High Level Action*
Controlled, stable core	water inventory in RCS	• inject into RCS • depressurize RCS
	water inventory in containment	• inject into containment
	heat transfer to IRWST	• initiate PRHR
	heat transfer to SGs	• inject into RCS • inject into SGs
	heat transfer to containment	• inject into RCS • inject into containment • depressurize RCS • initiate PRHR
Controlled, stable containment	heat transfer from containment	• depressurize containment • vent containment • water on outside containment
	isolation of containment	• inject into SGs • depressurize RCS
	hydrogen prevention/control	• burn hydrogen • pressurize containment • depressurize RCS • inject into containment • vent containment • water on outside containment
	core concrete interaction prevention	• inject into containment
	high pressure melt ejection prevention	• inject into containment • depressurize RCS
	creep rupture prevention	• depressurize RCS • inject into SGs
	containment vacuum prevention	• pressurize containment
Terminate fission product release	isolation of containment	• inject into SGs • depressurize RCS
	reduce fission product inventory	• inject into containment • depressurize RCS
	reduce fission product driving force	• depressurize containment • water on outside containment

Note:
* See Tables 19D-3, 19D-4 and 19D-5

Table 19D-3 (Sheet 1 of 3)
Equipment and Instrumentation Operation Prior to End of Time Frame 1 - Core Uncovery and Heatup

Action	Equipment	Instrumentation	Purpose	Comment
Inject into RCS	• CMT • accumulator • IRWST • CVS • RNS	• core-exit t/c's • RCS pressure • RCS RTDs • CVS flow • RNS flow • IRWST water level	• restore core cooling	• injection must often be recovered to be successful in severe accident
Inject to SGs	• MFW • SFW	• SG WR water level • steam line pressure	• decay heat removal • make SGs available to depressurize RCS • prevent SG tube creep rupture	• injection source must often be recovered to be successful in severe accident
Decay Heat Removal	• PRHR Hx • via SGs	• IRWST water level • IRWST temperature • core-exit t/c's • RCS RTDs	• decay heat removal	• only works if RCS is reflooded and IRWST water level covers PRHR Hx
Depressurize RCS	• ADS • aux pressurizer spray • via SGs • PRHR Hx	• RCS pressure • IRWST water level • IRWST temperature • steam line pressure	• facilitate injection to RCS • long term heat transfer path	• ADS often automatic
			• prevent SG tube creep rupture • containment integrity	• RCS depressurization required prior to significant cladding oxidation to prevent creep rupture
			• isolate break in SGTR	• uses intact SG or PRHR
			• prevent vessel failure	• requires injection to containment to be successful

Table 19D-3 (Sheet 2 of 3)
Equipment and Instrumentation Operation Prior to End of Time Frame 1 - Core Uncovery and Heatup

Action	Equipment	Instrumentation	Purpose	Comment
Depressurize SGs	• SG PORV • main steam bypass	• steam line pressure • RCS pressure • SG WR water level	• depressurize RCS • minimize pressure differential across SG tubes	• requires injection into SGs to prevent creep rupture
Inject Into Containment	• IRWST drains	• core-exit t/c's • containment water level • IRWST water level	• prevent vessel failure	• manual cavity flooding action in EOP
Containment Isolation	• containment isolation system • containment shell • penetrations	• containment isolation system valve position • containment pressure	• containment integrity	• containment isolation system often automatic • manual action in EOP
Control Hydrogen	• igniter	• containment hydrogen monitors • containment atmosphere sampling functions • containment pressure	• containment integrity	• manual igniter action in EOP
Containment Heat Removal	• PCS water • external water	• containment pressure • PCS flowrate • PCS tank level	• containment integrity • alleviate environmental challenge to equipment • long term heat transfer path	• PCS water automatic

Table 19D-3 (Sheet 3 of 3)
Equipment and Instrumentation Operation Prior to End of Time Frame 1 - Core Uncovery and Heatup

Action	Equipment	Instrumentation	Purpose	Comment
Accident Monitoring		• SG radiation • containment pressure • containment temperature • containment hydrogen monitors • containment water level • containment radiation • containment atmosphere sampling functions • auxiliary building radiation • core-exit t/c's • RCS pressure • IRWST water level	• accident management • emergency response(1) • emergency action levels(1)	• required by 10 CFR 50.34(f)

Note:
1. Note that the instrumentation required for emergency response and emergency action levels is an open item because the EALs are not yet developed.

Table 19D-4 (Sheet 1 of 3)
Equipment and Instrumentation Operation During Time Frame 2 - In-Vessel Core Melting and Relocation

Action	Equipment	Instrumentation	Purpose	Comment
Inject into RCS	• CMT • accumulator • IRWST • CVS • RNS	• RCS pressure • containment pressure • CVS flow • RNS flow • RCS temperature	• cool core debris in-vessel	• RCS injection needed to cool in-vessel debris for reasonable assurance of controlled, stable state
Decay Heat Removal	• via SGs	• SG WR water level • steam line pressure • core-exit t/c's • RCS RTDs	• decay heat removal	
Inject Into Containment	• containment spray • overflow IRWST • RNS • IRWST drains	• containment water level	• prevent vessel failure	• containment spray only actuated on high containment radiation in SAMG which occurs in Time Frame 2
Inject to SGs	• MFW • SFW	• SG WR water level • steam line pressure	• isolate containment in SGTR • scrub fission products	• also requires RCS depressurization for containment isolation
Depressurize RCS	• ADS • aux pressurizer spray • reactor vessel head vent	• RCS Pressure	• prevent vessel failure • containment integrity	• needed for in-vessel retention of core debris • needed for prevention of TI-SGTR • try to recover in Time Frame 2, if not successful in Time Frame 1

Table 19D-4 (Sheet 2 of 3)
Equipment and Instrumentation Operation During Time Frame 2 -
In-Vessel Core Melting and Relocation

Action	Equipment	Instrumentation	Purpose	Comment
Depressurize SGs				• not needed in Time Frame 2
Containment Heat Removal	• PCS water • external water • containment spray	• PCS flowrate • PCS tank level • containment water level • containment pressure	• containment integrity	• active operation completed in Time Frame 1; needs to be continued in Time Frame 2
Containment Isolation	• containment shell • penetrations	• containment pressure	• containment integrity	• containment isolation system active operation completed in Time Frame 1
Control Hydrogen	• igniters	• containment hydrogen monitors • containment atmosphere sampling function • containment pressure	• containment integrity	• active operation continues in Time Frame 2 • monitors only required initially to verify hydrogen igniter operation
Control Fission Product Releases	• containment spray	• containment water level	• scrub fission products	• containment spray only actuated on high containment radiation in SAMG which occurs in Time Frame 2

Table 19D-4 (Sheet 3 of 3)
Equipment and Instrumentation Operation During Time Frame 2 -
In-Vessel Core Melting and Relocation

Action	Equipment	Instrumentation	Purpose	Comment
Accident Monitoring		• SG radiation • containment pressure • containment temperature • containment hydrogen monitors • containment water level • containment radiation • containment atmosphere sampling functions • auxiliary building radiation • RCS pressure	• accident management • emergency response(1) • emergency action levels(1)	• active operation continues in Time Frame 2

Note:
1. Note that the instrumentation required for emergency response and emergency action levels is an open item because the EALs are not yet developed.

Table 19D-5 (Sheet 1 of 2)
Equipment and Instrumentation Operation During Time Frame 3 - Ex-Vessel Core Relocation

Action	Equipment	Instrumentation	Purpose	Comment
Inject into RCS				• not needed in Time Frame 3
Decay heat removal				• not needed in Time Frame 3
Inject into SGs				• not needed in Time Frame 3
Depressurize RCS				• not needed in Time Frame 3
Depressurize SGs				• not needed in Time Frame 3
Inject Into Containment	• Containment spray • Overflow IRWST - CVS - RNS - SFS • IRWST drains	• containment water level	• cool ex-vessel core debris to prevent or mitigate consequences of CCI • scrub fission products released from ex-vessel core debris	• only get to Time Frame 3 if there is no water in containment or if RCS depressurization fails
Containment Heat Removal	• PCS water • external water • containment spray	• PCS flowrate • PCS tank level • containment water level • containment pressure	• containment integrity	• active operation completed in Time Frame 1; needs to be continued in Time Frame 3
Containment Isolation	• containment shell • penetrations	• containment pressure • containment temperature	• containment integrity	• active operation of containment isolation system completed in Time Frame 1
	• RNS hot leg suction MOVs	• containment pressures • SFP water level	• containment vent	• manual action within SAMG
Control Hydrogen	• igniters	• containment atmosphere sampling function • containment pressure	• containment integrity	• active operation continues in Time Frame 3 • PARS may be effective in Time Frame 3 if igniters are not effective

Table 19D-5 (Sheet 2 of 2)
Equipment and Instrumentation Operation During Time Frame 3 - Ex-Vessel Core Relocation

Action	Equipment	Instrumentation	Purpose	Comment
Control Fission Product Release	• containment spray	• containment water level	• scrub fission products	• containment spay only actuated on high containment radiation in SAMG which occurs in Time Frame 3
Accident Monitoring		• SG radiation • containment pressure • containment temperature • containment hydrogen monitors • containment water level • containment radiation • containment atmosphere sampling function • auxiliary building radiation monitors	• accident management • emergency response(1) • emergency action levels(1)	• active operation continues in Time Frame 3

Note:
1. The instrumentation required for emergency response and emergency action levels is an open item because the EALs are not yet developed.

TABLE 19D-6 NOT USED.

Table 19D-7 (Sheet 1 of 3)
Sustained Hydrogen Combustion Survivability Assessment

EQUIPMENT AND INSTRUMENTATION	SUSTAINED HYDROGEN COMBUSTION SURVIVABILITY ASSESSMENT
Equipment	
PXS equipment (injection)	The PXS equipment utilized for introduction of cooling water includes component redundancy and is separated into two delivery flow paths. The two flow paths are physically separated into two trains such that if one train is disabled due to a sustained burn from DVI or other line break within that subsystem, the other subsystem will function.
CVS equipment (injection)	The equipment providing for CVS injection is located within the CVS compartment with the exception of the CVS makeup isolation valve. In accordance with the above, a sustained burn will not occur within the CVS compartment and, therefore, the equipment within this compartment utilized for CVS makeup will be operable. The CVS makeup isolation valve is normally in the correct position for severe accident scenario and is considered operable.
RNS equipment (injection)	Injection via the RNS is dependent only upon check valves within containment and, therefore, is not susceptible to sustained burning effects.
Main Feedwater	The operability of main feedwater system to inject feedwater to steam generators is not dependent upon equipment located within containment and, therefore, is not susceptible to sustained burning effects.
Startup Feedwater	The operability of startup feedwater system to inject feedwater to steam generators is not dependent upon equipment located within containment and, therefore, is not susceptible to sustained burning effects.
Fire Water, containment spray, and external containment vessel cooling	The operability of the fire water system to provide makeup for containment spray and for external containment vessel cooling is not dependent upon equipment located within containment and, therefore, is not susceptible to sustained burning effects.

Table 19D-7 (Sheet 2 of 3)
Sustained Hydrogen Combustion Survivability Assessment

EQUIPMENT AND INSTRUMENTATION	SUSTAINED HYDROGEN COMBUSTION SURVIVABILITY ASSESSMENT
Equipment	
Containment Shell	As discussed in Subsection 19.41.7 of this document, hydrogen plumes are located away from the containment shell to mitigate the threat to the containment integrity.
Igniters	Igniters are specified and designed to withstand the effects of sustained burning and, therefore, are considered operable for these events.
Instrumentation	
RCS Pressure	There are four RCS pressurizer pressure transmitters. Two transmitters are located at a distance greater than 75 feet from the vent from the PXS valve/accumulator room and are therefore beyond the distance that potentially causes operability concerns from a sustained flame. The other two transmitters are located in a different room from the fourth stage ADS valves. This precludes radiative heating, which could potentially cause operability concerns.
Containment Pressure	There are three extended range containment pressure transmitters. The three transmitters are located such that they cannot all be exposed to a sustained flame from either of the vents from the PXS valve/accumulator room into the maintenance floor at the base of the CMTs. Therefore, continued operability of the containment pressure function is provided.
SG 1 Wide Range Level	There are four steam generator wide range levels for SG 1. Two of the transmitters are located at a distance of greater than 20 feet from a CMT and are, therefore, beyond the distance that could potentially cause operability concerns from a sustained flame from the vent from the PXS valve/accumulator room into the maintenance floor at the base of the CMT. The other two transmitters are located over 20 feet below the fourth stage ADS valves. This precludes radiative heating, which could potentially cause operability concerns.
SG 2 Wide Range Level	Based on the layout of the four steam generator wide range levels for SG 2, at least two of the transmitters will not be exposed to a sustained flame from either of the vents from the PXS valve/accumulator room into the maintenance floor at the base of the CMTs. Therefore, continued operability of the SG 2 wide range level indication function is provided.

Table 19D-7 (Sheet 3 of 3)
Sustained Hydrogen Combustion Survivability Assessment

EQUIPMENT AND INSTRUMENTATION	SUSTAINED HYDROGEN COMBUSTION SURVIVABILITY ASSESSMENT
Instrumentation	
Containment Hydrogen Monitors	There are 3 distributed containment hydrogen monitors. There are no sustained burns that could potentially affect the two sensors that are located at an elevation of 164 feet or the sensor located within the dome.
Containment Atmosphere Sampling Function	The capabilities to perform containment atmosphere sampling are discussed in Subsection 9.3.3.1.2.2 – Post-Accident Sampling. Successful containment atmosphere sampling is dependent on the availability of either of the hot leg sample source isolation valves and the containment isolation valves in series with the isolation valve. The sample isolation valve from reactor coolant hot leg number 1 is located in a different room from the fourth stage ADS valves. This precludes radiative heating, which could potentially cause operability concerns. The sample isolation valve from reactor coolant hot leg number 2 is located in a different room from the fourth stage ADS valves. This precludes radiative heating, which could potentially cause operability concerns. The containment isolation valves are located less than 20 feet from a CMT. However, a steel shroud around base of the CMT prevents a sustained flame existing on the containment side of that CMT and, therefore, affecting the operability of either of the containment isolation valves.

Appendix 19E Shutdown Evaluation

19E.1 Introduction

Westinghouse has considered shutdown operations in the design of the A1000 nuclear power plant. The AP1000 defense-in-depth design philosophy to provide normally operating active systems and passive safety-related systems gives the AP1000 a greater degree of safety during shutdown operations as well as normal power operation when compared to currently operating plants. This appendix presents and evaluates the AP1000 design features in the context of the specific shutdown issues identified by the Nuclear Regulatory Commission.

19E.1.1 Purpose

This appendix presents AP1000 design features that address the issues of shutdown risk and shutdown safety. This appendix further evaluates these design features with respect to their ability to reduce and or mitigate the consequences of events that can occur during shutdown.

19E.1.2 Scope

The scope of this appendix includes discussions of the following:

- Systems designed to operate during shutdown
- Shutdown operations – including maintenance insights, risk management, and Emergency Response Guidelines (ERGs) (Reference 1)
- Safety analyses and evaluations for shutdown operations
- Chapter 16, “Technical Specifications”
- Shutdown risk evaluations – including shutdown PRA results and insights and fire/flood risk
- Compliance with the guidance in NUREG-1449 (Reference 2)

19E.1.3 Background

The Diablo Canyon event of April 10, 1987, and the loss of ac power at the Vogtle plant on March 20, 1990, led the NRC staff to issue NUREG-1449, which provides an evaluation of the shutdown risk issue. During the AP600 Design Certification review, the NRC requested that Westinghouse perform a systematic assessment of the shutdown risk issue to address areas identified in NUREG-1449 as applicable to the AP600 design. The AP1000 design is based extensively on the AP600, and the systems, structures and components that are important in maintaining a low shutdown risk for AP600 are generally the same design and/or have the same design basis with respect to their role in reducing shutdown risk. Therefore, the conclusions from the assessment of the shutdown risk for the AP600 are applicable to the AP1000. This appendix summarizes the assessment of the shutdown risk issue for AP1000.

19E.2 Major Systems Designed to Operate During Shutdown

Westinghouse has considered shutdown modes, shutdown alignments, and industry issues related to shutdown in the design of the AP1000 safety-related and nonsafety-related systems designed to operate or be available during shutdown. This section provides descriptions of the important systems designed to operate during shutdown and includes specific design features that have been

incorporated for shutdown operations with a discussion of their operating modes or alignment during shutdown.

In this appendix, references are made to the various AP1000 operating modes. The AP1000 operating modes have been defined in the Technical Specifications (Section 16.1, Table 1.1-1). The mode definitions for the AP1000 are similar to that of current Westinghouse pressurized water reactors (PWRs), with the difference being the definition of Mode 4, safe shutdown.

In the AP1000, Mode 4 has been redefined as safe shutdown and corresponds to the range of RCS temperature between 420°F and 200°F. The upper temperature limit corresponds to the RCS temperature that can be achieved by the passive safety-related systems 36 hours after shutdown. The ability of the passive safety-related systems to achieve Mode 4 within 36 hours is shown in Subsection 4.10.2 of this appendix.

19E.2.1 Reactor Coolant System

19E.2.1.1 System Description

The reactor coolant system (RCS) is described in Chapter 5.

19E.2.1.2 Design Features to Address Shutdown Safety

The AP1000 has incorporated design features that address issues related to shutdown operations. This subsection provides a discussion of the RCS design features that are incorporated to address shutdown operations or that are important to minimizing the risk to plant safety during shutdown.

19E.2.1.2.1 Loop Piping Offset

The RCS hot legs and cold legs are vertically offset. This permits draining of the steam generators for nozzle dam insertion with the hot leg level much higher than traditional designs. The RCS must be drained to a level sufficient to provide a vent path from the pressurizer to the steam generators. This loop piping offset also allows an RCP to be replaced without removing the full core.

19E.2.1.2.2 RCS Instrumentation

Instrumentation is provided to monitor the RCS process parameters as required by the PLS and PMS as discussed in Chapter 7. This subsection describes RCS instrumentation designed to accommodate shutdown operations.

RCS Hot Leg Level

There are two safety-related RCS hot leg level channels, one located in each hot leg. These level indicators are provided primarily to monitor the RCS water level during mid-loop operation following shutdown operations. These are totally independent of each other. One level tap is at the bottom of the hot leg, and the other tap is on the top of the hot leg close to the steam generator. The steam generator tap is located at the high point of the tubing run. The level tap for the instrument in the hot leg with the normal residual heat removal system (RNS) step-nozzle suction line connection is between the reactor vessel and the step-nozzle. Figure 19E.2-1 shows a simplified sketch of the RCS level instruments.

These channels provide signals for the following protection functions:

- Isolation of letdown on low level on a one-out-of-two basis.

- Actuation of fourth-stage ADS valves on low (empty) hot leg level on a two-out-of-two basis. Actuation of fourth-stage ADS causes actuation of IRWST injection.

These functions protect the plant during shutdown operations. Letdown isolation assists the operators when draining the RCS to a mid-loop level. If the operators fail to isolate letdown, these channels send a signal to close the letdown valves and stop the draining process.

In the event of a loss of the RNS during shutdown, coolant inventory could be boiled away. When the hot leg water level indicates that the loops are empty, IRWST injection and fourth-stage ADS are actuated 30 minutes after receipt of the empty hot leg level signal.

These channels also provide signals to the letdown flow control valve to control the drain rate of the RCS via the letdown line during the transition to mid-loop operation. When the hot legs are full, the drain rate can proceed at a high level. As the water level is reduced to the hot legs, the drain rate is automatically decreased to a rate of approximately 20 gpm.

These channels are also used to generate the alarms on low hot leg water level. The alarm setpoints are selected to give the operator sufficient time to take the manual actions necessary to prevent the automatic actuation described previously. Indication of these channels is retrievable in the main control room. This variable is used by the operator to monitor the status of RCS inventory following an accident and is, therefore, classified as a post-accident monitoring system (PAMS) variable as discussed in Section 7.5.

The accuracy and response time of the hot leg level instruments are consistent with the standard engineered safety features (ESF) actuation discussed in Section 7.3. Concerns related to potential problems of noncondensible gases in the hot leg level instrument lines that have been raised in NRC Information Notice 92-54, Level Instrumentation Inaccuracies Caused by Rapid Depressurization (Reference 3), have been addressed in the layout of the instrument lines. In addition, as the hot leg level instruments are provided primarily for shutdown operations, off-gassing due to sudden depressurization of the RCS in shutdown modes is not a concern.

In the AP1000, draining of the RCS to mid-loop conditions is achieved in a controlled manner as discussed in Subsection 19E.2.1.2.4. Due to the low RCS drain rate, and the RCS step-nozzle as discussed in Subsection 19E.2.1.2.3, the amount of air-entrainment, and therefore RCS level perturbation during mid-loop, is negligible. Draining of the RCS is conducted in a quasi-steady-state, and the reliability of an accurate level reading is high.

Pressurizer Level

A fifth nonsafety-related independent pressurizer level transmitter, calibrated for low temperature conditions, provides water level indication during startup, shutdown, and refueling operations in the main control room and in the remote shutdown workstation. The upper level tap is connected to an ADS valve inlet header above the top of the pressurizer. The lower level tap is connected to the bottom of the hot leg. This provides level indication for the entire pressurizer and a continuous reading as the level in the pressurizer decreases to mid-loop levels during shutdown operations.

RCS Hot Leg Wide-Range Temperatures

The RCS contains two safety-related thermowell-mounted hot leg wide-range temperature detectors, one in each hot leg. The orientation of the resistance temperature detectors enables measurement of the reactor coolant fluid in the hot leg when in reduced inventory conditions. Their range is selected to accommodate the low RCS temperatures that can be attained during shutdown. In addition, at least two incore thermocouple channels are available to measure the core exit temperature during mid-loop RNS operation. These two thermocouple channels are associated with separate electrical divisions.

Pressurizer Surge Line Temperatures

There are three nonsafety-related temperature detectors located on the RCS pressurizer surge line. These instruments monitor the pressurizer surge line fluid temperature during plant normal operations to detect thermal stratification in the surge line. Two of the temperature detectors are on a moderately sloped run approximately midway between the RCS hot leg and the pressurizer. One detector is on the bottom of the pipe and the other detector on the top. The third detector is located on the pressurizer surge line close to the pressurizer nozzle. This detector is used to monitor cold water insurges to the pressurizer during transient operations.

The temperature is monitored at the three locations using strap-on resistance temperature detectors. Temperature indication is provided in the main control room. One low-temperature alarm is provided to alert the operator of thermal stratification in the surge line. This alarm is associated with the detector on the bottom of the pipe.

During shutdown operations, this temperature instrumentation will be monitored to detect possible surge line stratification. If stratification is detected, the operators can increase spray flow to increase the outsurge from the pressurizer and reduce stratification in the surge line.

19E.2.1.2.3 Step-nozzle Connection

The AP1000 RNS uses a step-nozzle connection to the RCS hot leg. The step-nozzle connection has two effects on mid-loop operation. One effect is to lower the RCS hot leg level at which a vortex occurs in the residual heat removal pump suction line due to the lower fluid velocity in the hot leg nozzle. This increases the margin from the nominal mid-loop level to the level where air entrainment into the pump suction begins.

Another effect of the step-nozzle is that, if a vortex should occur, the maximum air entrainment into the pump suction as shown experimentally will be no greater than 5 percent (Reference 4). The RNS pumps can operate with 5% air-entrainment. As discussed in NUREG-0897 (Reference 5), low levels of air ingestion can be tolerated, and a pump inlet void fraction of 5% has been shown experimentally to reduce the pump head less than 15%. At this level of degradation, the RNS pumps would maintain decay heat removal. The step-nozzle thereby precludes air binding of the pump and will allow for RNS pump operation with low water levels in the hot leg.

19E.2.1.2.4 Improved RCS Draindown Method

During the cooldown operations, the RCS water level is drained to a mid-loop level to permit steam generator draining and maintenance activities. The AP1000 has improved the reliability of draindown operations by incorporating a dedicated drain path to be used to reduce the water level in the RCS controlled in the main control room. In current plants, various drain paths can be used either locally or remotely from the control room. These drain paths include the safety-related residual heat removal system, loop drain valves, and letdown. The result is that draining of the RCS can be difficult to control, and perturbations in water level can occur due to inadvertent system manipulations of which the operators are not always aware.

The AP1000 RCS drain path is via the CVS letdown line from the RNS cross-connect provided to maintain full RCS purification flow during shutdown. The letdown line flow control valve controls the letdown rate, which controls the RCS draindown rate. At the appropriate time during the cooldown, the operator initiates the draindown by placing the CVS letdown control valve into a refueling draindown mode. At this time, the makeup pumps are turned off and the letdown flow control valve controls the drain rate to the liquid radwaste system at the initial maximum rate of approximately 100 gpm. The rate is reduced once the level in the RCS is to the top of the hot leg. The letdown rate is manually controlled based upon the difference in flow instruments readings in the CVS letdown line and injection line. The letdown flow control valve as well as the letdown line containment isolation

valve receives a signal to automatically close once the appropriate level is attained. Alarms actuate in the control room if the RCS level falls below the automatic letdown valve closure setpoint so that the operator is alerted to manually isolate the letdown line. Furthermore, an automatic isolation of the letdown line is actuated on low hot leg level. This draindown method provides a reliable means of attaining mid-loop conditions.

19E.2.1.2.5 ADS Valves

The ADS first-, second-, and third-stage valves, connected to the top of the pressurizer, are open whenever the core makeup tanks (CMTs) are blocked during shutdown conditions while the reactor vessel upper internals are in place. This provides a vent path to preclude pressurization of the RCS during shutdown conditions if decay heat removal is lost. This also allows the IRWST to automatically provide injection flow if it is actuated on a loss of decay heat removal. In addition, two of the four ADS fourth-stage valves are required to be available during reduced inventory operations to preclude surge line flooding following a loss of the RNS.

19E.2.1.2.6 Steam Generator Channel Head

The AP1000 steam generator is a vertical-shell U-tube evaporator with integral moisture separating equipment. The generator is discussed in Subsection 5.4.2.

On the primary side, the reactor coolant flow enters the primary chamber via the hot leg nozzle. The lower portion of the primary chamber is hemispherical and merges into a cylindrical portion, which mates to the tubesheet. This arrangement provides enhanced access to all tubes, including those at the periphery of the bundle, with robotics equipment. This feature enhances the ability to inspect, replace, and repair portions of the AP1000 unit compared to the more hemispherical primary chamber of earlier designs. The channel head is divided into inlet and outlet chambers by a vertical divider plate extending from the apex of the head to the tubesheet.

The reactor coolant enters the inverted U-tubes, transferring heat to the secondary side during its traverse, and returns to the cold leg side of the primary chamber. The flow exits the steam generator via two cold leg nozzles to which the reactor coolant pumps are directly attached.

The AP1000 steam generator channel head has provisions to drain the head. For minimizing deposits of radioactive corrosion products on the channel head surfaces and for enhancing the decontamination of these surfaces, the channel head cladding is machined or electropolished for a smooth surface.

The steam generator is equipped with permanently mounted nozzle dam brackets, which are designed to support nozzle dams during refueling operations. The design pressure of the nozzle dam bracket and nozzle dam is selected to withstand the RCS pressures that can occur during a loss of shutdown cooling. The nozzle dam design pressure is at least 50 psia.

The AP1000 nozzle dams can be installed with the hot leg water level at the nominal water level for mid-loop operations. The nozzle dams can be inserted via the steam generator manway. The ADS valves connected to the pressurizer are open during all reduced inventory operations including nozzle dam installation, and provide a vent path to preclude pressurization of the reactor coolant system following a loss of decay heat removal when the nozzle dams are installed.

19E.2.2 Steam Generator and Feedwater Systems

19E.2.2.1 System Description

This section discusses the AP1000 steam generator system (SGS) and the main and startup feedwater system (FWS) designs as they relate to shutdown operations. These systems are discussed in Chapter 10.

19E.2.2.2 Design Features to Address Shutdown Safety

19E.2.2.2.1 Feedwater Control

The AP1000 provides improvements in feedwater control that minimizes the probability of loss of feedwater transients during low power and shutdown modes. The main feedwater pumps are capable of providing feedwater during all modes of operation, including plant startup and standby conditions. In addition, the startup feedwater pumps are automatically started in the event that the main feedwater pumps are unable to continue to operate. The startup feedwater pumps are also automatically loaded on the diesels for operation following a loss of offsite power, during operating modes when the steam generators can be used for decay heat removal.

19E.2.2.2.2 Safety-Related Actuation in Shutdown Modes

The AP1000 has safety-related actuations associated with the SGS that are operable during shutdown modes. These include the PRHR HX actuation on low steam generator level during shutdown modes, and this is discussed in Subsection 19E.2.3 of this appendix. Also included is the isolation of the main steam line on a high (large) negative rate of change in steam pressure. This safety-related signal is provided to address a steam line break that could occur in Mode 3. If actuated, this signal causes the MSIVs to close to terminate the blowdown of the SGS following a steam line break. This signal is placed into service below the setpoint that disables the low steam line pressure signal (P11) that actuates steam line isolation as discussed in Section 7.3. When the operator manually blocks the low steam line pressure signal, the steam line high pressure-negative rate signal is automatically enabled.

This signal is operable during Mode 3 when a secondary side break or stuck open valve could result in the rapid depressurization of the steam line(s). In Modes 4, 5, and 6, this function is not needed for accident detection and mitigation. Subsection 19E.4.2.3 discusses steam line break events that could occur in shutdown modes. Operability of this actuation logic is discussed in the AP1000 Technical Specifications (Section 16.1).

19E.2.2.2.3 Steam Generator Cooling in Shutdown Modes

The secondary side of the steam generators can be cooled during shutdown by recirculating their contents through the blowdown system heat exchanger. This feature reduces the challenges to low-temperature overpressure events. During RCS water-solid operation, heat input from the steam generators is capable of challenging the low-temperature relief valve. The Technical Specifications prevent the operators from starting an RCP with the steam generator secondary side temperature more than 50°F higher than the primary side, with the pressurizer water-solid. With the RCS water-solid, the heat input that could occur would cause the system to be pressurized to the setpoint of the low-temperature overpressure relief valve in the RNS.

When the RCPs are operating, the secondary side of the steam generator is cooled by steaming to the MSS. Once the RNS is aligned, and steaming to the MSS is decreased, the secondary side of the steam generators is cooled by operation of the RNS. However, once the RCPs are tripped, water does not circulate through the primary side of the tubes and the secondary side of the steam

generators remains at elevated temperature. With the ability to cool the secondary side via the blowdown system, the AP1000 reduces the probability that an RCP would be started with the secondary side of the generator at elevated temperature. This cooling also makes the equipment available for maintenance at the earliest time in an outage.

The AP1000 has also incorporated steam generator fluid thermocouples to monitor the temperature of the fluid in the secondary side of the steam generator. This improves the ability of the operators to monitor this temperature to prevent them from inadvertently starting an RCP with the secondary side at elevated temperatures.

19E.2.3 Passive Core Cooling System

19E.2.3.1 System Description

The passive core cooling system (PXS) is described in Section 6.3.

19E.2.3.2 Design Features to Address Shutdown Safety

A significant improvement in shutdown safety for the AP1000 is the availability of a dedicated safety-related system that can be automatically or manually actuated in response to an accident that can occur during shutdown. In current plants, the safety-related systems that mitigate the consequences of an accident are also the operating systems that are used for decay heat removal. In the AP1000, nonsafety-related active systems provide the first level of defense, while the passive safety-related systems are available during shutdown modes to mitigate the consequences of an accident. This design approach results in a significant improvement in the AP1000 shutdown risk.

19E.2.3.2.1 Core Makeup Tanks

The CMTs provide RCS makeup. During shutdown, the CMTs are available in Modes 3, 4, and 5, until the RCS pressure boundary is open and the pressurizer water level is reduced. During power operation, the CMTs are automatically actuated on various signals including a safeguards actuation signal (low RCS pressure, low RCS temperature, low steam line pressure, and high containment pressure) and on low pressurizer water level. See Chapter 7 for a description of the AP1000 PMS actuation logic. In shutdown modes, portions of the safeguards actuation signal are disabled to allow the RCS to be cooled and depressurized for shutdown. For instance, the low RCS pressure and temperature, and low steam line pressure signals are blocked in Mode 3 prior to cooling and depressurizing the RCS. Therefore, during shutdown Modes 3, 4, and 5, the primary signal that actuates the CMTs due to a loss of inventory is the pressurizer level signal. In Mode 5, with the RCS open (in preparation for reduced inventory operations), the low pressurizer level signal is blocked prior to draining the pressurizer. Therefore, in Mode 5 with the RCS open, the CMTs are not required to be available and the RCS makeup function is provided by the IRWST.

The CMTs also provide an emergency boration function for accidents such as steam line breaks. However, the signals that provide the primary protection for this function (low steam line pressure, low RCS pressure, and low RCS temperature) are blocked in Mode 3 as discussed above. Prior to blocking these signals in Mode 3, the Technical Specifications require that the RCS be sufficiently borated. For these events, the pressurizer level signal provides automatic actuation of the CMTs for a steam line break that might occur due to the RCS shrinkage that would occur.

19E.2.3.2.2 Accumulators

The PXS accumulators provide safety injection following a LOCA. In Mode 3, the accumulators must be isolated to prevent their operation when the RCS pressure is reduced to below their set pressure.

The accumulator isolation valves are closed when the RCS pressure is reduced to 1000 psig to block their injection when the RCS pressure is reduced to below the normal accumulator pressure.

19E.2.3.2.3 In-containment Refueling Water Storage Tank

The IRWST provides long-term RCS makeup. During shutdown, the IRWST is available until Mode 6, when the reactor vessel upper internals are removed and the refueling cavity flooded. At that time, the IRWST is not required, due to the large heat capacity of the water in the refueling cavity.

The IRWST injection paths are actuated on a low-2 CMT water level. This signal is available in shutdown Modes 3, 4, and 5, with the RCS intact. When the RCS is open to transition to reduced inventory operations, the CMT actuation logic on low pressurizer level is removed, and the CMTs can be taken out of service. For these modes, automatic actuation of the IRWST can be initiated (on a two-out-of-two basis) on low hot leg level.

19E.2.3.2.4 Passive Residual Heat Removal Heat Exchanger

The PRHR HX provides decay heat removal during power operation and is required to be available in shutdown Modes 3, 4, and 5, until the RCS is open. In these modes, the PRHR HX provides a passive decay heat removal path. It is automatically actuated on a CMT actuation signal, which would eventually be generated on a loss of shutdown decay heat removal, as shown in the analysis provided in Section 19E.4 of this appendix. In modes with the RCS open (portions of Mode 5 and Mode 6), decay heat removal is provided by “feeding” water from the IRWST and “bleeding” steam from the ADS.

19E.2.3.2.5 Reduced Challenges to Low-Temperature Overpressure Events

Another design feature of the PXS that reduces challenges to shutdown safety is the elimination of high-head safety injection pumps in causing low temperature overpressure events. In current plants, during water solid operations that may be necessary to perform shutdown maintenance, the high-head safety injection pumps are a major source of cold overpressure events. To address this, plants are required to lock out safety injection pumps to prevent them from inadvertently causing a cold overpressure event. This eliminates a potential source of safety injection for a loss of inventory event that could occur at shutdown. With the AP1000 PXS, the CMTs are not pressurized above RCS pressure and are, therefore, not capable of causing a cold overpressure event. Therefore, they are not isolated until the pressurizer is drained for mid-loop. Low-temperature overpressure events are discussed in Subsection 19E.4.10.1.

19E.2.3.2.6 Discussion of Safe Shutdown for AP1000

The functional requirements for the PXS specify that the plant be brought to a stable condition using the PRHR HX for events not involving a loss of coolant. For these events, the PXS, in conjunction with the passive containment cooling system (PCS), has the capability to establish long-term safe shutdown conditions, cooling the RCS to less than 420°F within 36 hours, with or without the RCPs operating.

The CMTs automatically provide injection to the RCS as the temperature decreases and the pressurizer level decreases, actuating the CMTs. The PXS can maintain stable plant conditions for a long time in this mode of operation, depending on the reactor coolant leakage and the availability of ac power sources. For example, with a technical specification leak rate of 10 gpm, stable plant conditions can be maintained for at least 10 hours. With a smaller leak, a longer time is available. However, in scenarios when ac power sources are unavailable for as long as 24 hours, the ADS will automatically actuate.

For LOCAs and other postulated events where ac power sources are lost, or when the CMT levels reach the ADS actuation setpoint, the ADS initiates. This results in injection from the accumulators and subsequently from the in-containment refueling water storage tank, once the RCS is nearly depressurized. For these conditions, the RCS depressurizes to saturated conditions at about 240°F within 24 hours. The PXS can maintain this safe shutdown condition indefinitely.

The primary function of the PXS during a safe shutdown using only safety-related equipment is to provide a means for boration, injection, and core cooling. Analysis is provided in Subsection 19E.4.10.2 of this appendix that verifies the ability of the AP1000 passive safety systems to meet the safe shutdown requirements.

19E.2.3.2.7 Containment Recirculation Screens

The PXS containment recirculation screens may have to function in the longer-term during a shutdown accident that results in ADS operation. Effective screen design, plant layout, and other factors prevent clogging of these screens by debris during such accident operations.

- Two very large interconnected screens are provided.
- A significant delay is provided between the accident/ADS stage opening and the initiation of recirculation (at least 2 hours).
- Deep flood up levels are provided post ADS operation (31 ft of water above the lowest level in containment and 25.5 ft above floors around screens).
- Bottom of screens are located well above the lowest containment level (13.5 feet) as well as the floors around them (2 feet).
- Top of screens are located well below the containment floodup level (~10 ft from top screens to minimum flood level).
- Screens have protective plates located no more than 1 foot above the top of the screens and extend at least 10 feet in front and 7 feet to the side of the screens.
- Screens have conservative flow areas to account for plugging. Operation of the nonsafety-related normal residual heat removal pumps with suction from the IRWST and the containment recirculation lines is considered in sizing screens. Note that adequate PXS performance can be supported by one screen with more than 90 percent of its surface area completely blocked.
- During recirculation operation, the velocity approaching the screens is very low, which limits the transport of debris.
- Each screen has a fine screen.
- Technical Specifications require the screens to be inspected during each refueling outage.
- As discussed in Subsection 6.3.8.1, a cleanliness program to limit the amount of foreign materials that might be left in the containment following refueling and maintenance outages and become debris during an accident.

19E.2.3.3 Shutdown Operations

Operation of the PXS during operating modes and during accident events including shutdown events is discussed in Subsection 6.3.3. The following is a discussion of a loss of shutdown cooling during reduced inventory operations which can be a limiting shutdown event.

19E.2.3.3.1 Operation During Loss of Normal Residual Heat Removal Cooling During Mid-loop Events

During RCS maintenance, the most limiting shutdown condition anticipated is with the reactor coolant level reduced to the hot leg (mid-loop) level and the RCS pressure boundary opened. It is normal practice to open the steam generator channel head manway covers to install the hot leg and cold leg nozzle dams during a refueling outage. In this situation, the RNS is used to cool the RCS. The AP1000 incorporates features to reduce the probability of losing RNS. However, because the RNS is nonsafety-related, its failure has been considered.

In this situation, core cooling is provided by the safety-related PXS, using gravity injection from the IRWST, while venting through the ADS valves (and possibly through other openings in the RCS). Note that with the RCS depressurized and the pressure boundary opened, the PRHR HX is unable to remove the decay heat because the RCS cannot heat sufficiently above the IRWST temperature.

During plant shutdown, at 1000 psig, the accumulators are isolated to prevent inadvertent injection. Prior to draining the RCS inventory below the no-load pressurizer level, the CMTs are isolated by closing the inlet MOVs to preclude inadvertent draining into the RCS while preparing for mid-loop operation. Although these tanks are isolated from the RCS, the valves can be remotely opened by the operators to provide additional makeup water injection.

Prior to initiating the draindown of RCS to mid-loop level, the automatic depressurization first-, second-, and third-stage valves are opened. This alignment provides a sufficient RCS vent flow path to preclude system pressurization in the event of a loss of nonsafety-related decay heat removal during mid-loop operation. The ADS first- to third-stage valves are required to be opened before blocking the CMTs. They are required to remain open until either the RCS level is increased and the RCS is closed, or until the upper core internals are removed and the refueling cavity flooded. Note that the upper internals can restrict the vent flow path and prevent water in the refueling cavity from draining into the RCS unless ADS valves are open.

The IRWST injection squib valves and fourth stage ADS valves are automatically opened if the RCS hot leg level indication decreases below a low setpoint. A time delay is provided to provide time for the operators to restore nonsafety-related decay heat removal prior to actuating the PXS. The time delay with an alarm in the containment serves to protect maintenance personnel. Once the IRWST injection valves and fourth stage ADS valves open, the IRWST provides gravity-driven injection to cool the core. Containment recirculation flow would be automatically initiated when the IRWST level dropped to a low level to provide long-term core cooling.

Subsection 19E.4.8.3 provides the assessment of the loss of the RNS during mid-loop operations. Table 19E.2-1 provides the results of calculations performed to demonstrate the amount of time between a loss of RNS that could occur at mid-loop until core uncovery. This calculation is performed with the RCS water level at the nominal mid-loop water level and is performed with conservative, design basis assumptions for decay heat. As described previously and shown in Table 19E.2-1, the operators have a significant amount of time to actuate gravity injection before core uncovery. In addition, the PMS, on a two-out-of-two basis, provides a signal to actuate the IRWST when the hot legs empty.

This arrangement provides automatic core cooling protection, in mid-loop operation, while also providing protection (an evacuation alarm and sufficient time to evacuate) for maintenance personnel in containment during mid-loop operation.

Containment closure capability is required to be maintained during mid-loop operation, as discussed in Subsection 19E.2.6.2 of this appendix. With the containment closed, containment recirculation can continue indefinitely with decay heat generating steam condensed on the containment vessel and drained back into the IRWST and/or the containment recirculation.

19E.2.4 Normal Residual Heat Removal System

19E.2.4.1 System Description

The normal residual heat removal system (RNS) is discussed in Subsection 5.4.7.

19E.2.4.2 Design Features to Address Shutdown Safety

The AP1000 has incorporated various design features to improve shutdown safety. The RNS features that have been incorporated to address shutdown safety are described in this subsection.

19E.2.4.2.1 RNS Pump Elevation and NPSH Characteristics

The AP1000 RNS pumps are located at the lowest elevation in the auxiliary building. This location provides the RNS pumps with a large available NPSH during all modes of operation including RCS mid-loop and reduced inventory operations. The large NPSH provides the pumps with the capability to operate during most mid-loop conditions without throttling the RNS flow. If the RCS is at mid-loop level and saturated conditions, some throttling of a flow control valve is necessary to maintain adequate net positive suction head for the RNS pumps. The RNS pumps can be restarted and operated with RCS conditions that might occur following a temporary loss of RNS cooling.

The plant piping configuration, piping elevations and routing, and the pump characteristics allow the RNS pumps to be started and operated at their full design flow rates in most conditions without the need to reduce RNS pump flow to meet pump NPSH requirements. This reduces the potential failure mechanism that exists in current PWRs, where failure of an air-operated control valve can result in pump runout and cavitation during mid-loop operations.

19E.2.4.2.2 Self-Venting Suction Line

The RNS pump suction line is sloped continuously upward from the pump to the RCS hot leg with no local high points. This eliminates potential problems with refilling the pump suction line if an RNS pump is stopped due to pump cavitation and/or excessive air entrainment. With the self-venting suction line, the line will refill and the pumps can be immediately restarted once an adequate level in the hot leg is re-established.

19E.2.4.2.3 IRWST Injection via the RNS Suction Line

During shutdown modes, initiating events such as the loss of the nonsafety-related RNS are postulated. Such events would require IRWST injection as discussed in Subsection 19E.2.3 of this appendix, and as shown in the accident analyses provided in Section 19E.4. For initiating IRWST injection, the operation of PXS squib valves in the IRWST injection line is required. However, the operators can use the RNS pump suction line that connects to the IRWST to provide controlled IRWST injection. This flow path, shown in Figure 19E.9-1, connects the IRWST directly to the RCS via the RNS hot leg suction isolation valves and provides a diverse method for IRWST injection. In addition, it would be the preferred method of providing IRWST injection because the flow would be

controllable by the operation of the IRWST suction line isolation valve. The RNS isolation valve is equipped with a throttle capability to provide the operators with the capability to control the injection flow via this path. The operator would monitor the RCS hot leg level while controlling flow through this valve. This path provides IRWST injection regardless of whether the RNS pumps are operating.

19E.2.4.2.4 Codes and Standards/Seismic Protection

The portions of the RNS located outside containment (that serve no active safety functions) are classified as AP1000 equipment Class C so that the design, manufacture, installation, and inspection of this pressure boundary is in accordance with the following industry codes and standards and regulatory requirements: 10 CFR 50, Appendix B (Reference 6); Regulatory Guide 1.26, quality group C (Reference 7); and ASME Boiler and Pressure Vessel Code, Section III, Class 3 (Reference 8). The pressure boundary is classified as seismic Category I.

19E.2.4.2.5 Increased Design Pressure

The portions of the RNS from the RCS to the containment isolation valves outside containment are designed to the operating pressure of the RCS. The portions of the system downstream of the suction line containment isolation valve and upstream of the discharge line containment isolation valve are designed so that its ultimate rupture strength is not less than the operating pressure of the RCS. The design pressure of the RNS is 900 psig, which is 40 percent of operating RCS pressure.

19E.2.4.2.6 Reactor Coolant System Isolation Valve

The RNS contains an isolation valve in the pump suction line from the RCS. This motor-operated containment isolation valve is designed to the RCS pressure. It provides an additional barrier between the RCS and lower pressure portions of the RNS.

19E.2.4.2.7 Normal Residual Heat Removal System Relief Valve

The inside containment RNS relief valve is connected to the residual heat removal pump suction line. This valve is designed to provide low-temperature, overpressure protection of the RCS as described in Subsection 5.2.2. The valve, connected to the high-pressure portion of the pump suction line, reduces the risk of overpressurizing the low-pressure portions of the system.

19E.2.4.2.8 Features Preventing Inadvertent Opening of Isolation Valves

The RCS isolation valves are interlocked to prevent their opening at RCS pressures above 450 psig. Section 7.6 discusses this interlock. The power to these valves is administratively blocked during normal power operation.

In addition, these valves are interlocked with the RNS/IRWST isolation valves to prevent their opening with the RNS open to the IRWST. This precludes the blowdown of the RCS to the IRWST through the RNS upon system initiation.

19E.2.4.2.9 RCS Pressure Indication and High Alarm

The AP1000 RNS contains an instrumentation channel that indicates pressure in each normal residual heat removal pump suction line. A high-pressure alarm is provided in the main control room to alert the operator to a condition of rising RCS pressure that could eventually exceed the design pressure of the RNS.

19E.2.5 Component Cooling and Service Water Systems

Two different means are provided to protect the lower-pressure CCS from overpressure if RNS heat exchanger tube leakage occurs during plant cooldown or shutdown operations.

A relief valve is located on the CCS cooling water line, inside the upstream and downstream manual isolation valves for each RNS heat exchanger. The valve satisfies requirements in Section VIII of the ASME code for overpressure protection of heat transfer equipment. This relief valve provides both thermal overpressure and tube leakage protection in the event that the section of piping containing the RNS heat exchanger is isolated from the remainder of the CCS. The valve discharges directly into the auxiliary building sump.

If RNS heat exchanger tube leakage occurs with the affected heat exchanger not isolated from the CCS, the excess volume added to the CCS by the leak will begin to fill the CCS surge tank. If the CCS surge tank fills before the leak is isolated, fluid is discharged through the tank vent into the turbine building sump to prevent over-pressurization of any portion of the CCS. Leakage into the system will produce a CCS liquid radiation monitor alarm, and an increase in CCS surge tank level that results in a tank high level alarm.

Doses from the RNS heat exchanger tube rupture event would be below those produced by the primary sample line break outside containment with the plant at power.

19E.2.6 Containment Systems

19E.2.6.1 System Description

The containment systems are described in Section 6.2.

19E.2.6.2 Design Features to Address Shutdown Safety

The AP1000 has addressed the issue of containment closure at shutdown and incorporated the following requirements in the Technical Specifications (Chapter 16). In shutdown Modes 3 and 4, containment status is the same as at-power. Specifically, containment integrity is required, the major equipment hatches are closed and sealed, and containment air locks and isolation valves are operable.

In Modes 5 and 6, containment closure capability is required during shutdown operations when there is fuel inside containment. Containment closure is required to maintain, within containment, the cooling water inventory. Due to the large volume of the IRWST and the reduced sensible heat during shutdown, the loss of some of the water inventory can be accepted. Further, accident analyses provided in Section 19E.4 of this appendix show that containment closure capability is not required to meet offsite dose requirements. Therefore, containment does not need to be leak-tight as required for Modes 1 through 4.

In Modes 5 and 6, there is no potential for steam release into the containment immediately following an accident. Pressurization of the containment could occur only after heatup of the IRWST due to PRHR HX operation (Mode 5 with RCS intact), after heatup of the RCS with direct venting to the containment (Mode 5 with reduced RCS inventory or Mode 6 with the refueling cavity not fully flooded), or after heatup of the RCS and refueling cavity (Mode 6 with refueling cavity fully flooded). To limit the magnitude of cooling water inventory losses and because local manual action may be required to achieve containment closure, the containment hatches, air locks, and penetrations must be closed prior to steaming into containment.

The containment equipment hatches, which are part of the containment pressure boundary, provide a means for moving large equipment and components into and out of containment. If closed, the equipment hatch is held in place by at least four bolts. If open, each equipment hatch can be closed using a dedicated set of hardware, tools, and equipment. A self-contained power source is provided to drive each hoist while lowering the hatch into position. Large equipment and components may be moved through the hatches as long as they can be removed and the hatch closed prior to steaming into the containment.

The containment air locks, which are also part of the containment pressure boundary, provide a means for personnel access during Modes 1, 2, 3, and 4 unit operation. Each air lock has a door at both ends. The doors are normally interlocked to prevent simultaneous opening when containment operability is required. During periods of unit shutdown when containment closure is not required, the door interlock mechanism may be disabled, allowing both doors of an air lock to remain open for extended periods when frequent containment entry is necessary. Temporary equipment connections (for example, power or communications cables) are permitted as long as they can be removed to allow containment closure prior to steaming into the containment.

Containment spare penetrations, which also provide a part of the containment boundary, provide for temporary support services (electrical, I&C, air, and water supplies) during Modes 5 and 6. Each penetration is flanged and normally closed. During periods of plant shutdown, temporary support systems may be routed through the penetrations; temporary equipment connections (for example, power or communications cables) are permitted as long as they can be removed to allow containment closure prior to steaming into the containment.

The spare penetrations must be closed or, if open, capable of closure prior to reaching boiling conditions within reactor coolant inventory. Temporary containment penetrations that may be employed during shutdown modes must have a design pressure equal to the containment design pressure of 59 psig.

Containment penetrations, including purge system flow paths, that provide direct access from containment atmosphere to outside atmosphere must be isolated or isolatable on at least one side. Isolation may be achieved by an operable automatic isolation valve or by a manual isolation valve, blind flange, or equivalent.

The fuel transfer canal may be opened to provide for the transfer of new and spent fuel into and out of containment during Modes 5 and 6. At times when the canal is opened, it must be isolatable on at least one side by closure of the flange within containment or the gate valve outside containment.

19E.2.7 Chemical and Volume Control System

19E.2.7.1 System Description

The chemical and volume control system (CVS) is described in Subsection 9.3.6.

19E.2.7.2 Design Features to Address Shutdown Safety

The AP1000 CVS is a nonsafety-related system. However, portions of the system are safety-related and perform safety-related functions, such as containment isolation, termination of inadvertent RCS boron dilution, RCS pressure boundary preservation, and isolation of excessive makeup.

Boron dilution events during low power modes can occur for a number of reasons, including malfunctions of the makeup control system. Regardless of the cause, the protection is the same. The CVS is designed to avoid and/or terminate boron dilution events by automatically closing either one of two series, safety-related valves in the demineralized water supply line to the makeup pump

suction to isolate the dilution source. Additionally, the suction line for the CVS makeup pump is automatically realigned to draw borated water from the boric acid tank. The automatic boron dilution protection signal is safety-related and is generated upon any reactor trip signal, source-range flux multiplication signal, low input voltage to the Class 1E dc and uninterruptible power supply system battery chargers, or a safety injection signal.

The safety analysis of boron dilution accidents is provided in Chapter 15 and is discussed in Subsection 19E.4.5 of this appendix. For dilution events that occur during shutdown, the source-range flux-doubling signal is used to isolate the line from the demineralized water system by closing the two safety-related remotely operated valves. The three-way pump suction control valve aligns the makeup pumps to take suction from the boric acid tank and, therefore, stops the dilution.

For refueling operations, administrative controls are used to prevent boron dilutions by verifying that the valves in the line from the demineralized water system are closed and locked. These valves block the flow paths that can allow unborated makeup water to reach the RCS. Makeup required during refueling uses borated water supplied from the boric acid tank by the CVS makeup pumps.

During refueling operations (Mode 6), two source-range neutron flux monitors are operable to monitor core reactivity. This is required by the plant Technical Specifications. The two operable source-range neutron flux monitors provide a signal to alert the operator to unexpected changes in core reactivity. The potential for an uncontrolled boron dilution accident is precluded by isolating the unborated water sources. This is also required by the plant Technical Specifications.

19E.2.8 Spent Fuel Pool Cooling System

19E.2.8.1 System Description

The spent fuel pool cooling system (SFS) is discussed in Subsection 9.1.3.

19E.2.8.2 Design Features to Address Shutdown Safety

The AP1000 has incorporated various design features to improve shutdown safety. The SFS features that have been incorporated to address shutdown safety are described in this subsection.

19E.2.8.2.1 Seismic Design

The spent fuel pool, fuel transfer canal (FTC), cask loading pit (CLP), cask washdown pit (CWP), and gates from the spent fuel pool-CLP and FTC-spent fuel pool are all integral with the auxiliary building structure. The auxiliary building is seismic Class I design and is designed to retain its integrity when exposed to a safe shutdown earthquake (SSE). The suction and discharge connections between the spent fuel pool and RNS are safety Class C, which is also seismic Class I. The emergency makeup water line from the PCS water storage tank to the spent fuel pool actually connects with the RNS pump suction line. This emergency makeup line is also safety Class C and seismic Class I. The spent fuel pool level instruments connections to the spent fuel pool are safety Class C, seismic Class I, and have 3/8-inch flow restricting orifices at the pool wall to limit the amount of a leak from the pool if the instrument or its piping develops a leak.

The refueling cavity is integral with the containment internal structure, and as such, is seismic Class I, and is designed to retain its integrity when exposed to an SSE. In addition, the AP1000 has incorporated a permanently welded seal ring to provide the seal between the vessel flange and the refueling cavity floor. This refueling cavity seal is part of the refueling cavity and is seismic Class I. Figure 19E.9-2 is a simplified drawing of the AP1000 permanent reactor cavity seal. The cavity seal is designed to accommodate the thermal transients associated with the reactor vessel flange.

19E.2.9 Control and Protection Systems

The AP1000 control and protection systems support the operations necessary for the AP1000 to achieve shutdown. These systems consist of a nonsafety-related plant control system (PLS), a safety-related protection and safety monitoring system (PMS), and a nonsafety-related diverse actuation system (DAS). These systems are discussed in Chapter 7.

19E.3 Shutdown Maintenance Guidelines and Procedures

This section presents an overview discussion of AP1000 shutdown maintenance guidelines and procedures captured as part of the AP1000 design and design certification program. Shutdown maintenance requirements and guidelines have been identified in various licensing submittals, such as the AP1000 Technical Specifications, (Section 16.1), and the design reliability assurance program, (Section 17.4).

Shutdown procedures were addressed in the AP600 design certification program by the submittal of the AP600 Emergency Response Guidelines (ERGs) (Reference 1), which include shutdown emergency procedures. These shutdown emergency procedures are applicable to the AP1000.

This section summarizes the major shutdown maintenance guidelines and procedures that have been identified.

19E.3.1 Maintenance Guidelines and Insights Important to Reducing Shutdown Risk

This section presents an overview of AP1000 shutdown maintenance guidelines and insights, which are either required for plant safety or are effective at reducing shutdown risk.

19E.3.1.1 Availability Requirements for Safety-Related Systems

Availability controls of the AP1000 safety-related systems are provided by the Technical Specifications. These availability requirements cover all modes of operation including shutdown.

19E.3.1.2 Availability Guidelines for Systems Important for Investment Protection

Availability guidelines for systems important for investment protection are discussed in the AP1000 Design Reliability Assurance Program, Section 17.4.

19E.3.1.3 Reactor Coolant System Precautions and Limitations at Shutdown

Precautions and limitations for RCS operation at shutdown are considered to minimize the risk to plant safety at shutdown. The most important of these are captured in the AP1000 Technical Specifications. However, other precautions and limitations associated with maintenance and operation at shutdown have been identified during the design of the AP1000. These are based on both the past operating experience of PWRs, as well as the designer's knowledge of the unique AP1000 design features. A summary of these precautions and limitations that apply to shutdown maintenance and operation is provided in this section.

19E.3.1.3.1 General Shutdown

Precautions and limitations for general shutdown are as follows:

- To provide mixing, at least one reactor coolant pump (RCP) or a normal residual heat removal pump should be in service while chemicals are being added to the system or the boron concentration is being changed. This requirement is included in the AP1000 Technical Specification 3.3.9.

- Reactor coolant samples must be taken at the regular intervals to check coolant chemistry, activity level, and boron concentration as specified in the appropriate Technical Specifications including 3.1.1, 3.4.11, and 3.1-1. In addition, during shutdown modes, more frequent checks on RCS boron concentration should be made when changes in RCS boron concentration are being made.

- When the RNS is in operation, the reactor coolant temperature should not exceed 350°F. The reactor coolant pressure should be limited to avoid approaching the RNS relief valve setpoint.

- The maximum allowable heatup and cooldown rates for the RCS are provided in the Technical Specifications.

- During cooldown, the RCPs located in the loop containing the pressurizer spray line should be operated to provide adequate pressurizer spray.

- The accumulators must be isolated prior to reducing the RCS pressure to the accumulator pressure (637 to 769 psig).

19E.3.1.3.2 Water-Solid Operation

Precautions and limitations for water-solid operation are as follows:

- The RNS inlet line should not be isolated from the reactor coolant loop unless there is a steam bubble in the pressurizer or the makeup pumps are stopped. This precaution provides relief valve protection of the RCS when it is at low pressure and water-solid.

- Whenever the plant is water-solid and the reactor coolant pressure is being maintained by the letdown containment isolation outside-containment valve, the RNS should remain open to the reactor coolant loops to maintain sufficient letdown flow through the bypass line from the RNS to the letdown heat exchanger, until a steam bubble is formed in the pressurizer. During this mode of operation, the isolation valve in the bypass line from the RNS to the letdown heat exchanger should be in the full-open position and the letdown orifice bypass valve should also be open.

- If all RCPs are stopped and the reactor coolant temperature is greater than 200°F, the first pump should not be restarted until a steam bubble has formed in the pressurizer. This precaution will minimize the pressure transient when the first pump is started. The steam bubble will accommodate the resultant expansion.

- When the reactor coolant pressure is being maintained by the letdown containment isolation outside containment valve, changes to the flow rate through the RNS loop by throttling of valves or starting and stopping the RNS pumps will result in changes to the reactor coolant pressure.

- Whenever the reactor coolant temperature is above 160°F, at least one RCP should be in operation.

19E.3.1.3.3 Steam Generators

Precautions and limitations for steam generators are as follows:

- During cooldown, all steam generators should be connected to the steam header to provide uniform cooldown of the reactor coolant loops.
- During steam plant warmup and at hot standby, draw steam slowly and regulate feedwater additions carefully to avoid rapid cooling of the reactor coolant.
- During cooldown, once RNS is in operation, and after the RCPs have been tripped, actions should be taken to cool the contents of the steam generator secondary side, either by recirculation and cooling of this water or by draining the contents via the blowdown lines.

19E.3.1.3.4 Surge Line

During heatup and cooldowns, the temperature difference between the pressurizer and the hot legs should be less than 320°F. This prevents unacceptable stress levels in the surge line.

19E.3.1.3.5 Reduced-Inventory Operations

Precautions and limitations for reduced-inventory operations are as follows:

- The timing of the initiation of draindown is highly dependent of the scenario that requires the drained condition. However, in order to drain down to mid-loop conditions, the reactor coolant pumps must be tripped, and the RCS temperature must be less than saturation. Typically, the reactor coolant pumps operate until the RCS temperature is reduced to less than 160°F. For a refueling outage, the transition to reduced inventory conditions should typically begin about 3-4 days after shutdown. For a forced outage condition, reduced inventory operations should not begin until the RCS temperature is less than 160°F.

  The time after shutdown directly affects the time that the RCS would boil and the rate at which inventory would be depleted following a loss of cooling event. Table 19E.2-1 presents the time to reach saturation, and the time to core uncovery for a loss of heat sink event initiated from mid-loop conditions at 28 hours after shutdown. For loss of heat sink events initiated earlier, the time to reach saturation and the time to uncover the core would be slightly decreased. The performance of the IRWST injection, in conjunction with ADS, is sufficient to mitigate the consequences of the event.

  The time after shutdown impacts the requirements for containment closure during shutdown as discussed in Subsection 19E.2.6.2 of this appendix (and captured in the Technical Specifications). For reduced inventory conditions, if the time to steaming (inside containment) following a loss of heat sink event is less than the time required to close the containment equipment hatches, then these hatches should be closed. If the time after shutdown is sufficiently long, such that steaming to containment would not occur prior to the containment hatches being able to be closed, then the equipment hatches could be open, with the ability to close them.

- As the RCS is drained, the rate of change in water level will vary non-linearly for a given drain rate due to the geometry of the RCS and the offset hot leg and cold leg piping. It is important to drain the RCS at a low rate to minimize the possibility of overdraining the system. Evaluations have been performed that indicate that a drain rate of 20 gpm is sufficient once the water level has been reduced to the top of the hot leg.

- After maintenance operations that result in draining the RCS, the system should be refilled with borated makeup water at the prevailing RCS boron concentration via the chemical and volume control system (CVS) makeup pumps. If the RCPs are drained, the pumps should be refilled with borated water via the pump drain line so that the pump is completely filled with borated water.

- After maintenance operations on the CVS purification loop (demineralizer, filters, and heat exchangers), the system should be purged, draining potential unborated water to the liquid radwaste system, and refilling it with borated water from the RCS. These operations should not be conducted at mid-loop or reduced inventory operations to avoid an inadvertent drop in RCS water level during mid-loop.

- The RCS hot leg level instruments should be operable and available prior to reduced inventory operations. Their automatic actuation functions are required to be operable in shutdown modes as described in Technical Specification 3.3.2.

19E.3.2 Shutdown Risk Management

This appendix contains insights of which Westinghouse is currently aware and which are related to AP1000 design certification.

19E.3.3 Shutdown Emergency Response Guidelines Overview

The AP600 ERGs (Reference 1) provide functional guidance for responding to accidents and transients that affect plant safety during shutdown modes of operation (operational Modes 5 and 6). The shutdown ERGs consist of a shutdown safety status tree for monitoring the critical safety functions and six shutdown guidelines for responding to the respective challenges to plant safety. The AP600 ERGs are applicable to AP1000 for the purpose of developing Emergency Operating Procedures.

The shutdown safety status tree provides a systematic method of determining the safety status of the plant. This status tree represents the critical safety functions that are of concern during plant shutdown conditions. Prior to this shutdown condition, the plant can be in any state ranging from heatup and pressurization (from 200°F to no-load temperature) to full power operation. Under these conditions (plant Modes 4 through 1), plant monitoring and response to a reactor trip or requirement for safety injection are covered by the optimal recovery guidelines, status trees, and function restoration guidelines of the at-power ERGs.

By using the shutdown status tree, plant conditions are monitored during plant shutdown after entering Mode 5 while normal operating procedures are in use for plant shutdown operations. The shutdown safety status tree is arranged so that the functions are checked in order of importance. Core cooling during shutdown conditions is addressed first. During plant shutdown conditions, the RNS provides core cooling, which requires adequate RCS inventory to operate properly. RCS inventory checks are made first to show core cooling will not be interrupted because of inadequate RCS inventory and as an early symptom to a loss of shutdown core cooling. After adequate RCS inventory is checked, RNS operation is checked to verify shutdown core cooling is being provided by the RNS. After RNS operation is verified, containment radiation is checked so that an unexpected uncontrolled release will not occur because containment integrity may be breached during plant shutdown maintenance activities. Core reactivity is then checked by monitoring source range flux doubling as an early symptom of an unintended RCS boron dilution, which should occur at a slow enough rate to allow appropriate action to be taken to reestablish shutdown margin. RCS cold overpressure symptoms of RCS pressure and temperature are monitored for maintaining the RCS pressure boundary integrity safety function.

Lastly, RCS temperature change, aside from any normal expected RCS temperature change, is used as an early symptom for potential degradation of the core cooling safety function and the RCS pressure boundary integrity safety function. The shutdown safety status tree is considered to be satisfied when all status tree blocks have been satisfied. If a challenge is identified during the monitoring of the tree, the tree directs plant operators to one of the appropriate six shutdown guidelines for mitigating actions.

The format and arrangement of the shutdown ERG documentation is similar to the at-power ERGs consisting of guidelines and background documents. Implementation of the shutdown ERGs into plant procedures will also be similar to the at-power ERGs with the task allocation between the man and the computer for doing this to be decided when designing features of the man-machine interface system.

19E.4 Safety Analyses and Evaluations

19E.4.1 Introduction

This section reviews each of the design basis accidents (DBAs) and transients presented in Chapter 15, with respect to lower power and shutdown modes. In Subsections 19E.4.2 through 19E.4.9, evaluations or analyses are performed for each case of the transient and LOCA analyses for events occurring at low power and shutdown operations, including the reduced reactor coolant system (RCS) inventory and refueling operations. The evaluations discuss the effects of key plant parameters (for example, plant control parameters, neutronic and thermal hydraulic parameters, and engineering safety features [ESFs]) on plant transient response (such as departure from nucleate boiling ratio [DNBR], peak pressure, and peak cladding temperature). The limiting case for each event category is identified. For those limiting cases bounded by the cases analyzed at power conditions, supporting rationales are provided.

For those events where analyses are presented in the shutdown modes, a discussion of the adequacy of the codes used is presented in Subsection 19E.4.1.2.

In Subsection 19E.4.10, additional analyses and evaluations demonstrate that the passive systems can bring the plant to a stable, safe condition and maintain this condition.

19E.4.1.1 Matrix of Chapter 15 Events

Table 19E.4.1-1 provides a list of Chapter 15 events. This table categorizes the events as “E” (requiring evaluation), “A” (requiring analysis), or “n/a” (not applicable). The “n/a” events are bounded by at-power analyses or current analyses.

The events denoted by an “n/a” in Table 19E.4.1-1 are as follows:

- Boron dilution design basis transient explained in Subsection 15.4.6 because it explicitly considers all modes such that no analysis or evaluation is required for this appendix

- Rod cluster control assembly (RCCA) withdrawal at-power explained in Subsection 15.4.2 because this event occurs only at-power

19E.4.2 Increase in Heat Removal from the Primary System

19E.4.2.1 Feedwater System Malfunctions Which Increase Heat Removal from the Primary System

Faults that decrease feedwater temperature or increase feedwater flow can be postulated in the feedwater system. These faults could increase heat removal from the primary system, which reduces RCS temperature. The reduction in RCS temperature could lead to an increase in core power generation (due to a negative moderator temperature coefficient) and result in a reduction in margin-to-core design limits. Unchecked, excessive feedwater flow could also result in overfilling the steam generators.

Discussions and analyses, initiated from Modes 1 and 2, of RCS cooldowns caused by feedwater system malfunctions are presented in Subsections 15.1.1 and 15.1.2. Subsection 15.1.1 covers reductions in feedwater temperature, and Subsection 15.1.2 covers increases in feedwater flow. Modes 1 and 2 are the limiting initial conditions for feedwater system induced RCS cooldown transients.

Protection against feedwater system induced cooldown transients is provided by the protection and safety monitoring system (PMS) through automatic functions that trip the reactor and isolate the feedwater system. The protection functions are available in all modes during which the feedwater system is in operation. Reactor trip includes overpower Δt, high power-range nuclear flux, high intermediate-range nuclear flux, or high source-range nuclear flux. The PMS closes the main feedwater control valves on low-1 RCS average temperature signal. The PMS also closes the main feedwater isolation valves and trips the booster/main feedwater pumps when RCS average temperature decreases below the low-2 RCS T_{avg} setpoint. These protection functions are arranged to detect symmetrical plant transients with a channel out of service and a single channel failure.

Additional PMS functions are provided to detect and protect against asymmetrical feedwater system malfunctions. Automatic reactor trip, closure of the main feedwater control and isolation valves, closure of the startup feedwater control and isolation valves, tripping of the booster/main feedwater pumps, and tripping of the startup feedwater pumps occur if the level in a single steam generator is above the high-2 water level setpoint. Similar actions occur if cold leg temperature in a single RCS loop decreases below the low T_{cold} setpoint. The high-2 steam generator level setpoint is active in Modes 1 through 4 unless the various feedwater valves are closed. This ensures that the steam generators cannot inadvertently be overfilled. The low T_{cold} signal is available in Modes 1 through 3. In Mode 3 prior to blocking the low T_{cold} signal, the RCS must be borated to cold shutdown conditions. With the RCS borated, no feedwater malfunction can be postulated to cool the RCS such that a core power excursion would occur.

The feedwater malfunction associated with a drop in feedwater temperature is less severe as power level is decreased. Normal operating feedwater temperature decreases as plant power level decreases. Therefore, if a fault suddenly reduces the feedwater temperature, the maximum change in feedwater temperature will occur if the plant is operating at full power.

As discussed in Subsection 19E.2.2 of this appendix, in Modes 2 and below, feedwater entering the steam generators is routed through the startup feedwater control valves. The maximum achievable flow rate through the startup feedwater path is much less than when flow is being controlled by the main feedwater control valves. Therefore, failure of a main feedwater control valve in Mode 2 and below is not likely. The assumption of a failed open startup feedwater control valve, in Mode 2 and below, will result in a relatively slow transient due to low feedwater flow rate.

The most severe RCS cooldowns caused by feed system malfunctions will occur in Modes 1 or 2. In Modes 3 or 4, RCS cooldowns due to feedwater malfunctions would be precluded, inconsequential,

or less severe than in Modes 1 or 2. The analyses presented in Chapter 15 bound the consequences of this class of events initiated in the shutdown modes.

19E.4.2.2 Excessive Increase in Secondary Steam Flow

An excessive increase in secondary steam flow (excessive load increase) is caused by a rapid increase in steam flow that results in a power mismatch between the reactor core power and the steam generator load demand. The plant control system (PLS) is designed to accommodate a 10-percent step load increase in steam flow in the range of 25 to 100 percent of full power. Analyses results for a 10-percent step increase in steam flow are presented in Subsection 15.1.3. The analyses are performed for Mode 1 from full-power initial conditions. Depending upon the plant and PMS characteristics (setpoint uncertainties), a reactor trip signal may or may not be generated for an excessive load increase from full power.

An excessive load increase in Mode 1 is considered limiting because an excessive load increase at full power will put the plant at the highest achievable power level. Load increases at less than full power, or during startup (Mode 2), will not reach as high a power level. The excessive load increase, in Mode 2, will not be as severe as the Mode 1 excessive load increase.

In Mode 3, the excessive load increase may be considered to be a simple steam release because there can be no load, per se, when the turbine is off-line and the core is subcritical. The Mode 3 load increase will be less limiting than the Mode 1 or Mode 2 case because the core is already subcritical. Automatic safeguards actuation signals may not be available if blocked by the operator (blocking is necessary to depressurize and cool down the RCS). However, the RCS must be borated to meet shutdown margin requirements at cold shutdown (200°F) prior to blocking automatic safeguards actuation signals to prevent a return to criticality in the event of a cooldown.

The Mode 4 situation is bounded by Mode 3 because pressure and temperature conditions in the primary and secondary systems are reduced. At some point in Mode 4, the RNS will be placed in service. In Modes 5 and 6, the RNS should be in operation. Any steam release will have little or no effect upon the core.

19E.4.2.3 Credible and Hypothetical Steam Line Breaks

The spurious opening of a steam generator safety or relief valve is a Condition II event and referred to as a credible steam line break. This event affects the core like a load increase but the analysis assumptions that are applied are different. The credible steam line break is usually assumed to be an unisolatable, uncontrolled steam release, which causes a non-uniform core cooldown (typical of an open safety valve) during the period immediately following a reactor trip which inserts all but the most reactive rod cluster control assembly (RCCA). The resulting reactivity excursion may be large enough to overcome the shutdown margin and return the core to critical, especially when there is little or no decay heat (with power peaking in the region of the stuck RCCA). The credible steam line break is analyzed in Mode 2, and the results are presented in Subsection 15.1.4. The assumptions used in the analysis lead to a more severe, post-trip transient than will result from a load increase initiated in Mode 1.

In Mode 1, prior to reactor trip, the transient characteristics of an inadvertent opening of a steam generator safety or relief valve are similar to the excessive load increase. A reactor trip signal, if needed, may result from overpower ΔT logic. After the reactor trip, the concern becomes a possible return to criticality with the most reactive RCCA stuck in the fully withdrawn position, leading to high local power levels. However, a post-trip return to criticality is less likely when this event occurs in Mode 1 than in Mode 2 because there will be more decay heat present, which tends to retard the cooldown.

In Mode 3, results are expected to be better than the Mode 2 case because pressure, temperature, and flow conditions will be less limiting. An occurrence in Mode 4 will be less severe than in Modes 2 or 3 due to the lower initial RCS temperature, and an effective decoupling of the secondary system from the primary system as the reactor coolant pumps (RCPs) are removed from service and the RNS is started. Automatic safeguards actuation signals are available through Mode 3, until the RCS is borated and the automatic safeguards signals are blocked (see excessive load increase discussion). Both CMTs continue to be available for automatic actuation on low-2 pressurizer level or manual actuation through Mode 4 with the RCS not being cooled by the RNS (see Technical Specification LCO 3.5.2). In Mode 4 with the RNS in operation and in Mode 5 with the RCS pressure boundary intact, one CMT is available for activation if needed.

Any cooldown in Modes 5 and 6 caused by depressurization of the secondary system is meaningless because the RCS is already cold, and the RNS system effectively decouples the steam generators from the core.

The steam line rupture is a Condition IV event, producing a greater uncontrolled steam release than the spurious opening of a steam generator safety valve (described above), but the relative effects in the various modes and requirements for protection equipment are the same. This is the most severe cooldown event.

19E.4.2.4 Inadvertent PRHR HX Operation

Inadvertent actuation of the PRHR HX causes an injection of relatively cold water into the RCS. This produces a reactivity insertion in the presence of a negative moderator temperature coefficient. Because the PRHR HX is connected to only one RCS loop, the cooldown resulting from its actuation is asymmetric with respect to the core. Inadvertent actuation of the PRHR HX could lead to an asymmetric power increase and a reduction in margin-to-core design limits.

A limiting analysis of an inadvertent actuation of the PRHR HX heat exchanger is presented in Subsection 15.1.6. The analysis is initiated in Mode 1 from hot full-power conditions. This is the most limiting case.

The PRHR HX heat transfer rate is a function of the inlet temperature to the heat exchanger and the flow rate through the heat exchanger. PRHR HX heat transfer rate is higher with high flow rates and high inlet temperatures. Therefore, the maximum heat removal rate will occur when the plant is at full-power condition with forced RCS flow and a high hot leg temperature. At plant full-power conditions, the PRHR HX heat removal rate is approximately 10 percent of full power. At hot zero power (HZP) conditions with natural circulation, heat removal by the PRHR HX is approximately 1.5 percent to 2 percent of full power.

The heat sink for the PRHR HX is the in-containment refueling water storage tank (IRWST), in which the heat exchanger is submerged. Prior to actuation of the PRHR HX, the fluid within the heat exchanger is in thermal equilibrium with the fluid in the IRWST. Thus, the PRHR HX is initially filled with relatively cold fluid which is at containment ambient temperature. When the PRHR HX is actuated, the initial fluid outsurge is fluid at containment ambient temperature. Once the original fluid in the PRHR HX is purged, the out-flow temperature trend of the heat exchanger is set by the temperature entering the heat exchanger from the RCS hot leg minus the temperature drop through the heat exchanger. Thus, the outlet fluid temperature is limited by the cooling capacity of the PRHR HX.

If the reactor is at power (Mode 1 or 2) when the PRHR HX is inadvertently actuated, a cooldown induced increase in core power will occur. The transient response will have two parts. As the cold fluid from the PRHR HX, which is initially at the ambient IRWST temperature, enters the RCS, a large core power increase will occur. The magnitude of the power increase is proportional to the volume of

the cold fluid in the PRHR HX. Once the original fluid is purged from the PRHR HX, the fluid temperature exiting the PRHR HX increases to a value limited by the cooling capacity of the PRHR HX. Core power will then decrease to a value higher than the initial core power, but in equilibrium with the heat removal capability of the steam generators plus the PRHR HX.

With the assumptions of a protection system channel out of service as allowed by the Technical Specifications, a failure of an additional protection system channel, and maximum instrument uncertainties, the asymmetric core power transient may not result in actuating any overpower reactor trips, such as high nuclear flux or overpower Δt. In this case, the core power transient is controlled only by the initial volume of cold water in the PRHR HX and the heat removal capability of the heat exchanger.

Higher initial core power will result in the largest achievable core power and in more severe consequences. Therefore, if the reactor is at-power, the full-power case produces the worst results.

In Mode 3, because the reactor is subcritical, inadvertent actuation of the PRHR HX produces a less severe power excursion than if the reactor is at power or at HZP with the reactor just critical. If in Mode 3 below no-load temperature, the cooldown caused by the actuation of the PRHR HX results in the cold leg temperature dropping below the low T_{cold} safeguards signal setpoint. This function actuates a reactor trip, initiates boration by the CMTs, and most importantly, trips all the RCPs. When the RCPs trip, natural circulation flow begins in the RCS and the PRHR HX loop. When natural circulation flow is initiated, the heat removal capability of the PRHR HX decreases to approximately 1.5 percent of full power and the severity of the transient is minimized. With the RCS in natural circulation, the cooldown rate of the RCS is also slowed. If criticality is obtained, boration by the CMTs will bring the core subcritical again.

The low T_{cold} safeguards signal may be blocked by the operator in Mode 3 to allow plant depressurization and cooldown to lower modes. However, prior to blocking the low T_{cold} safeguards signal, the RCS is borated to the shutdown margin requirements at cold shutdown (200°F). Therefore, in Mode 3 with safeguards signals blocked or in Mode 4, cooldown of the RCS by inadvertent actuation of the PRHR HX will not result in a reactivity excursion, which produces a power increase.

In Modes 5 and 6, the RCS will be borated such that a cooldown-induced power excursion could not be postulated. The RCS will be at 200°F or less, and with initial RCS temperatures this low, no significant cooling of the RCS by inadvertent actuation of the PRHR HX could be postulated.

19E.4.3 Decrease in Heat Removal by the Secondary System

19E.4.3.1 Loss of Load and Turbine Trip

Discussions and analyses of the consequences of loss of load, turbine trip, inadvertent closure of main steam isolation valves (MSIVs), or loss of condenser vacuum are presented in Subsections 15.2.2 through 15.2.5. These events are characterized by a rapid reduction in steam flow from the steam generators. This results in an increase in steam pressure and a heatup of the primary side if the reactor power is not reduced. The effects of the primary to secondary power mismatch during these events are mitigated by tripping the reactor and opening secondary and primary side safety valves. The severity of these events is increased if the primary to secondary power mismatch is increased. Therefore, the most severe results occur if the plant is initially operating in Mode 1 at maximum-rated plant power conditions rather than lower power conditions. The turbine is off-line below Mode 1 and transients related to turbine-related faults cannot occur.

In Modes 2, 3, or 4, the plant may be removing decay heat by dumping steam to the condenser. In Mode 4 when the RCS is below 350°F, decay heat is removed using the RNS. In Modes 2, 3, or 4,

the transient response to a loss of condenser vacuum or inadvertent MSIV closure is bounded by the turbine trip analysis from full power because the power mismatch is low. Decay heat removal can still be accomplished by the steam generators through atmospheric steam relief through power-operated relief valves (PORVs) if available or through steam generator safety valves, which are available through Mode 4 (see Technical Specification LCO 3.7.1). Additionally, decay heat can be removed with the PRHR HX, which is available through Mode 5 with the RCS intact (see Technical Specifications LCO 3.5.4 and 3.5.5).

19E.4.3.2 Loss of ac Power

A discussion and an analysis of a loss of ac power event are provided in Subsection 15.2.6. The loss of ac power results in the loss of forced primary coolant flow and the loss of main feedwater flow. This results in a heatup and pressurization of the RCS. If the reactor is at power, the event is mitigated by tripping the reactor. The reactor may be automatically tripped on low RCP speed, low RCS flow, low steam generator level, or several other primary side heatup signals. Also reactor trip may occur due to the loss of power to the control rod drive mechanisms.

Following reactor trip, the PRHR HX is activated for decay heat removal. Automatic PRHR HX actuation on low steam generator level is available in Modes 1 through 3 and in Mode 4 when the RCS is not being cooled by the RNS. The most limiting case for loss of ac power would be if the plant were at full rated power. This will result in the highest decay heat levels and stored energy in the RCS and the heat removal capability of the PRHR HX will be maximized. In Modes 4 or 5 with the RNS in operation, the plant response to a loss of ac power is the same at the loss of RNS cooling as discussed in Subsection 19E.4.8 of this appendix.

19E.4.3.3 Loss of Normal Feedwater

The main feedwater system is in operation during Modes 1 and 2. The startup feedwater system is used in Mode 2 below approximately 2 percent power, in Mode 3, and in Mode 4 before the RNS is aligned. In Mode 4 with the RNS aligned and in Modes 5 and 6, the feedwater system is not used, and therefore, loss of feedwater events is irrelevant.

A discussion and an analysis of a loss of normal feedwater event from rated full-power conditions are provided in Subsection 15.2.7. The loss of normal feedwater flow results in a heatup and pressurization of the RCS. If the reactor is at-power, the event is mitigated by tripping the reactor on low steam generator level.

Following reactor trip, the PRHR HX is activated for decay heat removal. Automatic PRHR HX actuation on low steam generator level is available in Modes 1 through 3 and in Mode 4 when the RCS is not being cooled by the RNS. The most limiting case for a loss of normal feedwater is with the plant initially at full rated power. This case will have the highest decay heat levels and stored energy in the RCS and the heat removal capability of the PRHR HX will be maximized. The analysis initiated from full power bounds cases initiated from the shutdown modes.

19E.4.3.4 Feedwater System Pipe Break

Depending upon the size of the break and plant operating conditions, the break could cause either an RCS heatup or an RCS cooldown. The cooldown aspects are less severe than a steam line break, which is discussed in Subsection 19E.4.2.3 of this appendix and is not considered in the following discussion.

The main feedwater system is in operation during Modes 1 and 2. The startup feedwater system is used in Mode 2 below approximately 2 percent power, in Mode 3, and in Mode 4 before the RNS is aligned. In Mode 4 with the RNS aligned and in Modes 5 and 6, the feedwater system is not used,

and therefore, a loss of feedwater caused by a feedwater system pipe break will not cause a heatup of the RCS.

A discussion and an analysis of feedwater system pipe break from rated full-power conditions are provided in Subsection 15.2.8. A rupture of a feedwater system pipe results in a loss of feedwater flow causing a heatup and pressurization of the RCS. If the reactor is at-power, the event is mitigated by tripping the reactor on low steam generator level.

Following reactor trip, the PRHR HX is activated for decay heat removal. Automatic PRHR HX actuation on low steam generator level is available in Modes 1 through 3 and in Mode 4 when the RCS is not being cooled by the RNS. The most limiting case for a feedline break occurs with the plant at full rated power. This case will have the highest decay heat levels and the highest stored energy in the RCS and the heat removal capability of the PRHR HX will be maximized.

19E.4.4 Decrease in Reactor Coolant Flow Rate

19E.4.4.1 Partial and Complete Loss of Forced RCS Flow

A partial loss of forced RCS flow may be caused by a mechanical or an electrical failure in an RCP or from a fault in the power supply to the pumps. An RCP failure will result in only the loss of a single RCP. A fault in the power supplies for the RCPs could result only in the loss of one, two, or all four RCPs.

The loss of one or more RCPs reduces the heat removal rate from the primary to the secondary coolant system and thereby causes a heatup in the RCS. The heatup of the RCS results in an increase in RCS pressure and a decrease in margin-to-core design limits (that is, departure from nucleate boiling [DNB]). An occurrence at full power will produce a greater and more rapid heatup than at part-power conditions or low-power conditions in Mode 2. Therefore, for evaluating the maximum RCS pressure or the minimum DNB ratio, analyses are performed at full-power conditions. Analyses for partial loss of forced RCS flow transients are presented in Subsection 15.3.1. Analyses for a complete loss of flow are presented in Subsection 15.3.2. These analyses bound loss of flow events initiated in other modes.

Protection for loss of forced RCS flow events is provided by tripping the reactor. This reduces reactor power and preserves margin-to-DNB limits. The AP1000 PMS includes a reactor trip on low RCS flow in any cold leg and a reactor trip on low RCP speed in any two of four RCPs. These two reactor trips are used to detect all possible partial and complete loss of RCS flow transients. Opening of the pressurizer safety valves in conjunction with the reactor trip prevents overpressurization of the RCS.

Below Mode 2, when the core is subcritical, forced RCS flow is not needed because margin-to-DNB is not an issue. It is common to have one or more RCPs out of service below Mode 2 because full RCS flow is no longer needed. In Modes 3 through 5, LCO 3.4.5 of the Technical Specifications requires that all four RCPs need to be operating if the reactor trip breakers are closed, to ensure that DNB limits are not exceeded, in the event RCCAs are inadvertently withdrawn. If the trip breakers are open and RCCA withdrawal is precluded, no RCPs are required to be operating in Modes 3 through 5.

Following reactor trip in loss of forced RCS flow events, decay heat removal is required. The PRHR HX or the steam generators can be used for decay heat removal. In the event of a complete loss of forced RCS flow, RCS natural circulation is adequate to remove core decay heat. This is demonstrated by the loss of ac power analysis presented in Subsection 15.2.6.

19E.4.4.2 Reactor Coolant Pump Shaft Seizure or Break

An RCP shaft seizure or break results in a partial loss of forced RCS flow. The results are similar to partial loss of flow events discussed in Subsection 19E.4.4.2 of this appendix except that the rate of flow reduction is much more rapid if an RCP shaft breaks or seizes. Like the partial loss of flow, a locked or broken RCP shaft reduces the heat removal rate from the primary to secondary coolant system and thereby causes a heatup of the RCS. An occurrence at full power produces the most severe heatup transient. The discussion for the partial loss of flow with respect to limiting modes and protection is applicable to the RCP shaft seizures or breaks.

Analyses and evaluation of RCP shaft seizures and breaks for Mode 1, from full-power conditions, are provided in Subsections 15.3.3 and 15.3.4. The analyses bound events initiated from the shutdown modes.

19E.4.5 Reactivity and Power Distribution Anomalies

19E.4.5.1 Uncontrolled RCCA Bank Withdrawal from a Subcritical Condition

An uncontrolled RCCA bank withdrawal from a subcritical condition could cause a reactivity excursion, which if not terminated by a reactor trip, could result in DNB. Subsection 15.4.2 presents an analysis for the uncontrolled RCCA bank withdrawal from a subcritical condition in Mode 2. Assumptions are used that make the analysis bound an occurrence in Modes 2, 3, 4, or 5. Specific conservative assumptions are made for the number of RCPs operating, the reactor trip functions credited, initial RCS temperature, and the magnitude of the reactivity excursion.

A single failure in the rod control system could cause the withdrawal of only one bank, and its withdrawal rate would be expected to be slower than the maximum rod speed possible when in automatic rod control. The analysis assumes the simultaneous withdrawal of the combination of two sequential RCCA banks having the greatest combined worth at the maximum possible speed.

LCO 3.3.1 of the AP1000 Technical Specifications gives the operational requirements for reactor trips. The source-range high neutron flux trip must be in operation in Modes 3, 4, and 5 if the reactor trip breakers are closed. If the reactor trip breakers are open, then an RCCA withdrawal is precluded from occurring. The source-range high neutron flux trip is available in Mode 2 if power is below the P-6 interlock. In these instances, the source-range high neutron flux trip would be available to terminate the event, by tripping any withdrawn and withdrawing rods, before any significant power level could be attained. Therefore, DNB would be precluded. The intermediate-range high neutron flux reactor trip is also available in Mode 2. The analysis assumes that reactor trip does not occur until the power-range (low setting) high neutron flux setpoint is reached. No credit is assumed in the analysis for the source-range high neutron flux reactor trip or the intermediate-range high neutron flux reactor trip.

LCOs 3.4.4 and 3.4.5 of the AP1000 Technical Specifications give the operation requirements for RCPs. LCO 3.4.4 specifies that all four RCPs must be operating whenever the reactor trip breakers are closed in Modes 1 through 5.

The RCS temperature is assumed to be at the HZP value in the analysis. This is more limiting than that of a lower initial system temperature for DNB and core kinetics feedback calculations.

These conservative assumptions result in the core returning to critical and generating power before reactor trip occurs. The analysis presented in Chapter 15 bounds the inadvertent RCCA bank withdrawal from a subcritical condition transient in Modes 2 through 5.

19E.4.5.2 Uncontrolled RCCA Bank Withdrawal at Power

This transient is defined only in Mode 1.

19E.4.5.3 RCCA Misalignment

RCCA misalignment events are analyzed in Subsection 15.4.3. RCCA misalignment events include the following:

- One or more dropped RCCAs
- Statically misaligned RCCA
- Withdrawal of a single RCCA

This group of events may result in core radial power distribution perturbations, which may cause allowable design power peaking factors and DNB design limits to be exceeded. Therefore, these events are a concern only in the at-power modes, and the severity will be increased at high power. If the reactor is subcritical, DNB will not be a concern.

Following the dropping of one or more RCCAs while at-power, core power will immediately be reduced. The reduced core power and the continued steam demand to the turbine causes a reactor coolant temperature decrease. If the reactor is in manual control, the core power rises due to moderator feedback to the initial power level at a reduced core inlet temperature. If the reactor is in automatic control, the control system detects the drop in power and initiates withdrawal of a control bank. Power overshoot above the initial power level may occur as the control system withdraws a bank. Following dropping of one or more RCCAs, the most severe results occur when the control system overshoots the initial power level in conjunction with a perturbation in the radial power distribution. This is the most limiting case for this event, and the results are presented in Chapter 15. If the reactor is in any of the subcritical modes, dropping RCCAs will not result in any power transient.

As in the case of dropped RCCAs, statically misaligned RCCAs have no effect in the absence of a critical neutron flux and are not a concern below Mode 2. The most limiting case, and analysis, is for Mode 1 which also bounds Mode 2 operation.

The most limiting case for the withdrawal of a single RCCA is an occurrence while in Mode 1. An occurrence in any of the subcritical modes will have no effect. The shutdown margin requirements are specified in LCO 3.1.1 of the AP1000 Technical Specifications. The shutdown margin requirements are determined assuming the most reactive RCCA is fully withdrawn from the core. Therefore, no single RCCA withdrawal initiated from the subcritical modes will insert enough reactivity to attain criticality.

19E.4.5.4 Startup of an Inactive Reactor Coolant Pump at an Incorrect Temperature

This event is precluded from occurring during at-power modes by Technical Specifications. Startup of an inactive RCP while in any of the subcritical modes will have relatively little effect upon core temperature because there will be little or no temperature difference between the loops. Subsection 15.4.4 discusses the consequences of this event for the AP1000.

19E.4.5.5 Chemical and Volume Control System Malfunction That Results in a Decrease in the Boron Concentration in the Reactor Coolant

Boron dilution analyses and evaluations for Modes 1 through 5 are provided in Subsection 15.4.6. In Mode 6, administrative controls isolate the RCS from potential sources of unborated water by locking closed specified valves in the chemical and volume control system (CVS) and thereby preclude an

uncontrolled boron dilution transient. Makeup needed during refueling is supplied from the boric acid tank which contains borated water.

19E.4.5.6 Inadvertent Loading of a Fuel Assembly in an Improper Position

Fuel loading errors – such as inadvertent loading of one or more fuel assemblies into improper positions, having a fuel rod with one or more pellets of the wrong enrichment, or having a fuel assembly with pellets of the wrong enrichment – may result in power shapes in excess of design values. Subsection 15.4.7 presents Mode 1 results for this event which bound the results for operation in Mode 2. This event is meaningful only if the reactor is at-power and, therefore, not applicable in the subcritical Modes of 3 through 6.

19E.4.5.7 RCCA Ejection

Analyses for RCCA ejections in Mode 1 and Mode 2 are presented in Tier 2 Information Subsection 15.4.8. The cases analyzed in Chapter 15 are the most limiting cases. The shutdown margin requirements are specified in LCO 3.1.1 of the AP1000 Technical Specifications. The shutdown margin requirements are determined assuming the most reactive RCCA is fully withdrawn from the core. Therefore, the ejection of a single RCCA initiated from the subcritical modes would not insert enough reactivity to attain criticality.

19E.4.6 Increase in Reactor Coolant Inventory

An increase in RCS inventory could be caused by inadvertent actuation of the CMTs or by malfunctions in the CVS system. Analyses of events that increase the RCS inventory are provided in Section 15.5. Subsection 15.5.1 presents the analysis results for inadvertent actuation of the CMT. Subsection 15.5.2 contains results from the analysis of a CVS malfunction which increases RCS inventory. These events do not present a challenge to core design limits. If unchecked, these events could lead to an overfill of the pressurizer and possible loss of reactor coolant from the system. The increase in pressurizer water volume is slow during these events and is controlled by the injection rate, core decay heat produced, and heat removal rate from the RCS. While the pressurizer safety valves may open, the steam relief from the pressurizer safety valves is low and no serious challenge to the RCS pressure boundary occurs (if the pressurizer does not fill).

The Chapter 15 analyses for these events are performed with the plant initially in Mode 1 at full-power conditions. This results in the maximum amount of stored energy in the plant and in the maximum core decay heat. If the plant was assumed to be at part power, or in the subcritical modes, the amount of stored energy and decay heat will be significantly reduced.

If a spurious “S” signal occurs causing the CMTs to be actuated, the reactor is also tripped and the PRHR HX is also actuated. The CMTs will begin injecting cold, borated fluid into the RCS. The injected fluid expands as it is heated in the RCS by decay heat. The expansion is counteracted by decay heat removal through the PRHR HX. The severity of the expansion is increased with higher decay heat levels.

Malfunctions in the CVS, which add excess inventory to the RCS, are protected against by the inclusion of automatic CVS isolation functions in the PMS. If a safeguards signal has occurred (which also would activate the CMTs), the CVS is automatically isolated if the pressurizer level exceeds the high-1 pressurizer level setpoint. Above the high-1 pressurizer level setpoint, there is a high-2 pressurizer level setpoint, which also isolates the CVS. The high-2 pressurizer level function is not interlocked with the safeguards signal. The high-2 function protects in situations where the reactor is at-power or a safeguards signal has not occurred. The high-2 pressurizer level function is available in Modes 1 through Mode 3 and in Mode 4 when the RNS is not operating. These functions effectively

prevent overfilling of the pressurizer when the CVS acts alone or where CVS interacts to also cause the CMTs to be actuated.

Isolation of CVS on high-2 pressurizer level is available in Modes 1 through 4 until the plant is operating on RNS. There are applications where the RCS may be filled water-solid when the RNS is in operation. In Modes 4, 5, and 6 when the RNS is in operation, low-temperature overpressure protection (LTOP) of the RCS pressure boundary is provided by the RNS relief valve. A discussion of this is provided in Subsection 19E.4.10.1 of this appendix.

19E.4.7 Decrease in Reactor Coolant Inventory

19E.4.7.1 Inadvertent Opening of a Pressurizer Safety Valve or Inadvertent Operation of the Automatic Depressurization System

Subsection 15.6.1 includes analyses and evaluations of the inadvertent opening of a pressurizer safety valve or the inadvertent operation of the automatic depressurization system (ADS).

When analyzed as depressurization events, inadvertent opening of primary side relief valves, if the reactor is at-power, could result in exceeding core design limits, specifically DNB criteria. Violation of DNB criteria is not a realistic concern if the reactor is in any of the subcritical modes. Therefore, these events are analyzed in Mode 1 at the maximum rated power and the analysis performed bounds cases initiated from Mode 2. These events bound events that can occur at shutdown.

The inadvertent ADS is analyzed as a loss-of-coolant accident in Mode 1 to demonstrate acceptance to the limits specified in 10 CFR 50.46. As described in Subsection 15.6.5, this analysis is a “no-break” small-break LOCA calculation. The inadvertent opening of the 4-inch nominal size ADS Stage 1 valves is a situation that minimizes the venting capability of the RCS. Only the ADS valve vent area is available; no additional vent area exists due to a break. This case examines whether sufficient vent area is available to completely depressurize the RCS and achieve injection from the IRWST without core uncovery. The case analyzed at-power bounds the inadvertent ADS during shutdown because the lower decay heat levels at shutdown reduce the challenge to the ADS vent capacity. More limiting loss-of-coolant accidents at shutdown are analyzed as described in Subsection 19E.4.8.

19E.4.7.2 Failure of Small Lines Carrying Primary Coolant Outside Containment

This event is reported in Subsection 15.6.2 as the rupture of a primary coolant sample line; the radiological consequences of this event are analyzed during Mode 1 because the coolant temperature and iodine concentrations bound those that would exist in the other modes. Concerning shutdown risk, the consequences of a sample line break during Modes 2, 3, 4, or 5 are no more severe than if the accident occurs during Mode 1 operation.

19E.4.7.3 Steam Generator Tube Rupture in Lower Modes

The steam generator tube rupture (SGTR) analysis presented in Chapter 15 is the limiting case with respect to offsite doses. The analysis was performed at full power because this results in the maximum offsite dose. The key inputs from the thermal-hydraulic SGTR analysis performed with the LOFTTR2 computer code to the offsite dose analysis are the amount of flashed primary to secondary break flow and the steam released from the faulted steam generator. Both of these will be significantly reduced at lower power levels and in lower modes of operation.

Margin to overfill analyses are not presented in Chapter 15, however an analysis is performed to demonstrate margin to steam generator overfill with no operator actions modeled. This is necessary because the dose analysis does not include consideration of water relief from the ruptured steam generator PORV/MSSV. This margin to steam generator overfill analysis was supported by the

assertion that an analysis with operator actions modeled will also demonstrate margin to overfill. The overfill analysis with no operator actions discussed in Chapter 15 was initiated at full power. WCAP-10698-P-A (Reference 9) indicates that margin to overfill is reduced when the SGTR is initiated at zero power because of the higher initial steam generator secondary liquid inventory. WCAP-10698-P-A concludes that zero power and lower mode SGTR overfill analyses are not limiting, based primarily on more rapid operator responses expected in those conditions. This is discussed further in the Appendices to WCAP-10698-P-A. When operator actions are credited for AP1000 SGTR mitigation, the plant behaves in a manner comparable to a standard Westinghouse PWR and the conclusions of WCAP-10698-P-A apply.

When operator actions are not relied upon and only the AP1000 automatic RCS cooling and depressurization are credited, margin to overfill would still be maintained for SGTR events initiated at lower power levels despite the increased initial steam generator secondary side inventory corresponding to the lower initial power assumption. This is because the automatic protection system actions that prevent overfill are independent of the operator actions. For operating plants, there is a set period of time from the start of the event until the operator can reverse the trend toward filling the steam generator. Therefore, the initial margin to overfill directly impacts the final margin. For the AP1000, the primary cooldown and depressurization occur automatically when the PRHR HX is actuated on a low pressurizer pressure “S” signal or low pressurizer level CMT actuation signal. The primary pressure may still be held up by the CVS, until it is isolated on a high steam generator level signal. For the AP1000, a higher initial steam generator water level results in the CVS flow being terminated earlier.

In lower modes, the PRHR HX actuation is provided only by the low pressurizer level signal. Although this results in delayed cooling and depressurization, margin to steam generator overfill is still maintained. The increase in mass in the secondary side of the ruptured steam generator is directly related to the reduction in pressurizer water level, because (once the CVS is isolated on high steam generator water level) there is no source of makeup to the RCS. The steam generator secondary side can accommodate the amount of fluid initially contained in the pressurizer and still retain a significant amount of margin to steam generator overfill. The PRHR HX will, therefore, be actuated on low pressurizer water level in sufficient time for the PRHR HX to cool and depressurize the primary and terminate break flow before steam generator overfill will occur.

19E.4.8 Loss-of-Coolant Accident Events in Shutdown Modes

The AP1000 DCD presents a spectrum of break sizes of the postulated LOCAs at the full-power operating condition. Other things being equal, the reduction in power to decay heat levels associated with shutdown mode operations will make all LOCA events less limiting than those analyzed at full power and reported in Subsection 15.6.5. However, as the plant proceeds through shutdown modes of operation, various PXS equipment are removed from service at identified points in time. One particularly significant action in the course of taking the AP1000 to cold shutdown, in the elimination of PXS equipment, is the isolation of the accumulators at 1000 psig. This procedural action reduces the capability of the PXS to mitigate LOCAs. For assessing the adequacy of the remaining PXS components to mitigate postulated LOCA events, the limiting double-ended cold-leg guillotine (DECLG) break, analyzed in Chapter 15, is analyzed assuming it occurs immediately after the isolation of the accumulators. The analysis is performed using the AP1000 Large-Break LOCA WCOBRA-TRAC model used for the at-power Design Basis Accident analysis. Only safety-related systems are modeled in the analysis of this event.

Depressurization of the AP1000 primary system during shutdown operations will be performed with the same care taken to avoid the flashing of liquid in the core and upper head that is taken by current operating plants. Prudent plant operation dictates that subcooling margin be retained as pressure is reduced. Therefore, since the AP1000 shutdown operations will be conducted in a prudent,

controlled manner, it is anticipated that the RCS temperature will be near the 420°F lower limit of Mode 3 when the accumulators are isolated.

For these analyses, the plant was assumed to be shut down in Mode 3 at steady-state conditions of 1000 psig and 425°F with the accumulators isolated. An initial pressure of 1000 psig is assumed because this is the highest pressure with the accumulators isolated and a hot-leg temperature of 425°F is the highest expected temperature when the pressure is 1000 psig. The decay heat level is determined at 2.78 hours after reactor shutdown based on the time estimate to cool down the plant from full-power operation to 425°F at a cooldown rate of 50°F per hour. The low pressurizer pressure safeguards signal is also assumed to be disabled because the initial pressure is below the setpoint.

19E.4.8.1 Double-Ended Cold-Leg Guillotine

The DECLG break is analyzed using the WCOBRA/TRAC computer code and the AP1000-specific noding, which is based on the AP600 noding, presented in WCAP-14171, Revision 1 (Reference 10). Table 19E.4.8-1 summarizes the results.

This case models the double-ended rupture of one of the two cold legs in the RCS loop without the PRHR HX at a pressure of 1000 psig just after the accumulators are isolated. Only the core makeup tanks (CMTs) and IRWST are available to deliver PXS flow. This break evaluates the ability of the plant to withstand a large LOCA during shutdown with its conditions and equipment availability. The nominal discharge coefficient (1.0) is modeled. The analysis is performed with 10 CFR 50, Appendix K (Reference 11), required decay heat, and Technical Specification/Core Operating Limits Report maximum peaking factors.

The break is assumed to open instantaneously at 0.0 seconds. The subcooled discharge from the broken cold leg (Figure 19E.4.8-1) causes a rapid RCS depressurization (Figure 19E.4.8-2). In Figure 19E.4.8-1, the positive flow direction is the normal operation direction. The reversal of flow entering the vessel to flow out of the break is shown. Due to high-1 containment pressure, an “S” signal is generated at 2.2 seconds. Following a 2.0-second delay, the isolation valves on the CMT and PRHR HX outlet lines begin to open. The reactor coolant pumps trip at 8.2 seconds. The nominal discharge coefficient of 1.0, identified in full-power LOCA analyses, is assumed.

Within a few seconds, the collapsed liquid level drops within the upper plenum due to voiding (Figure 19E.4.8-3). The downcomer collapsed liquid level (Figure 19E.4.8-4) quickly falls below the elevation of the cold legs; the elevation of the top of the core is 20.47 feet. Because the RCS fluid enthalpy is lower than the full-power value, the RCS depressurization rate is decreased from the Tier 2 Information cases and more of the initial inventory is retained in the reactor vessel.

CMT injection from both tanks replenishes the RCS mass inventory. Injection from the CMTs as the RCS pressure declines terminates the peak cladding temperature (PCT) transient because the stable injection of water from the CMTs exceeds the break flow. The core collapsed level refills are as shown in Figure 19E.4.8-5. The pressure is low enough that the IRWST injection will begin once the CMTs drain to the low-2 level actuation setpoint. The maximum PCT value is approximately 1420°F for this bounding break size as shown in Figure 19E.4.8-6, and all the 10 CFR 50.46 (Reference 16) acceptance criteria are met.

19E.4.8.2 Loss of Normal Residual Heat Removal System Cooling in Mode 4 with Reactor Coolant System Intact

For this analysis, it is assumed that the RNS has just been placed in operation at 4 hours after reactor shutdown with the RCS at 350°F and 450 psig (464.7 psia). It is assumed that a loss of offsite power occurs, resulting in a loss of flow through the RNS, and thus, in a loss of RNS cooling. The MSS is assumed to be unavailable for heat removal although the steam generator secondary side is

assumed to be at saturated conditions for 350°F with the normal water level. Because the Mode 4 plant conditions assumed for the analysis are more limiting than Mode 5 conditions, this analysis is also applicable for a loss of RNS cooling in Mode 5 when the RCS is intact.

It is assumed that both CMTs are available for injection. Although the Technical Specifications permit one CMT to be taken out of service in Mode 4, there is a high probability that both CMTs will be available and, therefore, they were both assumed to operate. If only one CMT is available, the overall results should be similar although the timing of the event will be affected. Even though all of the fourth-stage ADS valves are available in Mode 4, the Technical Specifications permit one of the fourth-stage ADS valves to be out of service in Mode 5 when the RCS is intact. Thus, it was assumed that only three of the fourth-stage ADS valves are available for operation to bound the equipment availability in Mode 5. However, one of the three available fourth-stage ADS valves is assumed to fail to open on demand as the single failure, consistent with the single failure assumption used for the small-break LOCA analyses for shutdown conditions.

Two cases were analyzed. The first allowed for automatic safety system actuation on a low pressurizer level signal late in event. During this time, the only mechanism for removing decay heat is boiling off the RCS inventory and venting through the RNS relief valve. The second calculation assumes operator action 1800 seconds after the loss of RNS cooling.

Automatic Safety Injection Actuation Case

The accident analyzed is a loss of RNS cooling, which is assumed to result in a complete loss of heat removal for the RCS. The sequence of events for this analysis is presented in Table 19E.4.8-2.

Following the loss of RNS cooling, there is no mechanism for heat removal from the RCS. The core decay heat generation causes the reactor coolant temperature and pressure to increase. Although the MSS is assumed to be unavailable for heat removal, the steam generators represent a heat sink that slows the rate of heatup of the reactor coolant. The fluid temperature at the core outlet for the transient is shown in Figure 19E.4.8-7. The reactor coolant heatup causes the system pressure to increase, as shown in Figure 19E.4.8-8, until the pressure reaches the RNS relief valve setpoint of 500 psig (514.7 psia) at approximately 400 seconds. The normal relieving capacity of the RNS relief valve is 850 gpm, and the pressure is maintained at the relief valve setpoint as the temperature continues to increase and reactor coolant is discharged from the relief valve. Flow out the relief valve is shown in Figure 19E.4.8-9. The expansion of the water due to the coolant temperature increase also causes the pressurizer level to increase slightly as shown in Figure 19E.4.8-10.

The loss of reactor coolant through the relief valve is not sufficient to remove the core decay heat, and the reactor coolant temperature continues to increase until the core outlet temperature reaches saturation at the relief valve setpoint at approximately 3200 seconds. The generation of steam in the core causes the system pressure to increase above the RNS relief valve setpoint and the pressurizer level to continue to increase. A mixture level begins to form in the upper plenum at approximately 3800 seconds and drops to the top of the hot-leg elevation as shown in Figure 19E.4.8-11. At about 4100 seconds, enough mass has been discharged such that a mixture level also forms in the downcomer (Figure 19E.4.8-12) and the downcomer two-phase level begins to decrease. As the boiling front moves lower and lower into the core, more steam generation occurs and the pressure continues to increase. Once the entire core length is boiling, the upper plenum mixture level is within the hot-leg perimeter. At approximately 7000 seconds, when steam begins to flow through the relief valve along with liquid, the pressure begins to decrease. The pressurizer level also begins to decrease as water drains from the pressurizer into the reactor coolant system hot leg. However, the voiding in the RCS increases as the pressure decreases, and flashing begins to occur in the pressurizer at approximately 7300 seconds. This additional steam generation causes the pressure to begin to increase, and the relief valve flow becomes solely liquid again. The steam voiding in the pressurizer not only causes the pressure increase, but also facilitates draining, and the pressurizer level continues to decrease.

As the pressurizer level decreases, a CMT actuation signal is generated automatically on low pressurizer level. Following a 1.2-second delay, the isolation valves on the available CMT tank delivery lines open and CMT injection flow is initiated at approximately 7910 seconds as shown in Figure 19E.4.8-13. The opening of the PRHR HX isolation valve on a CMT actuation signal starts the flow through the heat exchanger. The CMT injection causes the reactor coolant pressure to decrease below the RNS relief valve setpoint, and the loss of reactor coolant is terminated at approximately 8100 seconds. As the CMT level decreases (Figure 19E.4.8-14), the first-stage ADS setpoint at 67.5 percent is reached at 9348 seconds. The second-stage and third-stage ADS valves also open following the timer delays for the actuation of the second-stage and third-stage ADS valves. The vapor and liquid flow through the ADS valves (Figures 19E.4.8-15 and 19E.4.8-16) results in a rapid depressurization of the reactor coolant system. The CMT reaches the fourth-stage ADS setpoint of 20 percent, and two of the four fourth-stage paths open at 10,225 seconds. As noted previously, it is assumed that one of the fourth-stage paths is out of service and one path is assumed to fail as the single active failure. The vapor and liquid flow through the fourth-stage ADS paths (Figures 19E.4.8-17 and 19E.4.8-18) further reduces the pressure to the point where IRWST injection begins at approximately 10,700 seconds (Figure 19E.4.8-19).

The CMT and IRWST injection reverses the decrease in the core stack and downcomer mixture levels as shown in Figures 19E.4.8-11 and 19E.4.8-12, respectively. As shown in Figure 19E.4.8-11, the core stack mixture level is maintained above the elevation of the top of the core active fuel (20.34 feet) throughout the transient. At the end of the transient, the core stack mixture level has been restored to within the hot-leg perimeter and the downcomer mixture level has been restored to the DVI nozzle elevation. The fluid temperature at the core outlet has also been reduced and is being maintained at less than 250ºF. As shown in Figure 19E.4.8-20, the reactor coolant mass inventory twice reaches a minimum of approximately 110,000 pounds when the CMT and IRWST injection then increase the inventory. The reactor coolant mass inventory is greater than 200,000 pounds and is slowly increasing at the end of the transient. Thus, it is concluded that the consequences of a loss of RNS in Modes 4 and 5 with the RCS intact are acceptable.

Manual Safety Actuation

If operator action occurs after 1800 seconds, the CMT and PRHR isolation valves would open. Initially, the decay heat is greater than the PRHR capacity and the RCS pressure increases to the RNS safety valve setpoint (Figure 19E.4.8-21). At this time, RCS inventory is vented through the valve (Figure 19E.4.8-22). Eventually, the decay heat matches the PRHR capacity (Figure 19E.4.8-42) and the RCS pressure decreases slowly to the valve setpoint. For this case, the ADS is not actuated. The sequence of events for this case is also shown in Table 19E.4.8-2.

19E.4.8.3 Loss of Normal Residual Heat Removal System Cooling in Mode 5 with Reactor Coolant System Open

For this analysis, it is assumed that the RNS is in operation in Mode 5 at 24 hours after reactor shutdown with the ADS Stage 1, 2, and 3 valves open and the RCS vented to the IRWST. The reactor coolant temperature is assumed to be at 160°F, and the pressurizer pressure is assumed to be at atmospheric pressure plus the elevation head in the IRWST, or 18.2 psia. The steam generator secondary side is assumed to be drained, and thus, there is no secondary heat sink for this case. It is assumed that the CMTs and the PRHR are not available because the Technical Specifications permit them to be taken out of service when the RCS is open in Mode 5. It is also assumed that only two of the fourth-stage ADS valves are available for potential use by the operators because the Technical Specifications permit two of the fourth-stage ADS valves to be out of service in Mode 5 when the RCS is open. In addition, one of the two available fourth-stage ADS valves is assumed to fail to open on demand as the single failure. The Technical Specifications also permit one of the two IRWST injection paths to be out of service in Mode 5 with the RCS open, and thus, only one of the IRWST injection paths is assumed to be available.

It is assumed that a loss of offsite power occurs, resulting in a loss of RNS flow, and thus a loss of RNS cooling. The sequence of events for this analysis is presented in Table 19E.4.8-3.

Following the loss of RNS cooling, there is no mechanism for heat removal from the RCS and the core decay heat generation results in an increase in the reactor coolant temperature. The fluid temperature at the core outlet for the transient is shown in Figure 19E.4.8-24. The core outlet fluid temperature increases steadily until approximately 3000 seconds when saturation temperature is reached and voiding is initiated in the core. Because the RCS is vented to the IRWST via ADS Stages 1, 2, and 3, the pressure initially remains constant until approximately 3200 seconds as shown in Figure 19E.4.8-25. As the void generation in the system increases, the vapor flow through ADS Stages 1, 2, and 3 is not sufficient to maintain the pressure. The pressure increases to approximately 44.0 psia, and then begins to decrease. As shown in Figure 19E.4.8-26, the pressurizer level also increases as the reactor coolant temperature increases. The level subsequently reaches the top of the pressurizer as a result of the steam generation in the system. As shown in Figures 19E.4.8-27 and 19E.4.8-28, a mixture of steam and water is discharged via ADS Stages 1, 2, and 3 after the pressurizer fills.

The continued loss of reactor coolant through ADS Stages 1, 2, and 3 causes the pressure to begin to decrease after approximately 4600 seconds. The core outlet temperature is at saturation and also begins to decrease as the pressure decreases. A mixture level begins to form in the upper plenum at approximately 3550 seconds, and the level begins to decrease, as shown in Figure 19E.4.8-29, as the voiding continues in the system. At about 4050 seconds, enough mass has been discharged that a mixture level forms in the downcomer (Figure 19E.4.8-30) and the downcomer level also begins to decrease. The pressurizer level does not decrease significantly due an increasing void fraction in the pressurizer.

As the voiding in the core continues, the core stack mixture level continues to decrease as shown in Figure 19E.4.8-29. The void fraction in the hot legs also increases, and the mixture level in the hot leg begins to decrease after 3250 seconds. The hot leg is empty at approximately 4800 seconds as shown in Figure 19E.4.8-31. This is the normal signal for opening the fourth-stage ADS valves and to initiate IRWST injection when the systems are aligned for automatic actuation. Thus, it is assumed that the operator will initiate manual action at 4800 seconds to open the fourth-stage ADS valves and to open the IRWST flow path to permit IRWST injection when the downcomer pressure is sufficiently low. Discharge through one of the fourth-stage ADS valves is initiated at 4890 seconds as shown in Figures 19E.4.8-32 and 19E.4.8-33. As noted previously, one of the two available fourth-stage ADS paths is assumed to fail to open as the single active failure. The flow through the fourth-stage ADS path results in a further reduction in the pressurizer pressure and a rapid decrease in the pressurizer level. The downcomer pressure is also reduced to the point where IRWST injection is initiated at approximately 5500 seconds (Figure 19E.4.8-34). However, the pressurizer level increases due to subsequent additional void formation at the lower pressure and the downcomer pressure increases slightly. This temporarily terminates the IRWST flow. The downcomer pressure then drops slowly, resulting in sustained IRWST injection.

The IRWST injection reverses the decrease in the core stack and downcomer mixture levels as shown in Figures 19E.4.8-30 and 19E.4.8-31, respectively. As shown in Figure 19E.4.8-30, the core stack mixture level is maintained well above the elevation of the top of the core active fuel (20.43 feet) throughout the transient. At the end of the transient, the core stack mixture level has been restored to above the middle of the hot-leg elevation and the downcomer mixture level is above the DVI nozzle elevation. The fluid temperature at the core outlet has also been reduced to approximately 250°F. As shown in Figure 19E.4.8-35, the reactor coolant mass inventory reaches a minimum of approximately 135,000 pounds and then begins to increase as a result of the IRWST injection. Thus, it is concluded that when the appropriate operator action is performed, one ADS Stage 4 valve is effective in reducing system pressure so that the consequences of a loss of RNS in Mode 5 with the RCS vented are acceptable.

The analysis presented here is a conservative analysis of a loss of RNS cooling during reduced inventory conditions. During Mode 5, prior to draining to mid-loop conditions, the operator manually opens the ADS Stages 1 through 3 paths to the IRWST. With the RCS "open," the operator then proceeds to slowly drain the RCS to "mid-loop" conditions for performing steam generator maintenance or other maintenance that requires a reduced RCS water level. At this moment, it is postulated that a loss of decay heat removal via the nonsafety-related RNS occurs. A loss of RNS cooling at this time is selected because it is the earliest time the RCS could be placed into a reduced inventory (that is, RCS open) condition. In addition, the backpressure on the reactor vessel, due to the presence of water in the pressurizer, is higher at this time. This presents the most challenging condition for the ADS to depressurize the RCS to IRWST cut-in pressure. This transient represents the most limiting "surge line flooding" scenario, a term commonly used for operating plants to refer to the phenomenon associated with water in the pressurizer and surge line causing a high backpressure in the RCS. This potentially challenges the ability of the low head safety injection systems to inject properly. In addition, this scenario can potentially challenge the design pressure of temporary nozzle dams placed in the steam generators to facilitate maintenance of the RCS during refueling.

For a loss of the RNS during mid-loop operations, calculations have been performed to determine the time until core uncovery would occur. The results of these calculations are presented in Table 19E.2-1. The progression of events following a loss of RNS cooling during mid-loop results in a heatup of the RCS to saturation, followed by a boiling off of the coolant to the IRWST via the ADS Stages 1, 2, and 3 valves. Eventually, the operator actuates the IRWST upon a loss of RCS subcooling, followed by the loss of RCS inventory. The conditions in the RCS following IRWST and fourth-stage ADS actuation are similar to those in this evaluation. As shown in Table 19E.2-1, the operator has at least 100 minutes from the loss of RNS cooling until the onset of core uncovery to manually actuate the IRWST and ADS Stage 4. In general, the results of a loss of RNS during mid-loop conditions are similar, but slightly less severe to those presented in this evaluation due to the lower levels of decay heat and to the absence of the initial water inventory in the pressurizer. This serves to reduce the surge line flooding phenomenon that degrades the depressurization capability of the ADS Stages 1 through 3 vent paths.

19E.4.9 Radiological Consequences

This section presents evaluations that confirm that the radioactive material releases from the AP600 events postulated to be initiated in a shutdown mode have acceptable consequences.

- The Standard Review Plan (Reference 12) no longer includes the atmospheric releases from radioactive gas waste system failure and radioactive liquid waste system leak or failure events as part of the review. As discussed in Subsections 15.7.1 and 15.7.2, no analysis for these events is provided.

- Release of radioactivity to the environment due to a liquid tank failure is addressed in Subsection 15.7.3 and is not mode dependent.

- The fuel handling accident described in Subsection 15.7.4, while not mode dependent, is analyzed in the applicable and bounding mode and accounts for spent fuel pool boiling. This accident analysis bounds radioactivity releases from other Chapter 15 events during low power and shutdown operations. The LOCA analysis results show PCT remains below 2200°F, and there are no fuel cladding failures.

- The spent fuel cask drop accident described in Subsection 15.7.5 is not mode dependent.

- Appendix 15A contains the evaluation models and parameters that form the basis of the radiological consequences analyses for the various postulated accidents. This methodology applies in all modes of operation.

In summary, there are no shutdown risks associated with the radiological consequences methodology or parameters, or the postulated or applicable events, which need to be considered outside the scope of what is already analyzed for Section 15.7.

19E.4.10 Other Evaluations and Analyses

19E.4.10.1 Low Temperature Overpressure Protection

For the AP1000, the normal residual heat removal system (RNS) suction relief valve is located immediately downstream of the RCS suction isolation valves. This relief valve protects the RNS from overpressurization and provides low temperature overpressure protection (LTOP) for the RCS components when the RNS is aligned to the RCS to provide decay heat removal during plant shutdown and startup operations. The RNS relief valve is sized to provide LTOP by limiting the RCS and RNS pressure to less than the 10 CFR 50 Appendix G (Reference 13) steady-state pressure limit. Subsection 5.2.2 provides a discussion of the AP1000 low temperature overpressure protection design bases.

19E.4.10.2 Shutdown Temperature Evaluation

In SECY-94-084, Item C, Safe Shutdown (Reference 14), the NRC staff recommended the Commission's approval of 420°F or below, rather than cold shutdown condition as a safe stable condition, which the PRHR HX must be capable of achieving and maintaining following non-LOCA events, predicated on acceptable passive safety system performance and an acceptable resolution of the regulatory treatment of nonsafety systems (RTNSS) issue. The NRC requested a safety analysis to demonstrate that the passive systems can bring the plant to a stable safe condition and maintain this condition so that no transients will result in the specified acceptable fuel design limit and pressure boundary design limit being violated and that no high-energy piping failure being initiated from this condition results in 10 CFR 50.46 (Reference 15) criteria.

As discussed in Subsection 7.4.1.1, the PRHR HX operates to reduce the RCS temperature to the safe shutdown condition following an event. An analysis of the loss of ac power event demonstrates that the passive systems can bring the plant to a stable safe condition following postulated transients. The results of this analysis are presented in Figures 19E.4.10-1 through 19E.4.10-4 The progression of this event is outlined in Table 19E.4.10-1.

Summarizing this transient, the loss of normal ac power occurs, followed by the reactor trip. The PRHR heat exchanger is actuated on the low steam generator narrow range level coincident with low startup feed water flow rate signal. Eventually a safeguards actuation signal is actuated on Low cold leg temperature and the CMTs are actuated.

Once actuated, at about 600 seconds, the CMTs operate in recirculation mode, injecting cold borated water into the RCS. In the first part of their operation, due to the cold flow rate, the CMTs operate in conjunction with the PRHR to reduce RCS temperature. Due to the primary system cooldown, the PRHR heat transfer capability drops below the decay heat and the RCS cooldown is essentially driven by the CMT cold injection flow. However, at about 3,500 seconds, the CMT cooling effect decreases and the RCS starts heating up again (Figure 19E.4.10-1). The RCS temperature increases until the PRHR HX can match decay heat. At about 31,000 seconds, the PRHR heat transfer matches decay heat and it continues to operate to reduce the RCS temperature to below 420°F within 36 hours. As seen from Figure 19E.4.10-1 the cold leg temperature in the loop with the

PRHR is reduced to 420°F at 82,600 seconds, while the core average temperature reaches 420°F in 123,600 seconds (approximately 34 hours).

As discussed in Subsection 7.4.1.1, this mode of operation can last for up to 72 hours. However, in about 22 hours after the event, if no ac power is available, or if condensate return is not available, then the operator is instructed to actuate the ADS. Operation of the ADS in conjunction with the CMTs, accumulators, and IRWST reduces the RCS pressure and temperature to below 420°F.

19E.5 Technical Specifications

While the Technical Specification guidance provided in NUREG-1449 (Reference 2) relates to existing plant shutdown operation concerns, the underlying concerns relating to causes of events and recovery from those events during shutdown operations are applicable to the AP1000. Subsection 19E.5.1 summarizes the shutdown Technical Specifications. Subsection 19E.5.2 summarizes the AP1000's compliance with SECY-93-190 (Reference 16).

19E.5.1 Summary of Shutdown Technical Specifications

The content of the AP1000 Technical Specifications meets the requirements of 10 CFR 50.36 (Reference 17) and is consistent with the guidance provided in NUREG-1431 (Reference 18). For the AP1000, passive systems are used to safely shut down the plant. Because this design feature is different from existing plants, and because NUREG-1449 provides a reasonable basis for creating shutdown Technical Specifications, the AP1000 Technical Specifications are improved to include specifications for these systems in the shutdown modes. These shutdown specifications are summarized in AP1000 Technical Specification Table B 3.0-1 (Section 16.1), which provides the passive systems shutdown mode matrix of system versus limiting conditions for operation (LCO), mode applicability, and required end state.

19E.6 Shutdown Risk Evaluation

The "AP1000 Probabilistic Risk Assessment (PRA)" (Chapter 19) provides an assessment of the plant risk associated with events at shutdown.

19E.7 Compliance with NUREG-1449

The Diablo Canyon event of April 10, 1987, and the loss of ac power event at the Vogtle plant on March 20, 1990, led the Nuclear Regulatory Commission (NRC) staff to issue NUREG-1449, "Shutdown and Low Power Operation at Commercial Nuclear Power Plants in the United States" (Reference 2), to provide an evaluation of the shutdown risk issue. The scope of NUREG-1449 includes subjects such as operating experiences as documented in generic letters, operator training, technical specifications, residual heat removal capacity, temporary reactor coolant boundaries, rapid boron dilution, containment capacity, fire protection, outage planning and control, and instrumentation.

The NRC requested Westinghouse to assess the compliance of AP600 with NUREG-1449. It was recognized that some of the issues discussed in NUREG-1449 are the responsibility of the plant owners because they relate to operation, maintenance, and refueling plans, procedures, and risk management. However, the NRC believed that the level of defense-in-depth against shutdown events would be improved if clear guidance is provided to the areas discussed above by the plant designer. The NRC requested that Westinghouse perform a systematic assessment of the shutdown risk issue to address areas identified in NUREG-1449 as they are applicable to the AP1000 design and document the results.

This Appendix provides the systematic assessment of the shutdown risk issue to address areas identified in NUREG-1449. This assessment includes design basis evaluations of events that can occur during shutdown and a probabilistic assessment of plant risk at shutdown. The design of the AP1000 builds on the lessons-learned from the industry with regard to shutdown safety, including the guidance provided in NUREG-1449.

19E.8 Conclusion

This AP1000 Shutdown Evaluation provides a systematic evaluation of the AP1000 during shutdown operations. As demonstrated in this appendix, the AP1000 is designed to mitigate events that can occur during shutdown modes. In addition, the risk of core damage as a result of an accident that may occur during shutdown has been demonstrated to be acceptably low.

19E.9 References

1. Letter, Westinghouse to NRC, DCP/NRC1385, AP600 Emergency Response Guidelines.

2. NUREG-1449, “Shutdown and Low Power Operations at Commercial Nuclear Power Plants in the United States,” September 1993.

3. NRC Information Notice 92-54, “Level Instrumentation Inaccuracies Caused by Rapid Depressurization,” July 24, 1992.

4. Letter, Westinghouse to NRC, DCP/NRC0124, APWR-0452, “AP600 Vortex Mitigator Development Test for RCS Mid-loop Operation,” July 6, 1994.

5. NUREG-0897, Rev. 1, “Containment Emergency Sump Performance,” October 1985.

6. Title 10, Code of Federal Regulations, Part 50, Appendix B, “Quality Assurance Criteria for Nuclear Power Plants and Fuel Processing Plants.”

7. NRC Regulatory Guide 1.26, “Quality Group Classifications and Standards for Water-, Steam-, and Radioactive-Waste-Containing Components of Nuclear Power Plants,” Revision 3, February 1976.

8. American Society of Mechanical Engineers Boiler and Pressure Vessel Code, Section III, 1988 with 1989 Addenda.

9. Lewis, R. N., Huang, P., Behnke, D. H., Fittante, R. L., and Gelman, A., WCAP-10698-P-A (Proprietary) and WCAP-10750-A (Non-Proprietary), “SGTR Analysis Methodology to Determine the Margin to Steam Generator Overfill,” August 1987.

10. WCAP-14171, Revision 2 (Proprietary) and WCAP-14172, Revision 2 (Non-Proprietary), “WCOBRA/TRAC Applicability to AP600 Large-Break Loss-of-Coolant Accident,” March 1998.

11. Title 10, Code of Federal Regulations, Part 50, Appendix K, “ECCS Evaluation Model.”

12. NUREG-0800, “Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants,” Revision 1, July 1981.

13. Title 10, Code of Federal Regulations, Part 50, Appendix G, “Fracture Toughness Requirements.”

14. SECY-94-084, “Policy and Technical Issues Associated with the Regulatory Treatment of Non-Safety Systems in Passive Plant Designs,” March 28, 1994.

15. Title 10, Code of Federal Regulations, Part 50, (10 CFR 50.46).

16. NRC letter, SECY-93-190, “Regulatory Approach to Shutdown and Low-Power Operations,” July 12, 1993.

17. Title 10, Code of Federal Regulations, Part 50.36, “Technical Specifications.”

18. NUREG-1431, “Standard Technical Specifications – Westinghouse Plants,” April 1995.

Table 19E.2-1
Evaluation of a Loss of RNS at Mid-Loop With no IRWST Injection

Time After Shutdown	Time to Boiling	Time to Empty Hot Leg	Time to Core Uncovery
28 hours	10 minutes	22 minutes	40 minutes

Table 19E.4.1-1 (Sheet 1 of 2)
AP1000 Accidents Requiring Shutdown Evaluation or Analysis

Tier 2 Section	Titles	Evaluation or Analysis Required
15.1	Increase in Heat Removal from the Primary System	
15.1.1	Feedwater System Malfunctions that Result in a Decrease in Feedwater Temperature	E
15.1.2	Feedwater System Malfunctions that Result in an Increase in Feedwater Flow	E
15.1.3	Excessive Increase in Secondary Steam Flow	E
15.1.4	Inadvertent Opening of a Steam Generator Relief or Safety Valve	E
15.1.5	Steam System Piping Failure	E
15.1.6	Inadvertent Operation of the Passive Residual Heat Removal Heat Exchanger	E
15.2	Decrease in Heat Removal by the Secondary System	
15.2.1	Steam Pressure Regulator Malfunction or Failure that Results in Decreasing Steam Flow	E
15.2.2	Loss of External Electrical Load	E
15.2.3	Turbine Trip	E
15.2.4	Inadvertent Closure of Main Steam Isolation Valves	E
15.2.5	Loss of Condenser Vacuum and Other Events Resulting in Turbine Trip	E
15.2.6	Loss of ac Power to the Plant Auxiliaries	E
15.2.7	Loss of Normal Feedwater Flow	E
15.2.8	Feedwater System Pipe Break	E
15.3	Decrease in Reactor Coolant System Flow Rate	
15.3.1	Partial Loss of Forced Reactor Coolant Flow	E
15.3.2	Complete Loss of Forced Reactor Coolant Flow	E
15.3.3	Reactor Coolant Pump Shaft Seizure (Locked Rotor)	E
15.3.4	Reactor Coolant Pump Shaft Break	E
15.4	Reactivity and Power Distribution Anomalies	
15.4.1	Uncontrolled Rod Cluster Control Assembly Bank Withdrawal from a Subcritical or Low-Power Startup Condition	E
15.4.2	Uncontrolled Rod Cluster Control Assembly Bank Withdrawal at Power	n/a
15.4.3	Rod Cluster Control Assembly Misalignment (System Malfunction or Operator Error)	E
15.4.4	Startup of an Inactive Reactor Coolant Pump at an Incorrect Temperature	E

Table 19E.4.1-1 (Sheet 2 of 2)
AP1000 Accidents Requiring Shutdown Evaluation or Analysis

Tier 2 Section	Titles	Evaluation or Analysis Required
15.4.6	Chemical and Volume Control System Malfunction That Results in a Decrease in the Boron Concentration in the Reactor Coolant	n/a
15.4.7	Inadvertent Loading and Operation of a Fuel Assembly in an Improper Position	E
15.4.8	Spectrum of Rod Cluster Control Assembly Ejection Accidents	
15.5	Increase in Reactor Coolant Inventory	
15.5.1	Inadvertent Operation of the Core Makeup Tanks (CMT) During Power Operation	E
15.5.2	Chemical and Volume Control System Malfunction That Increases Reactor Coolant Inventory	E
15.6	Decrease in Reactor Coolant Inventory	
15.6.1	Inadvertent Opening of a Pressurizer Safety Valve or Inadvertent Operation of the ADS	E
15.6.2	Failure of Small Lines Carrying Primary Coolant Outside Containment	E
15.6.3	Steam Generator Tube Rupture	E
15.6.5	Loss of Coolant Accidents Resulting from a Spectrum of Postulated Piping Breaks Within the Reactor Coolant Pressure Boundary	E/A
15.7	Radioactive Release From a Subsystem or Component	E

Table 19E.4.8-1
Double-Ended Cold-Leg Guillotine Break – Sequence of Events

Event	Time (seconds)
Break open	0.0
“S” signal receipt	4.2
RCPs start to coast down	8.2
CMT draindown begins	5
Lower plenum refilled	200

Table 19E.4.8-2
Loss of Normal Residual Heat Removal System Cooling in Mode 4 With Reactor Coolant System Intact – Sequence Of Events

Event	Automatic Actuation Time (seconds)	Manual Actuation Time (seconds)
Loss of RNS cooling	0	0
RNS relief valve flow starts	250	250
CMT and PRHR actuated	7910	1800
RNS relief valve flow terminated	8100	<1 lbm/s @ 25,000
ADS Stage 1 flow starts	9348	–
ADS Stage 2 flow starts	9418	–
ADS Stage 3 flow starts	9538	–
ADS Stage 4 flow starts	10,225	–
IRWST injection starts	10,700	–

Table 19E.4.8-3
Loss of Normal Residual Heat Removal System Cooling in Mode 5 With Reactor Coolant System Open – Sequence Of Events

Event	Time (seconds)
Loss of RNS cooling	0
Hot leg empty	4800
ADS Stage 4 flow initiated	4890
IRWST injection starts	5500

Tables 19E.4.8-4 and 19E.4.8-5 not used.

Table 19E.4.10-1
Sequence of Events Following a Loss of ac Power Flow with Condensate from the Containment Shell Being Returned to the IRWST

Event	Time (seconds)
Feedwater is Lost	10.0
Low Steam Generator Water Level (Narrow-Range) Reactor Trip Setpoint Reached	72.4
Rods Begin to Drop	74.4
PRHR HX Actuation on Low Steam Generator Water Level (Wide-Range)	129.4
Low T_{cold} Setpoint Reached	599.0
Steam Line Isolation on Low T_{cold} Signal	611.0
CMTs Actuated on Low T_{cold} Signal	617.0
IRWST Reaches Saturation Temperature	17,600
Heat Extracted by PRHR HX Matches Core Decay Heat	31,000
CMTs Stop Recirculating	43,500
Cold Leg Temperature Reaches 420°F (loop with PRHR)	82,600
Hot Leg Temperature Reaches 420°F (loop with PRHR)	123,600

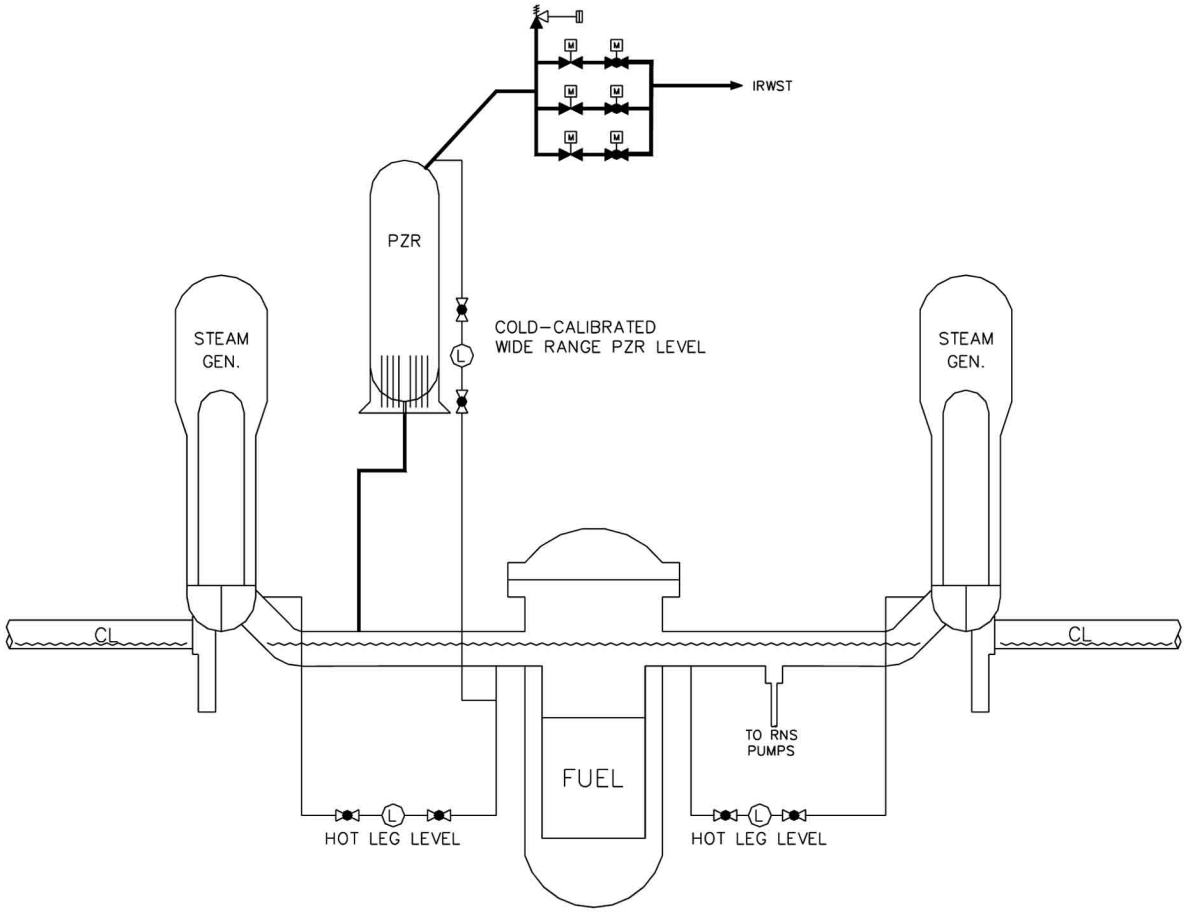

Figure 19E.2-1 Reactor Coolant System Level Instruments Used During Shutdown

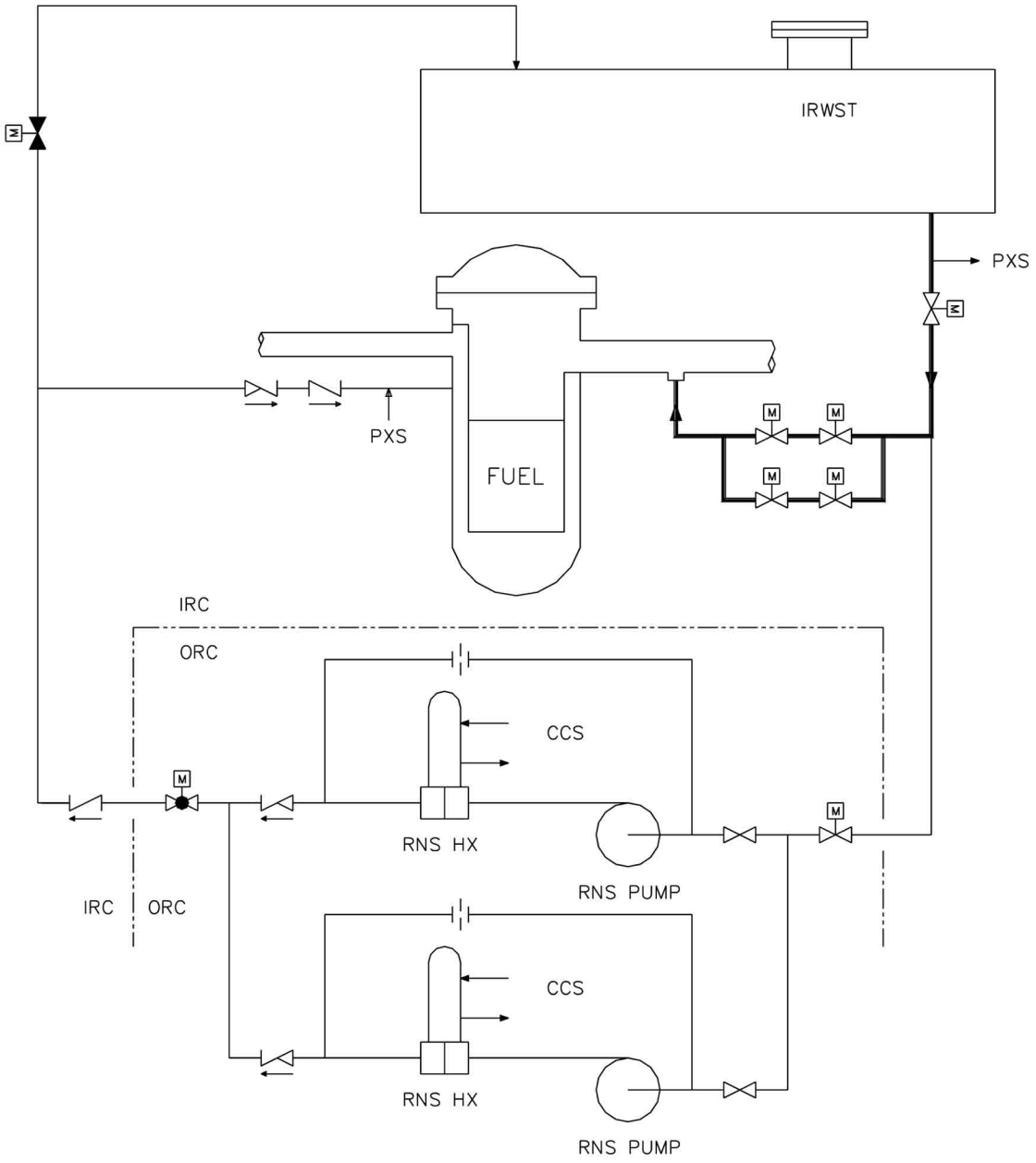

Figure 19E.9-1 IRWST Injection Flow Path

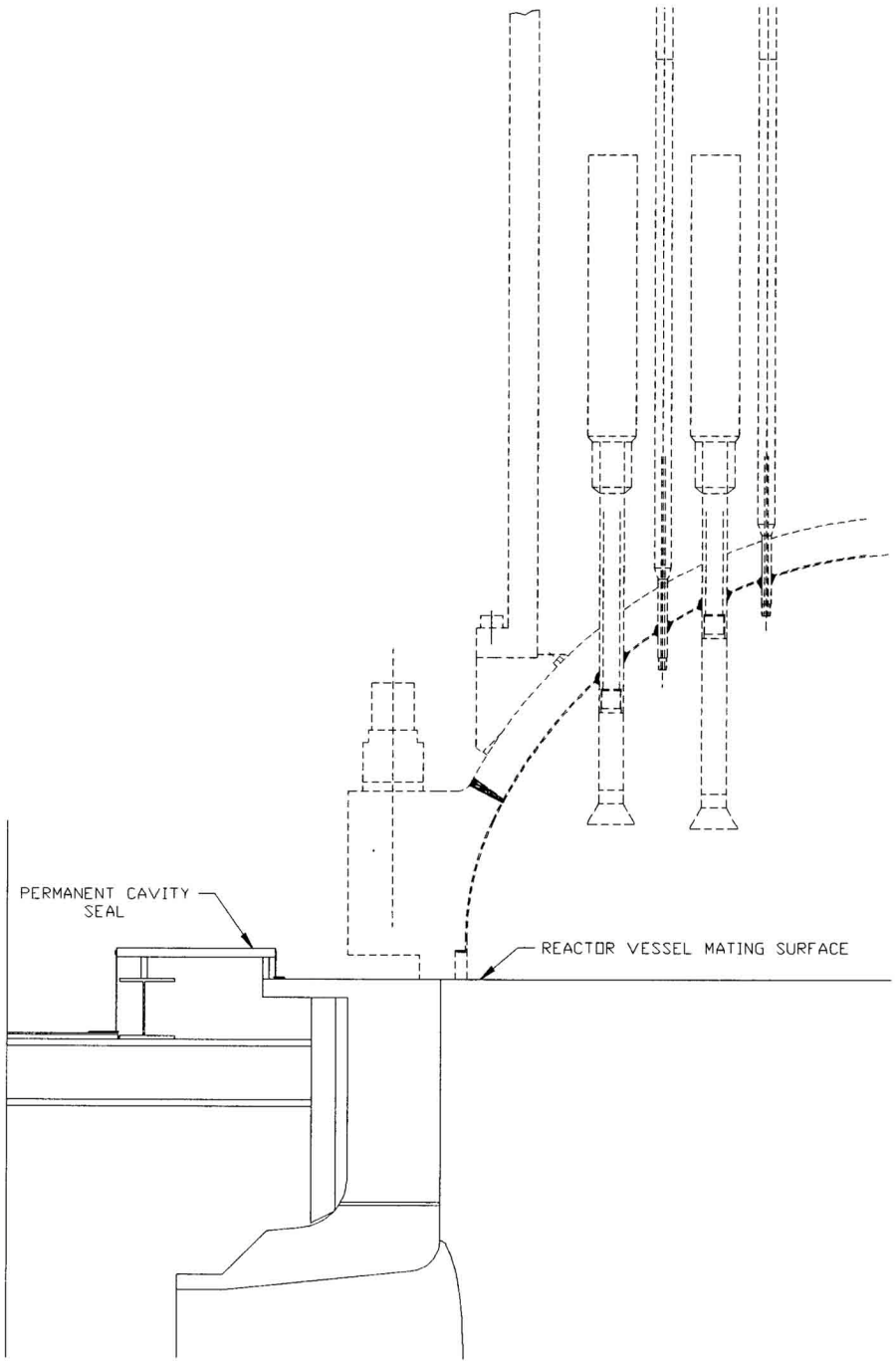

Figure 19E.9-2 AP1000 Permanent Reactor Cavity Seal

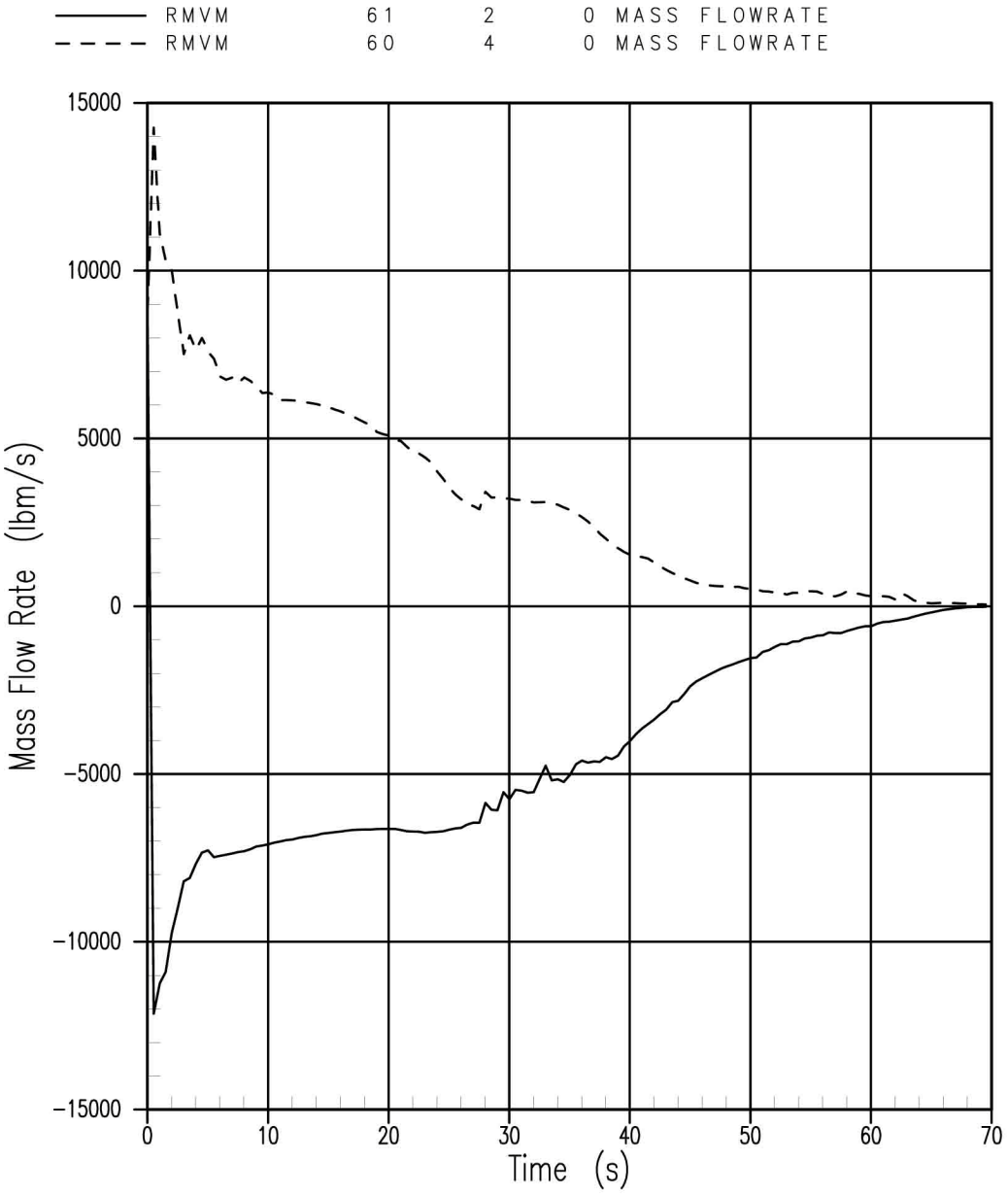

Figure 19E.4.8-1 Mode 3 DECLG Break, Break Flow Rates, Vessel and RCP Sides

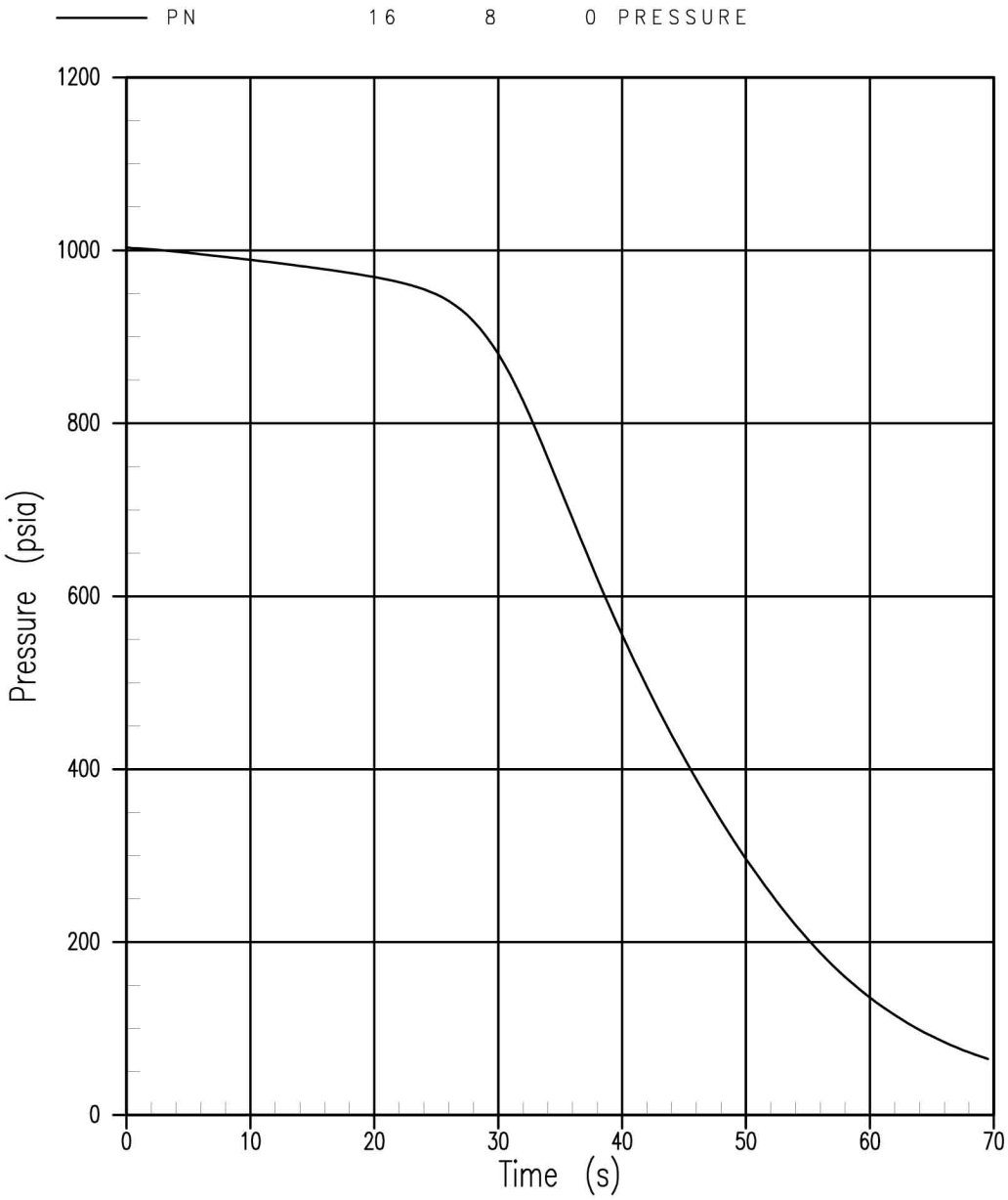

Figure 19E.4.8-2 Mode 3 DECLG Break, Pressurizer Pressure

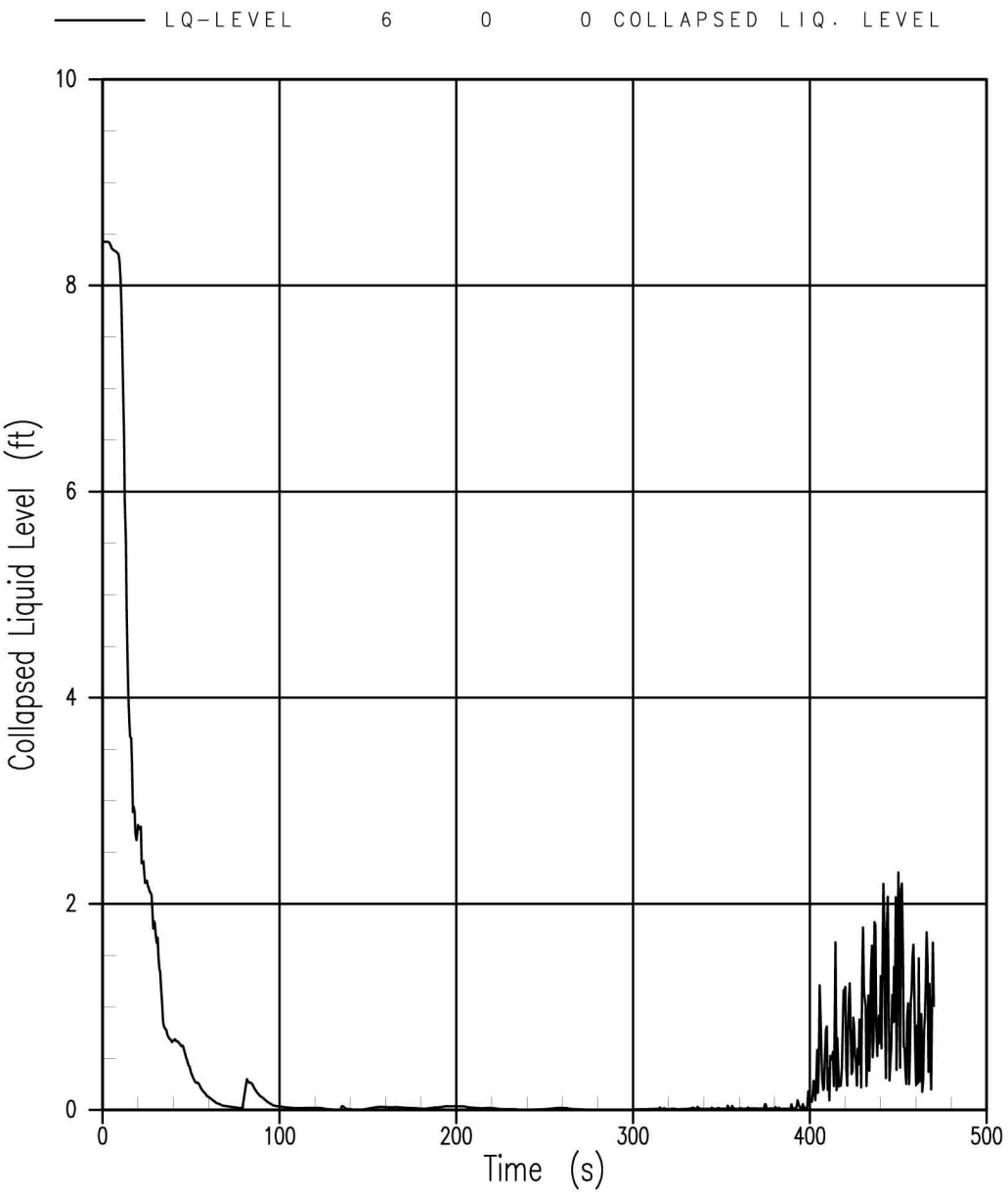

Figure 19E.4.8-3 Mode 3 DECLG Break, Upper Plenum Collapsed Liquid Level

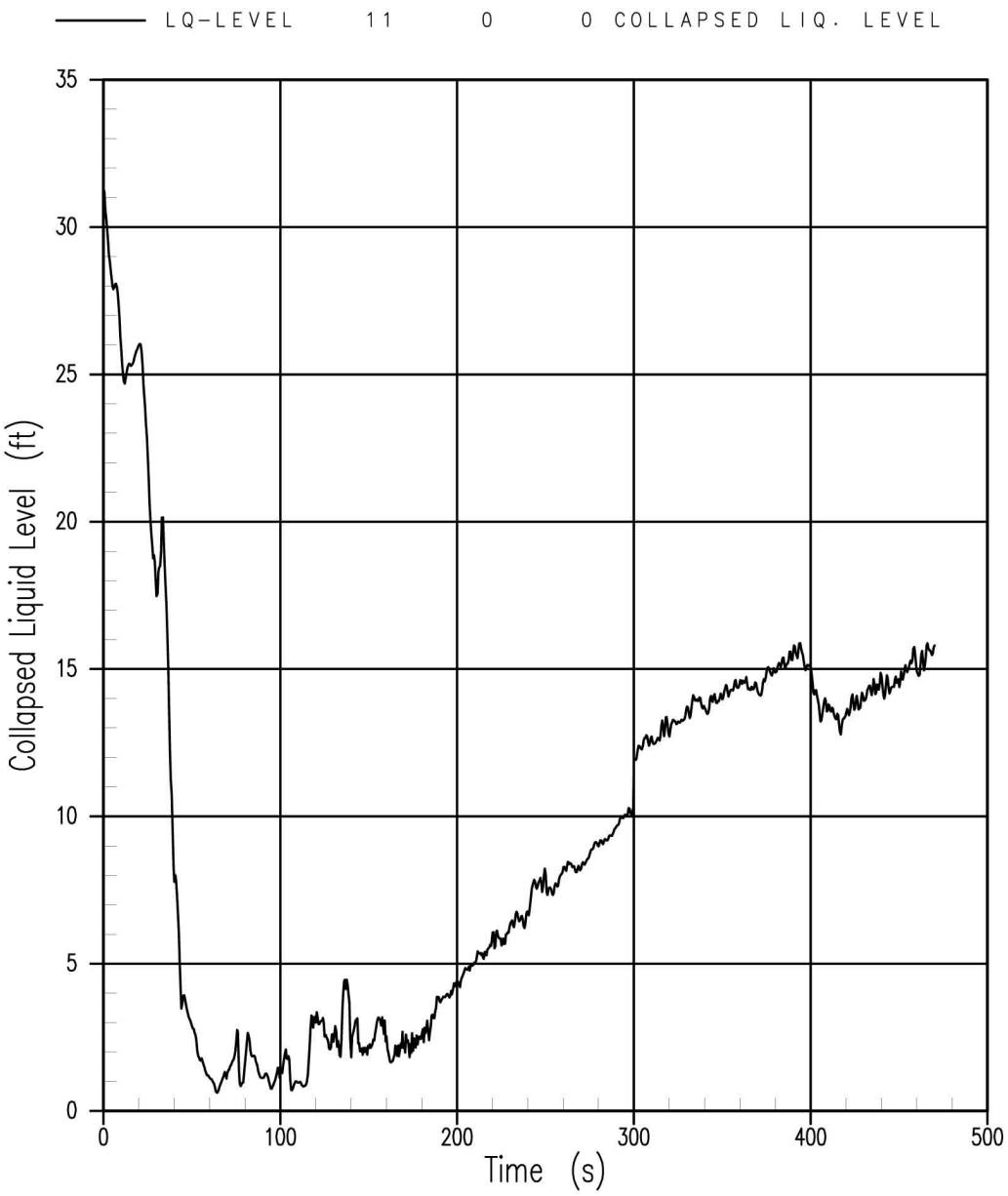

Figure 19E.4.8-4 Mode 3 DECLG Break, Downcomer Collapsed Liquid Level

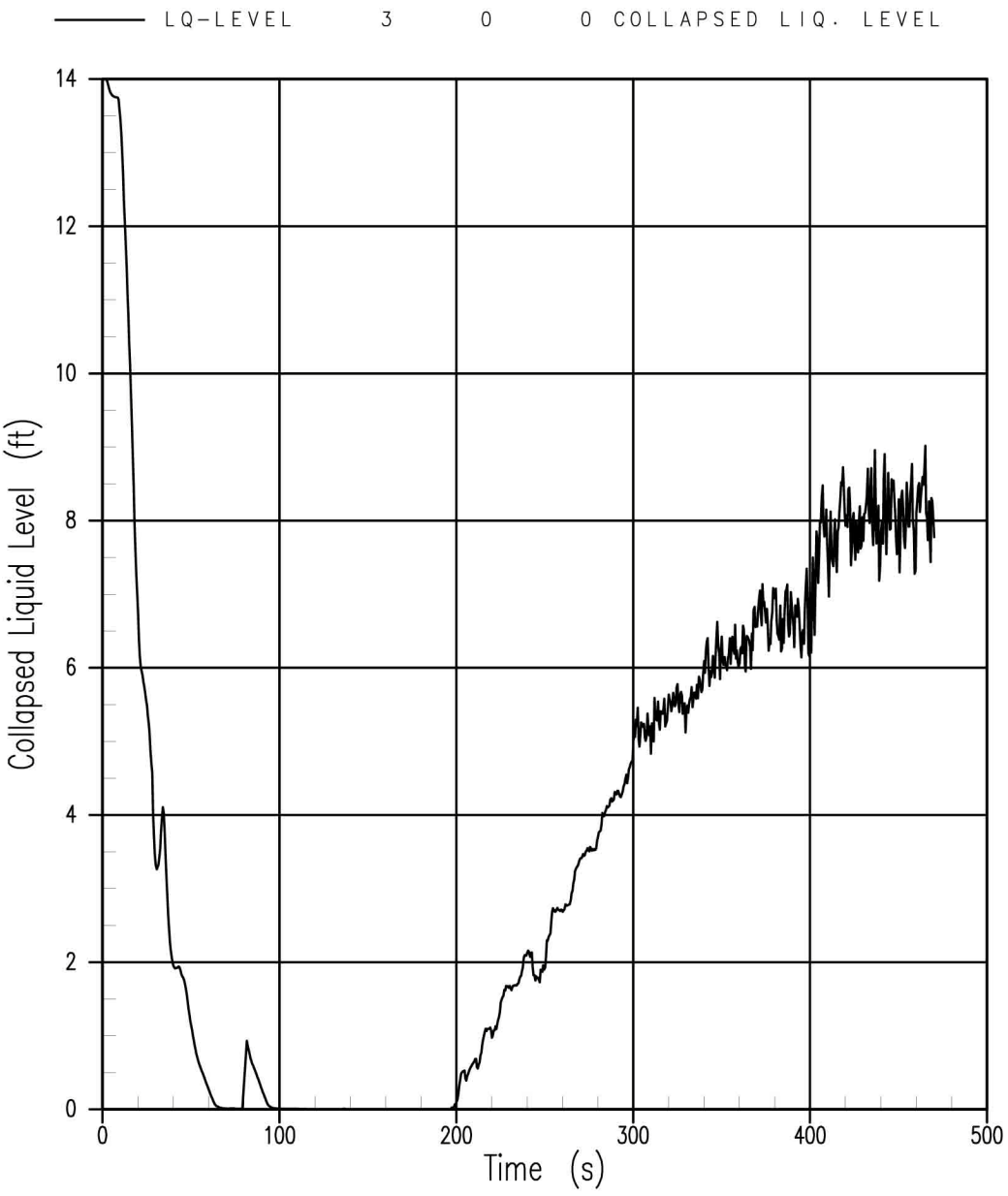

Figure 19E.4.8-5 Mode 3 DECLG Break, Core Collapsed Liquid Level

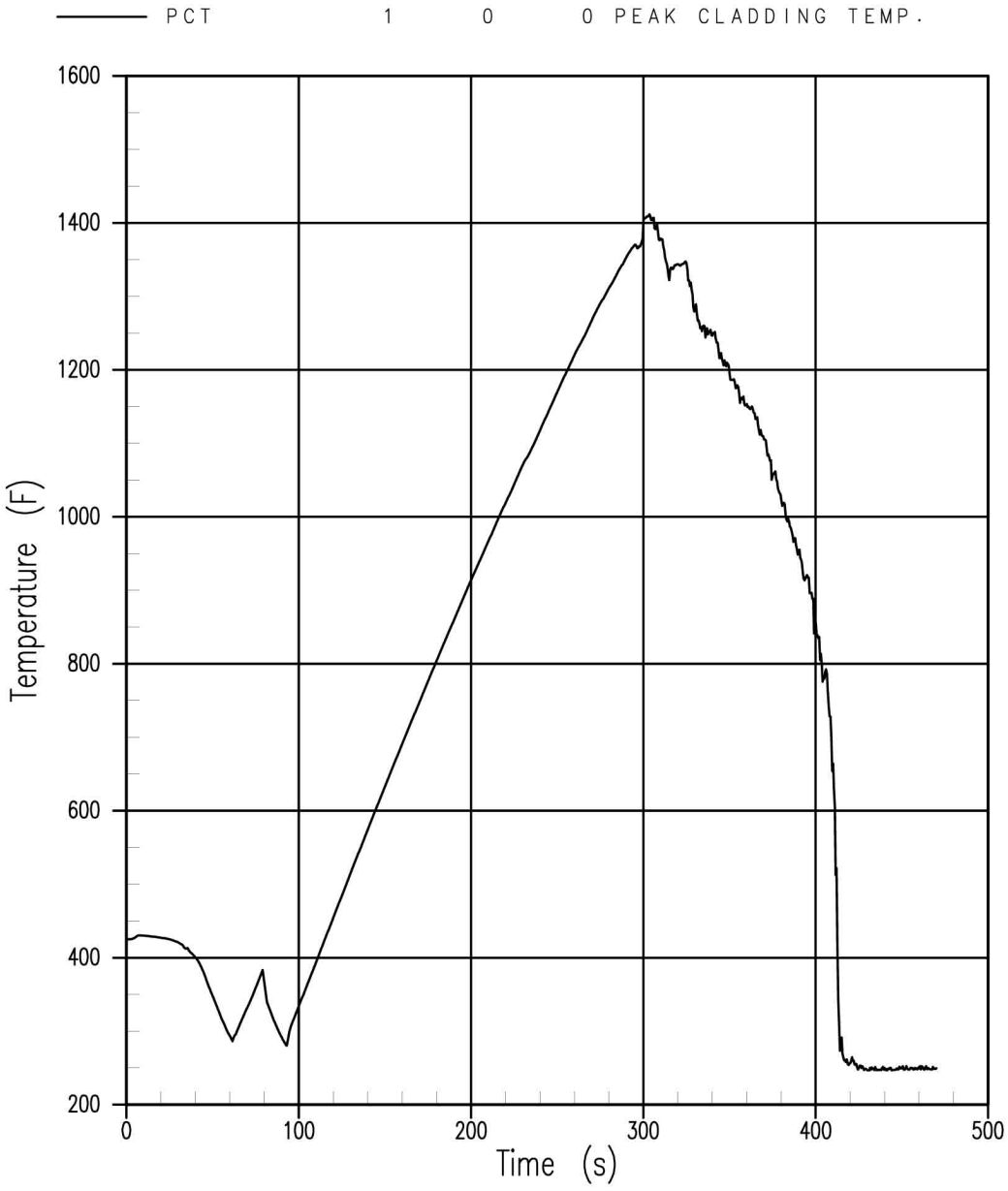

Figure 19E.4.8-6 Mode 3 DECLG Break, Peak Cladding Temperature

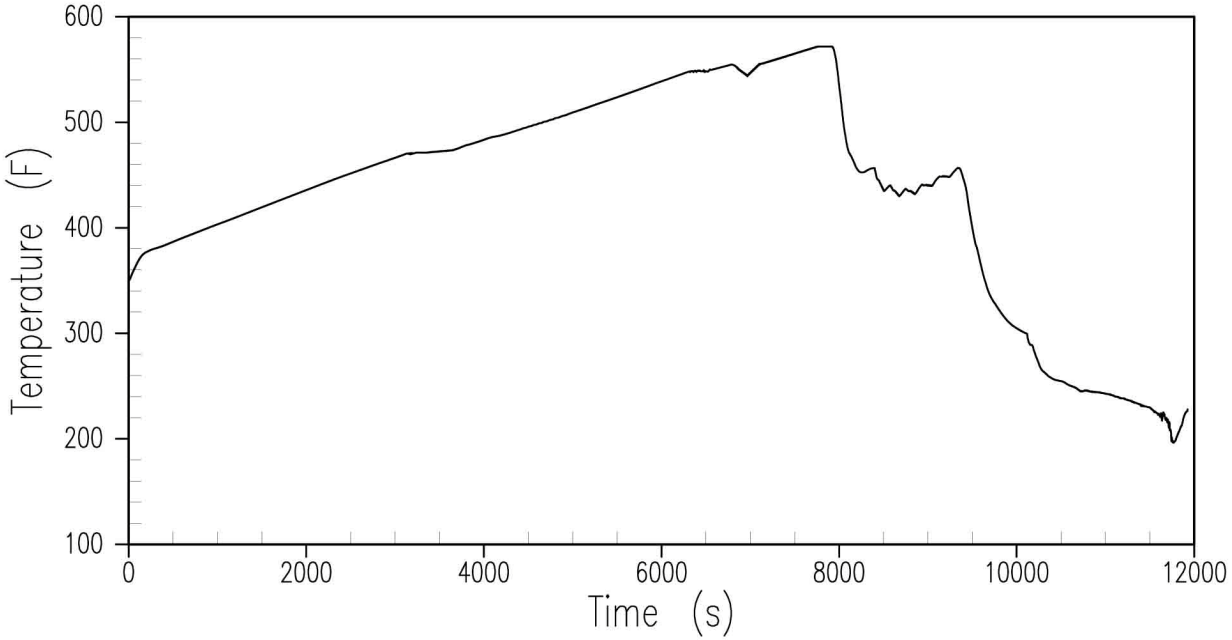

Figure 19E.4.8-7 Core Outlet Temperature, Loss of RNS in Mode 4 with RCS Intact

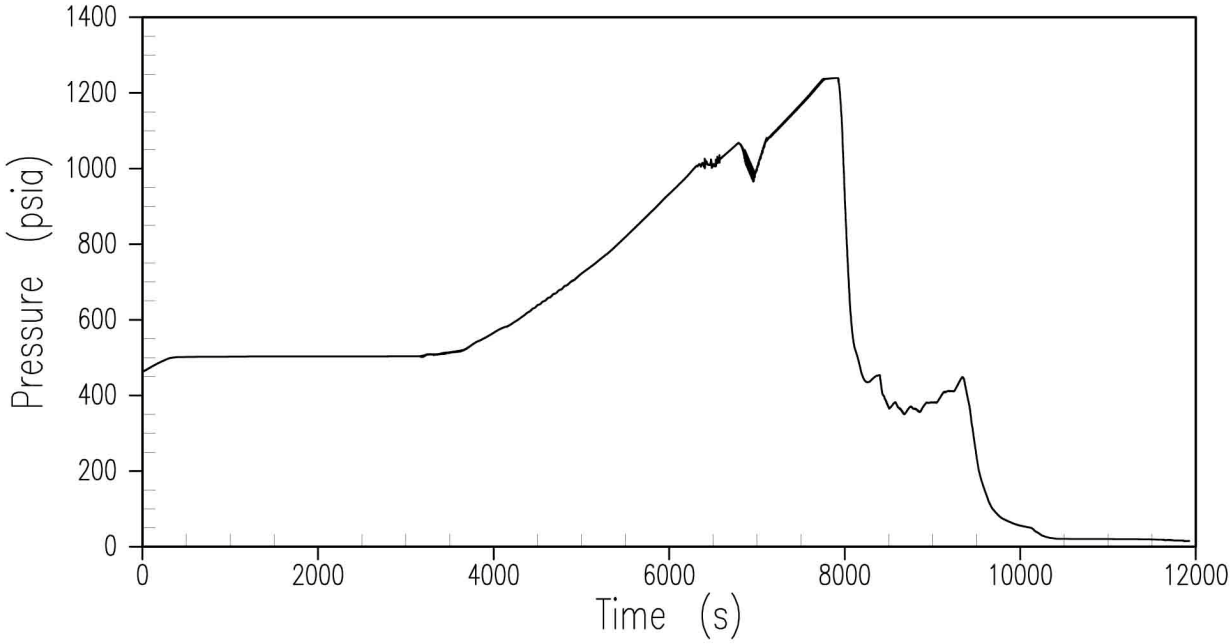

Figure 19E.4.8-8 Pressurizer Pressure, Loss of RNS in Mode 4 with RCS Intact

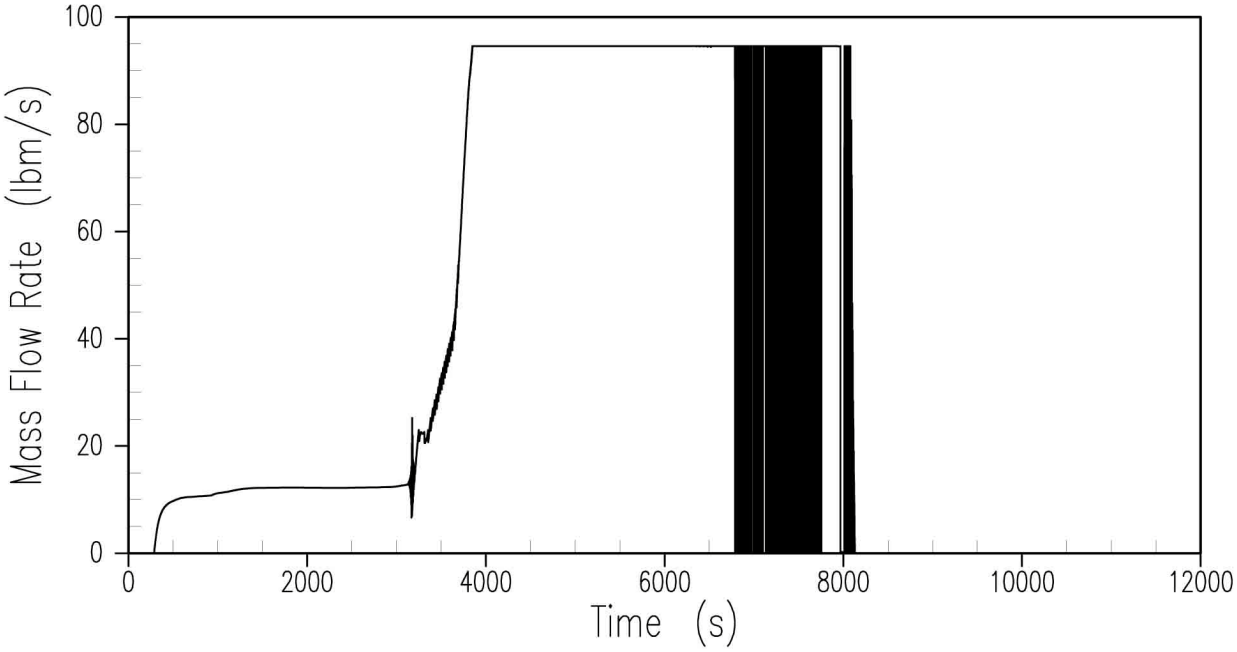

Figure 19E.4.8-9 RNS Relief Valve Flow, Loss of RNS in Mode 4 with RCS Intact

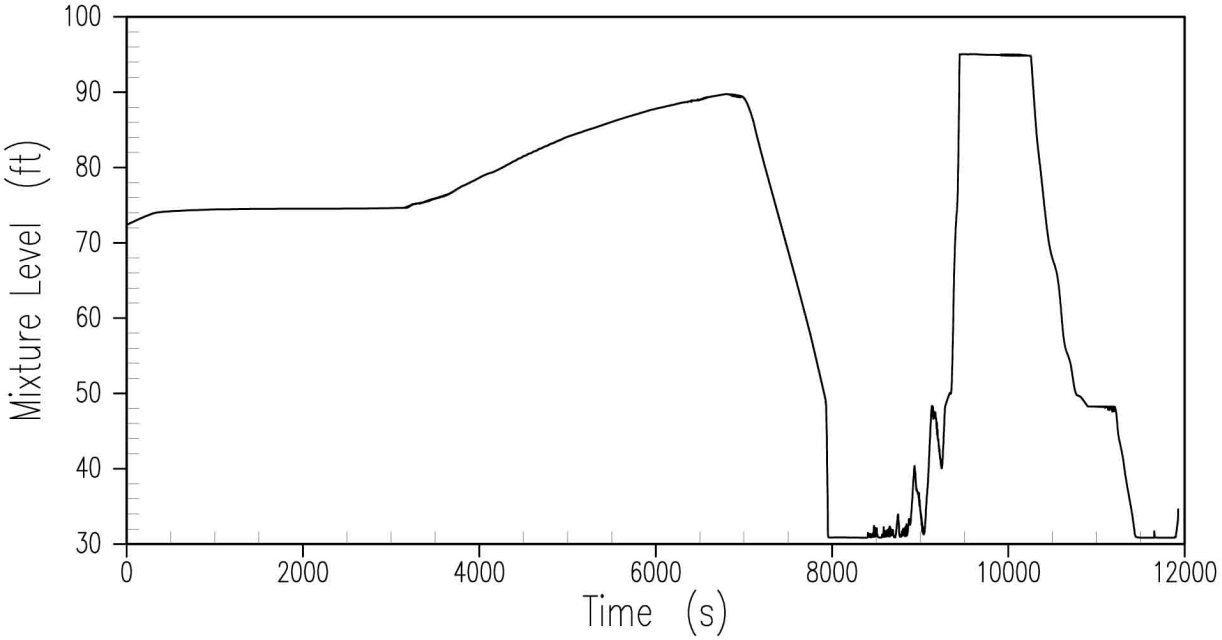

Figure 19E.4.8-10 Pressurizer Mixture Level, Loss of RNS in Mode 4 with RCS Intact

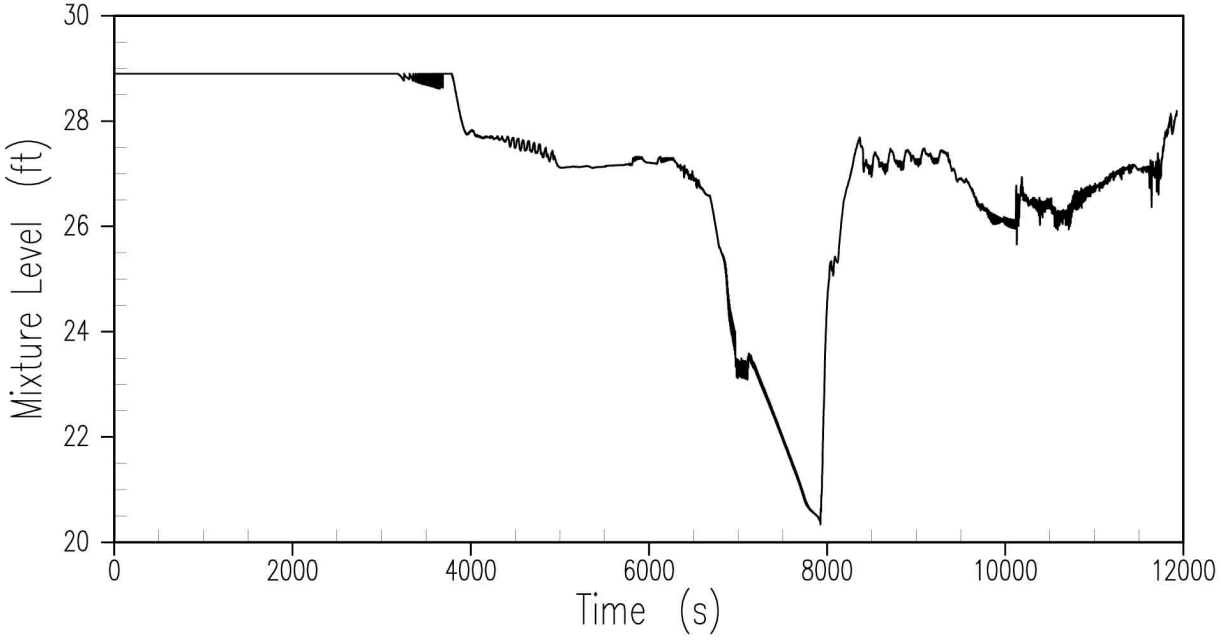

Figure 19E.4.8-11 Core Stack Mixture Level, Loss of RNS in Mode 4 with RCS Intact

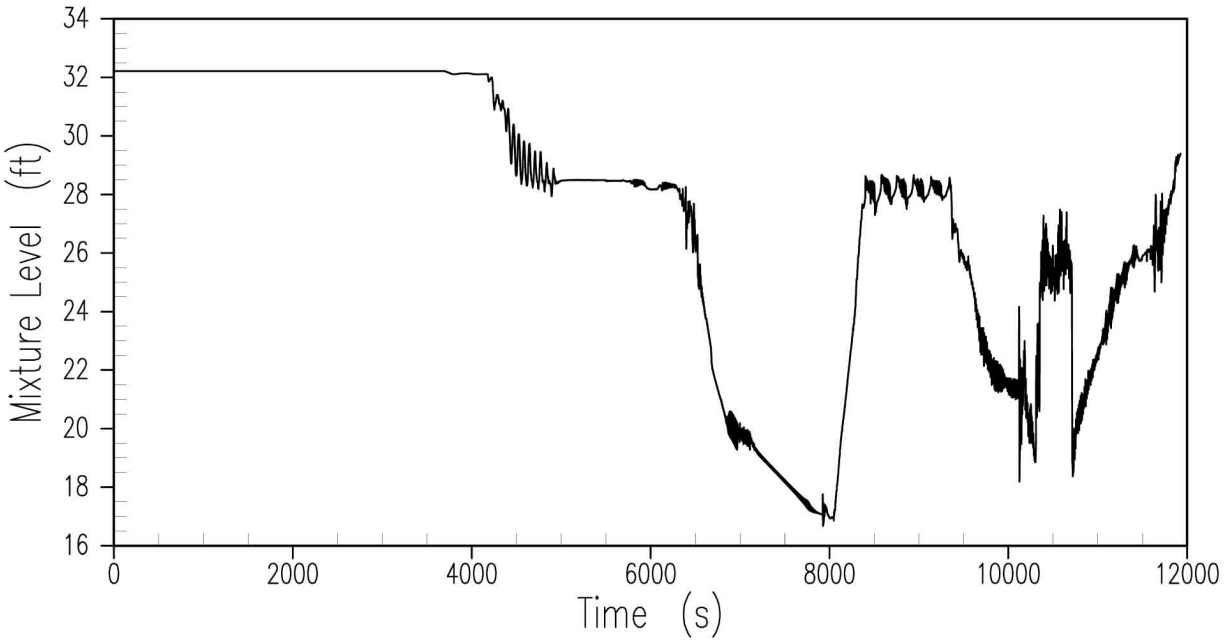

Figure 19E.4.8-12 Downcomer Mixture Level, Loss of RNS in Mode 4 with RCS Intact

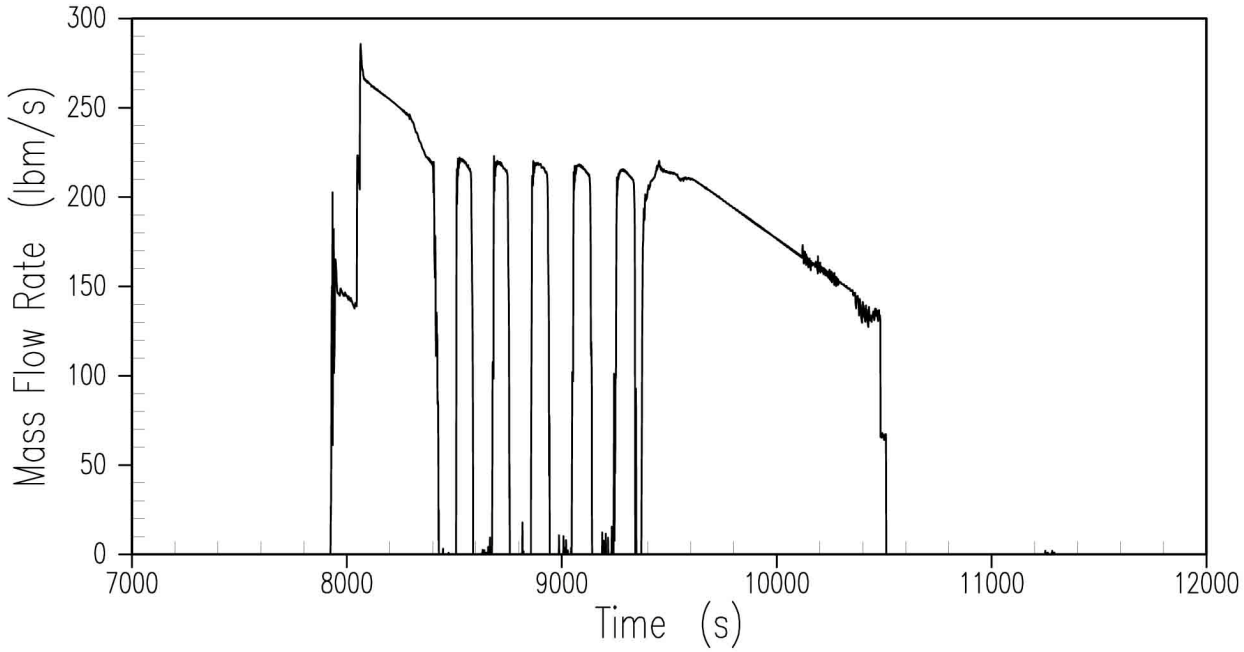

Figure 19E.4.8-13 CMT to DVI Flow, Loss of RNS in Mode 4 with RCS Intact

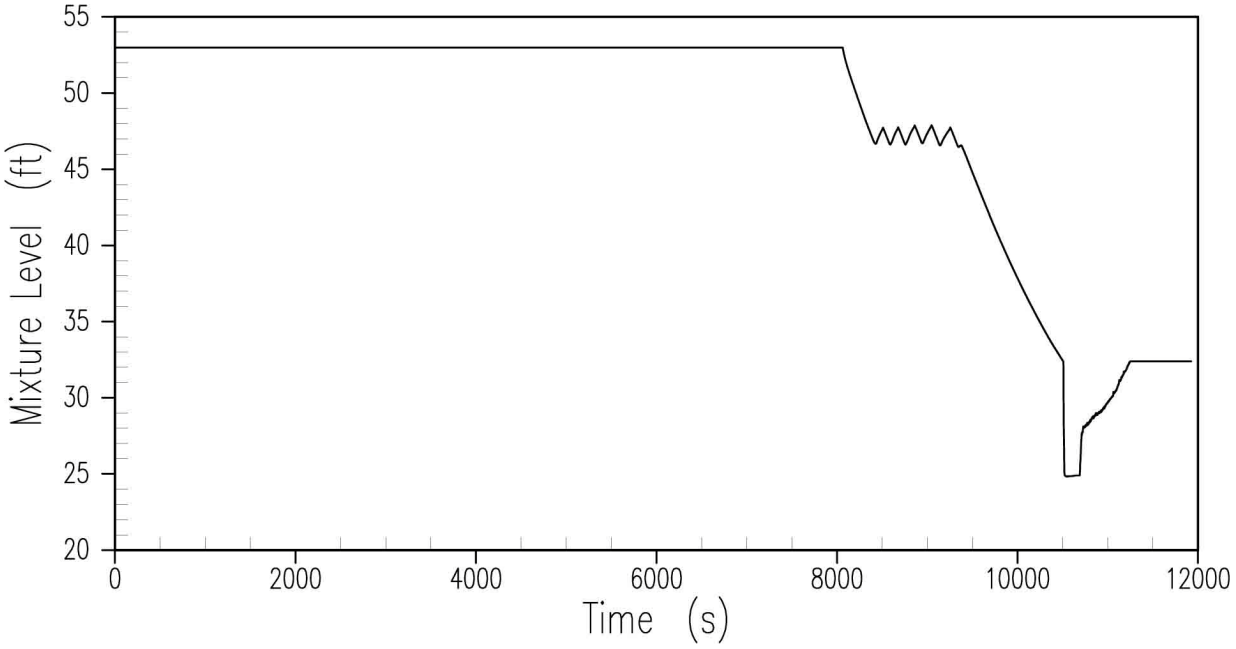

Figure 19E.4.8-14 CMT Mixture Level, Loss of RNS in Mode 4 with RCS Intact

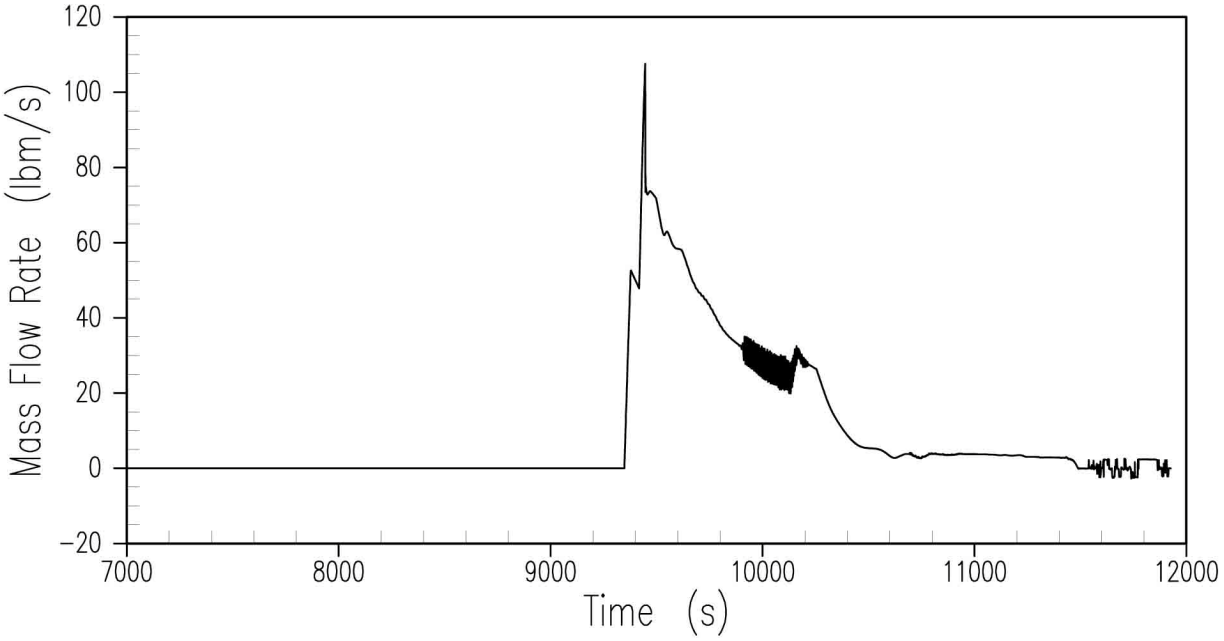

Figure 19E.4.8-15 ADS Stages 1-3 Vapor Flow, Loss of RNS in Mode 4 with RCS Intact

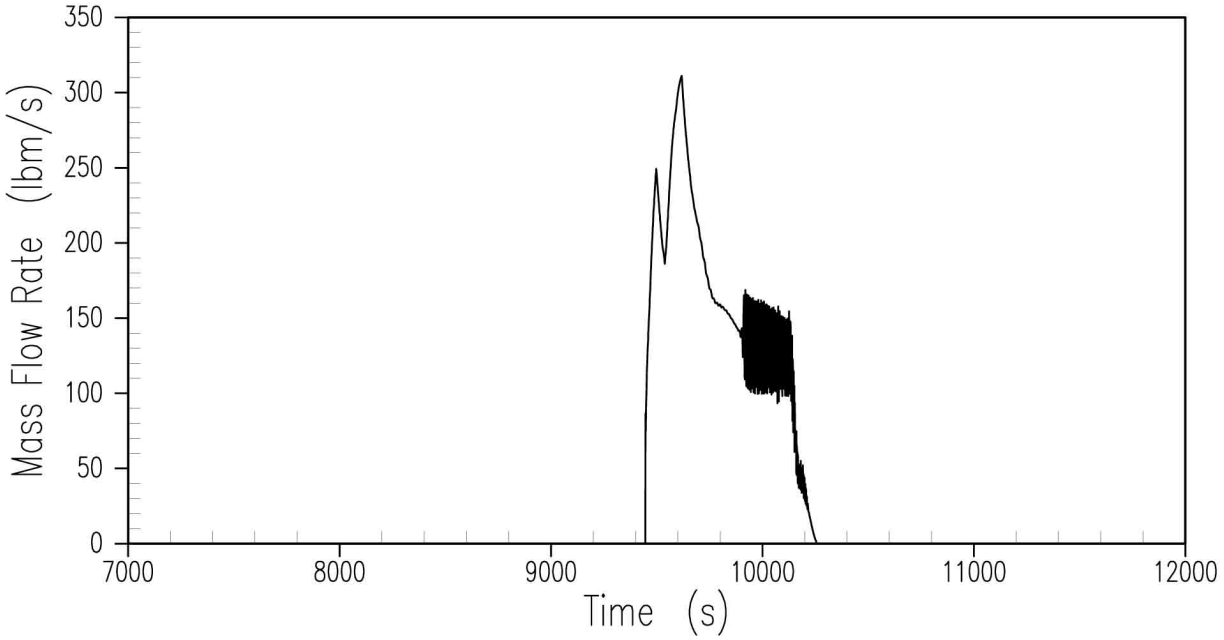

Figure 19E.4.8-16 ADS Stages 1-3 Liquid Flow, Loss of RNS in Mode 4 with RCS Intact

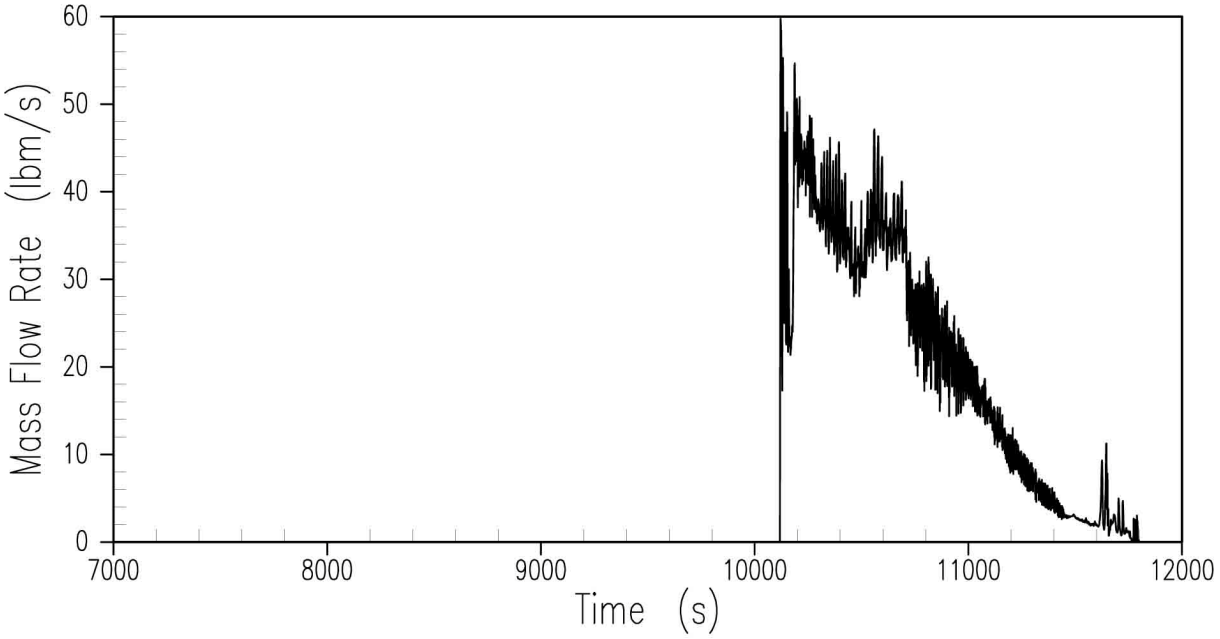

Figure 19E.4.8-17 ADS Stage 4 Vapor Flow, Loss of RNS in Mode 4 with RCS Intact

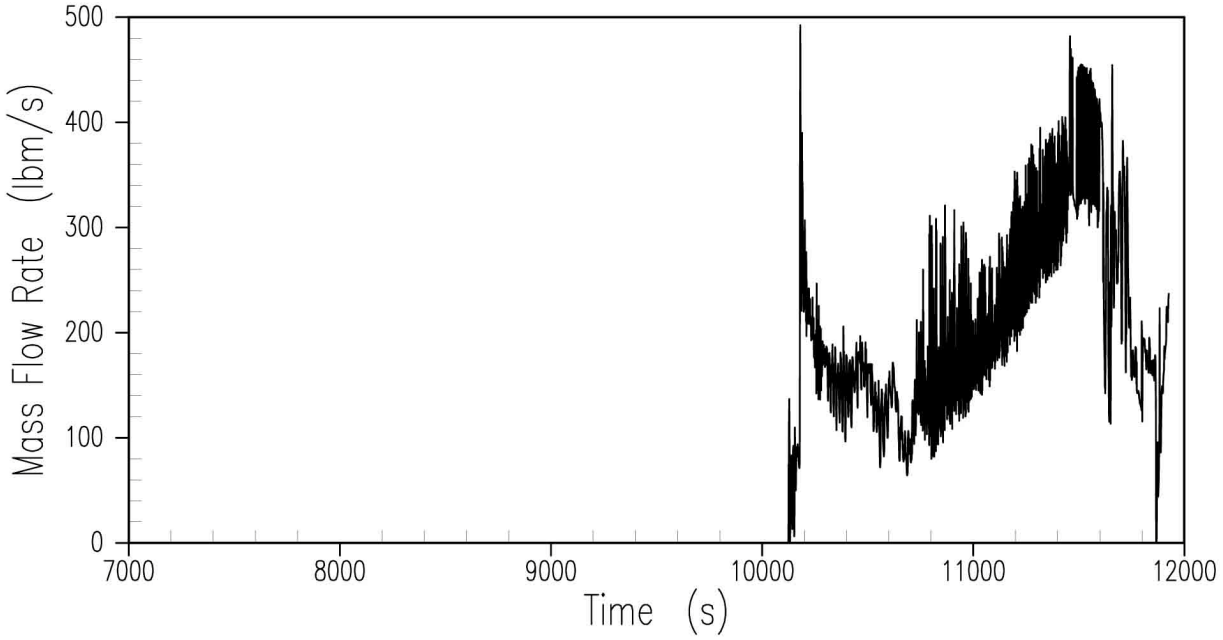

Figure 19E.4.8-18 ADS Stage 4 Liquid Flow, Loss of RNS in Mode 4 with RCS Intact

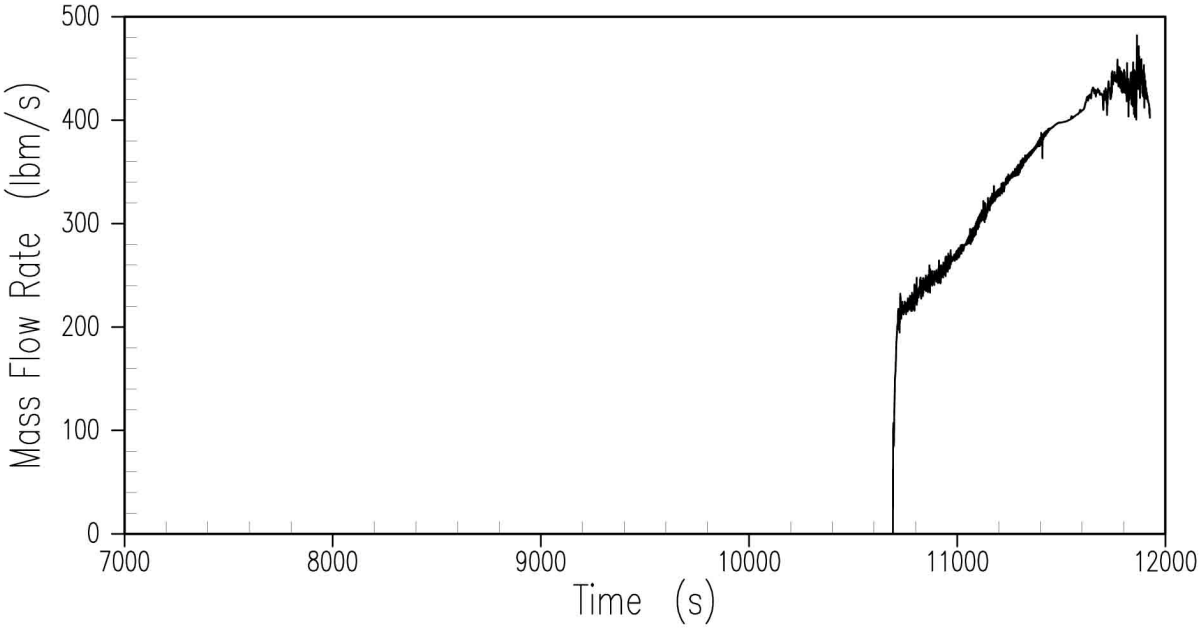

Figure 19E.4.8-19 Loop 1 IRWST Injection Flow, Loss of RNS in Mode 4 with RCS Intact

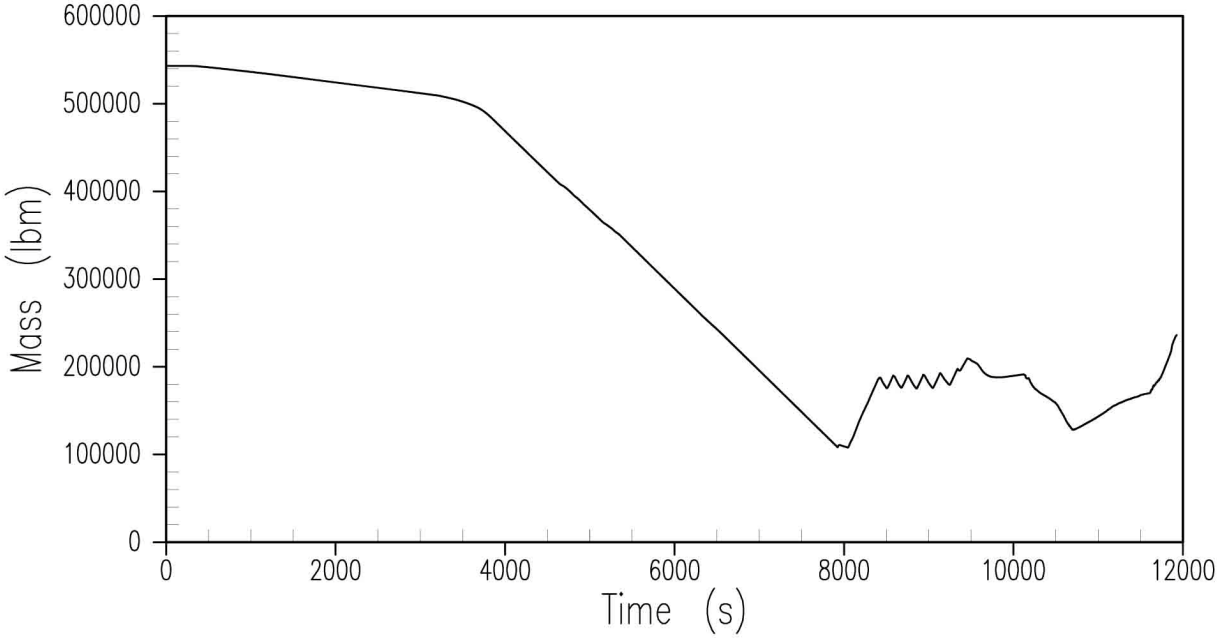

Figure 19E.4.8-20 Primary Mass Inventory, Loss of RNS in Mode 4 with RCS Intact

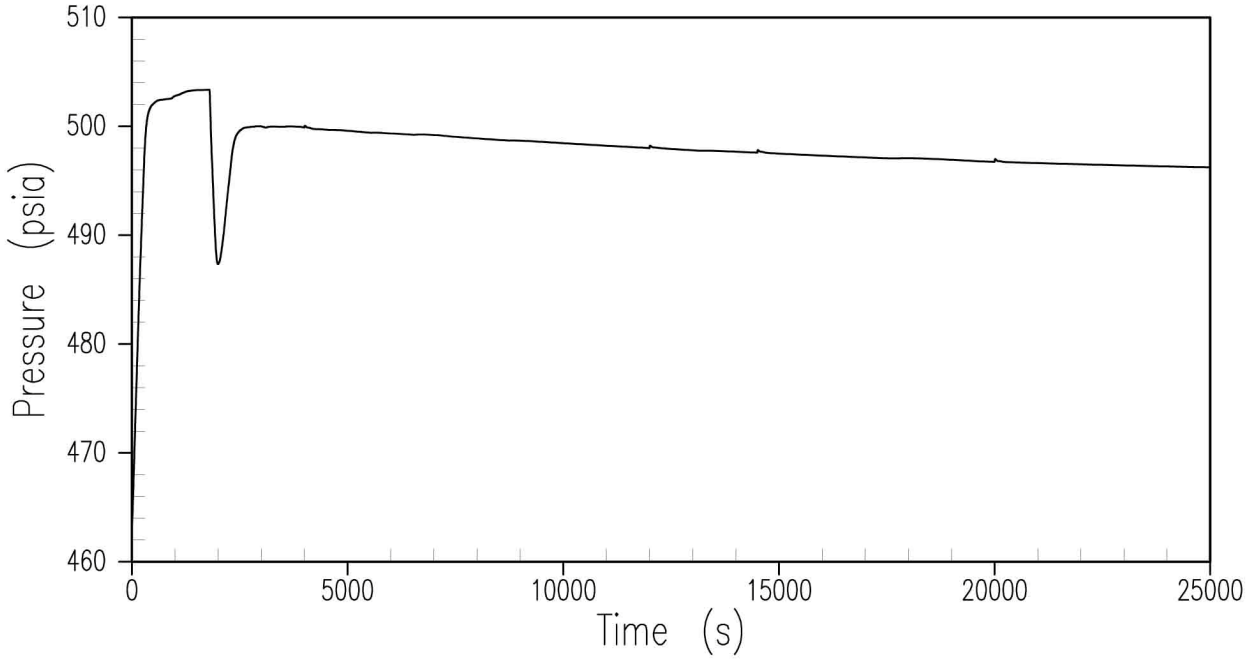

Figure 19E.4.8-21 Pressurizer Pressure, Loss of RNS in Mode 4 with RCS Intact, Manual Safety System Actuation at 1800 Seconds

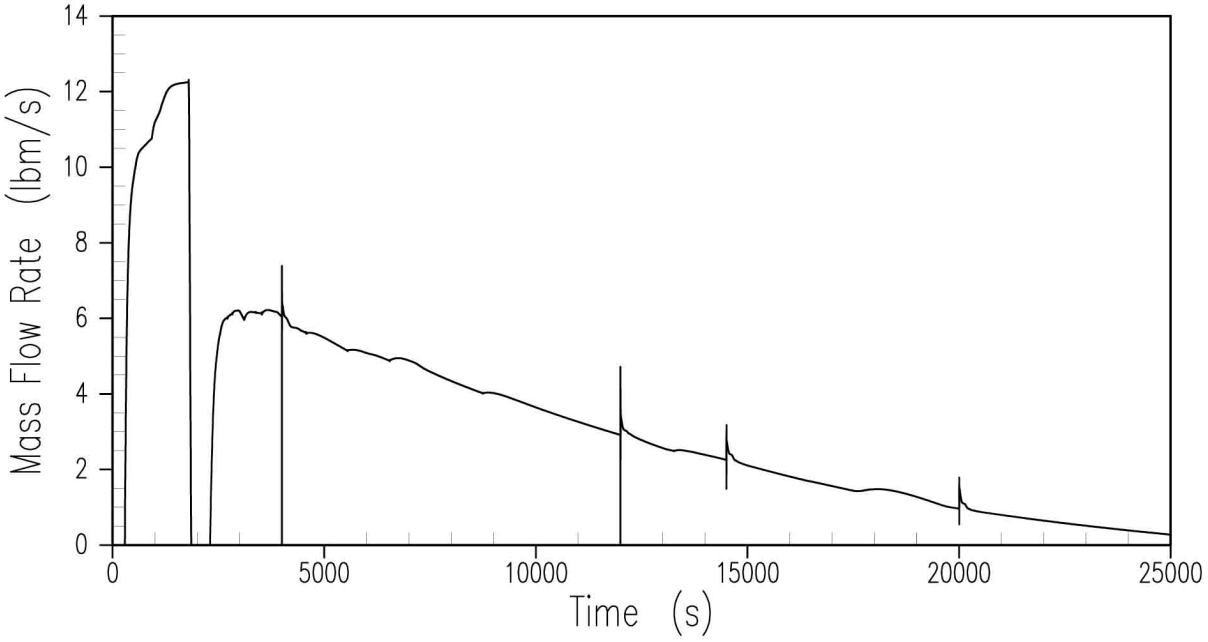

Figure 19E.4.8-22 RNS Safety Valve Flow, Loss of RNS in Mode 4 RCS Intact, Manual Safety System Actuation at 1800 Seconds

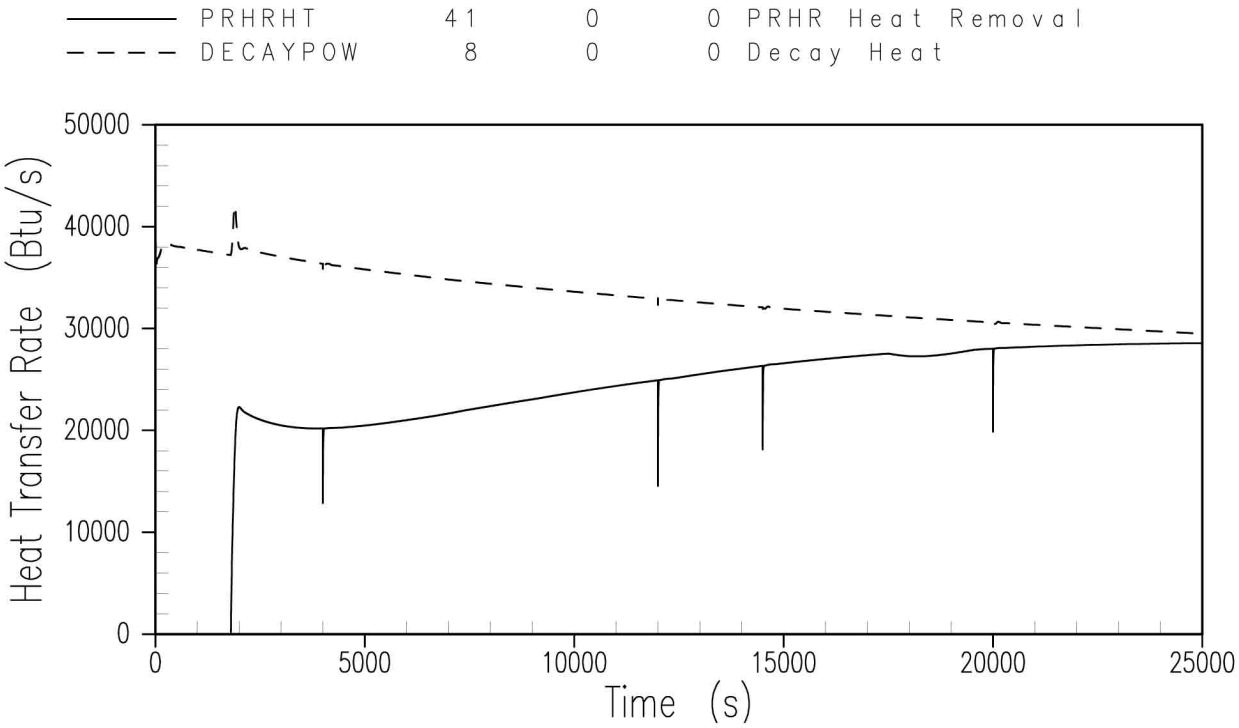

Figure 19E.4.8-23 Decay Heat and PRHR Heat Removal, Loss of RNS in Mode 4 with RCS Intact, Manual Safety System Actuation at 1800 Seconds

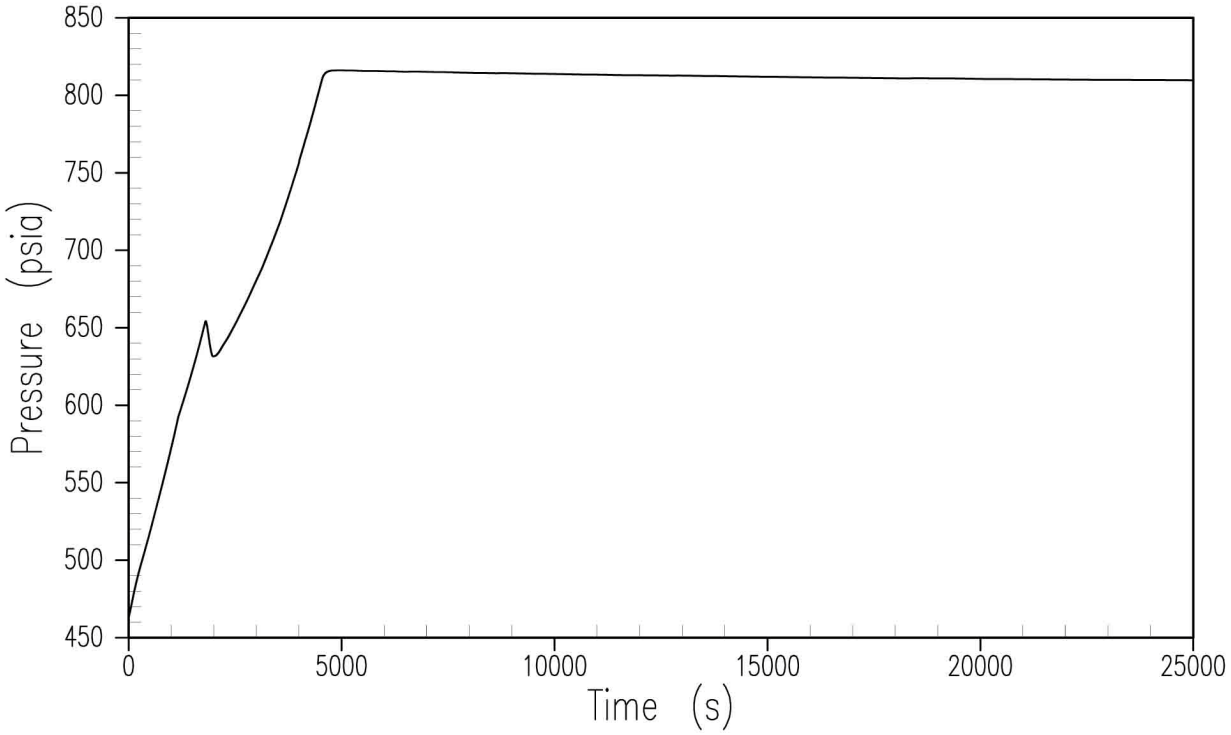

Figure 19E.4.8-24 Core Outlet Fluid Temperature, Loss of RNS in Mode 5 with RCS Open

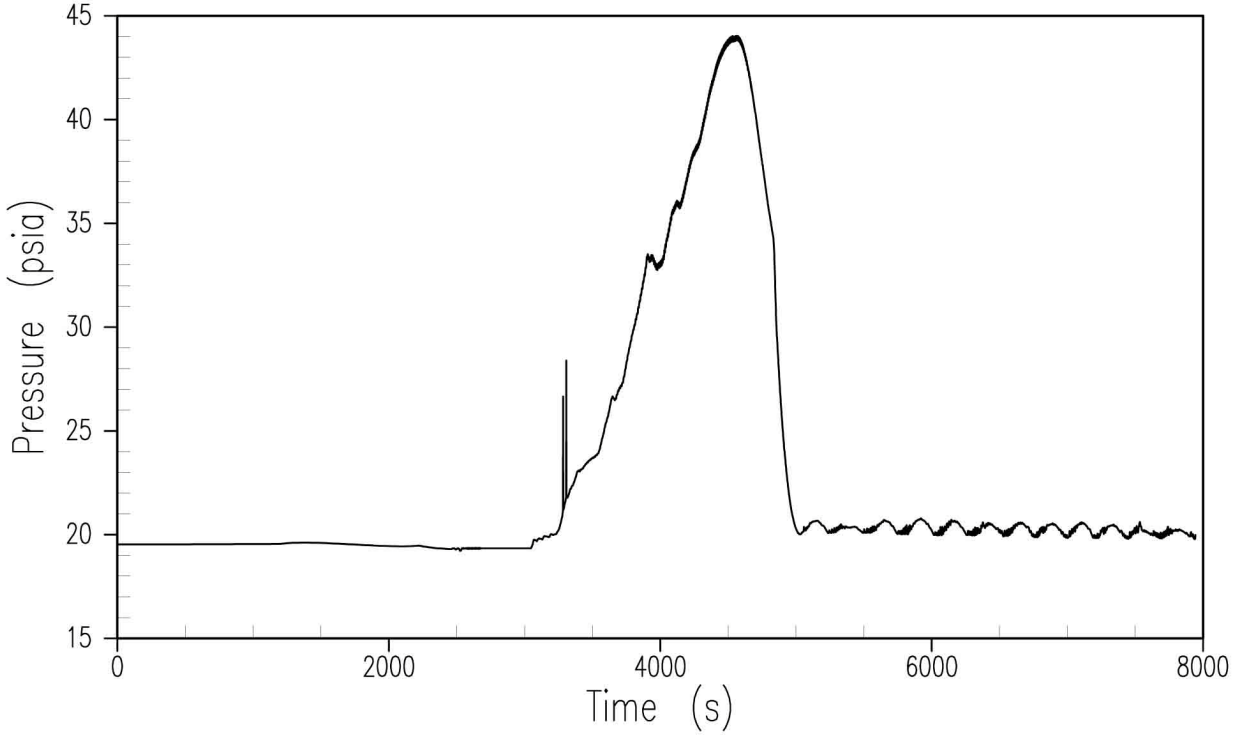

Figure 19E.4.8-25 Pressurizer Pressure, Loss of RNS in Mode 5 with RCS Open

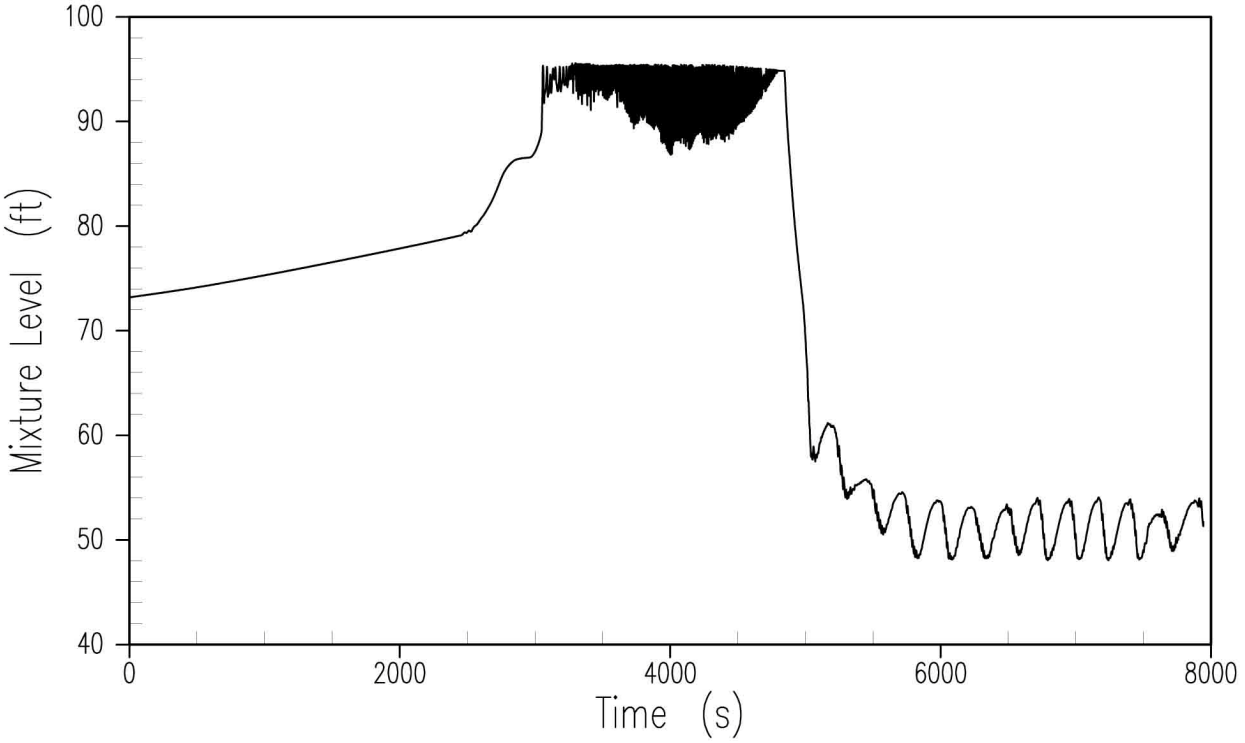

Figure 19E.4.8-26 Pressurizer Mixture Level, Loss of RNS in Mode 5 with RCS Open

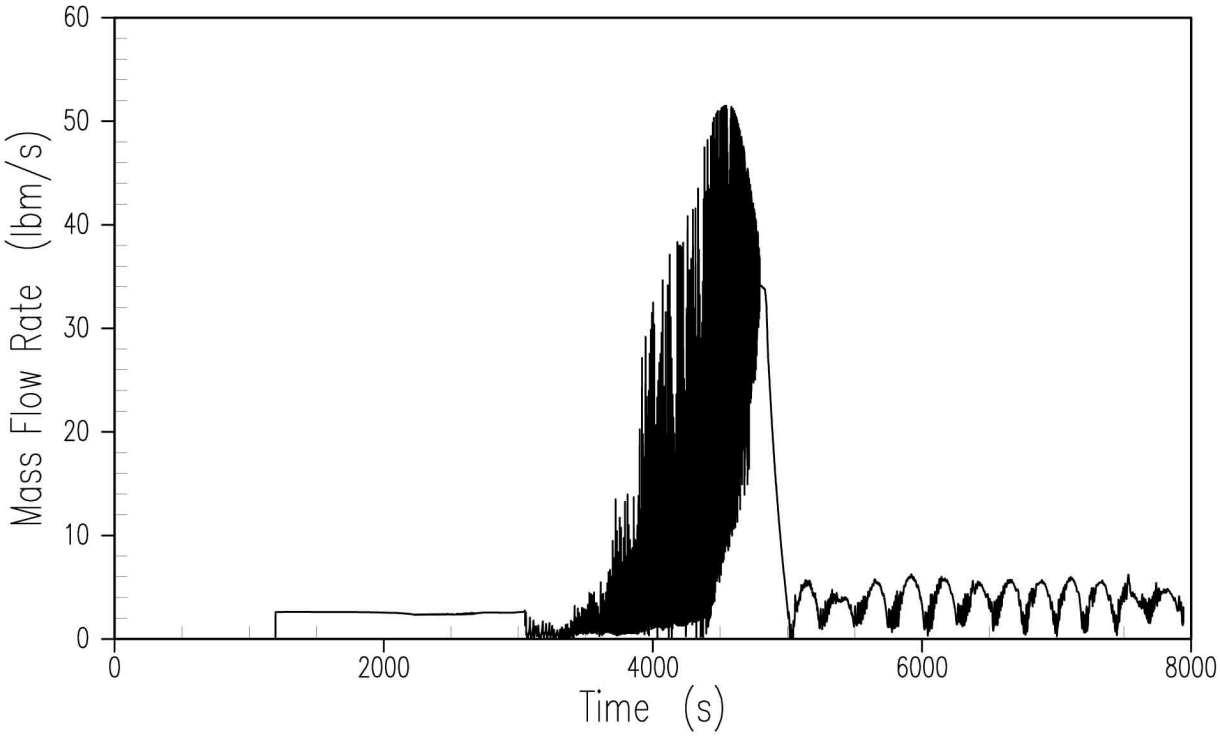

Figure 19E.4.8-27 ADS Stages 1-3 Vapor Flow, Loss of RNS in Mode 5 with RCS Open

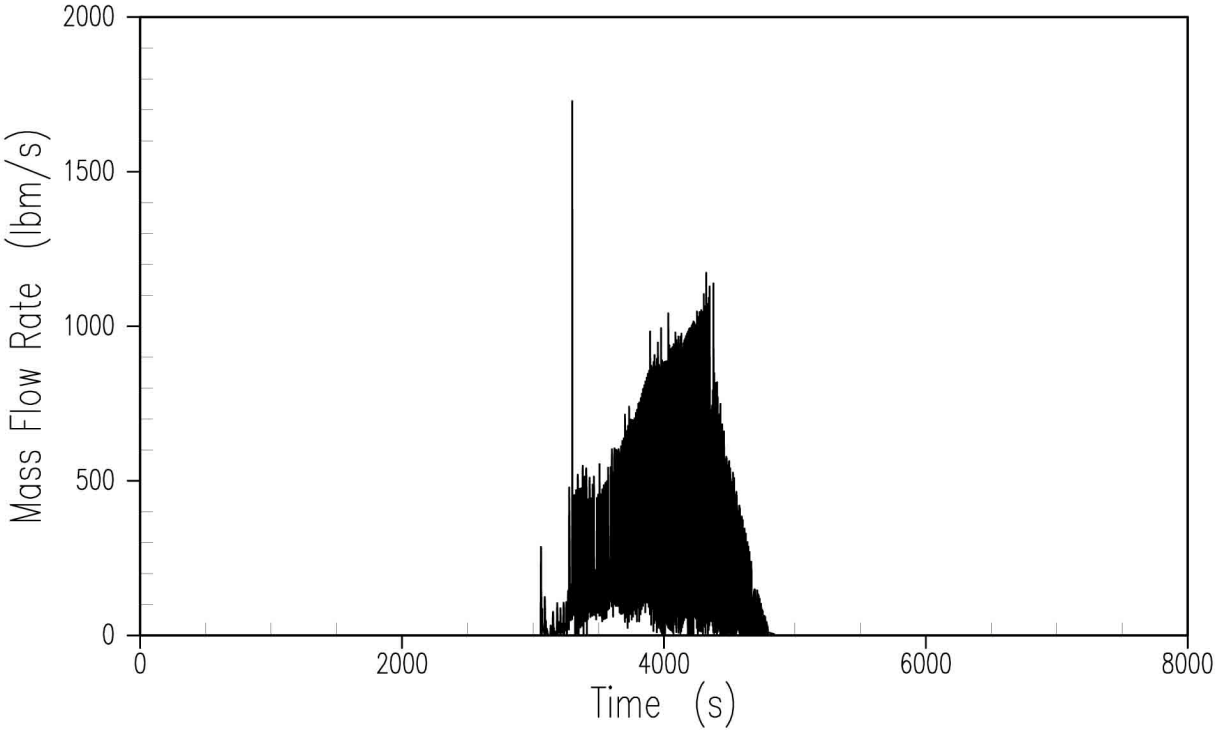

Figure 19E.4.8-28 ADS Stages 1-3 Liquid Flow, Loss of RNS in Mode 5 with RCS Open

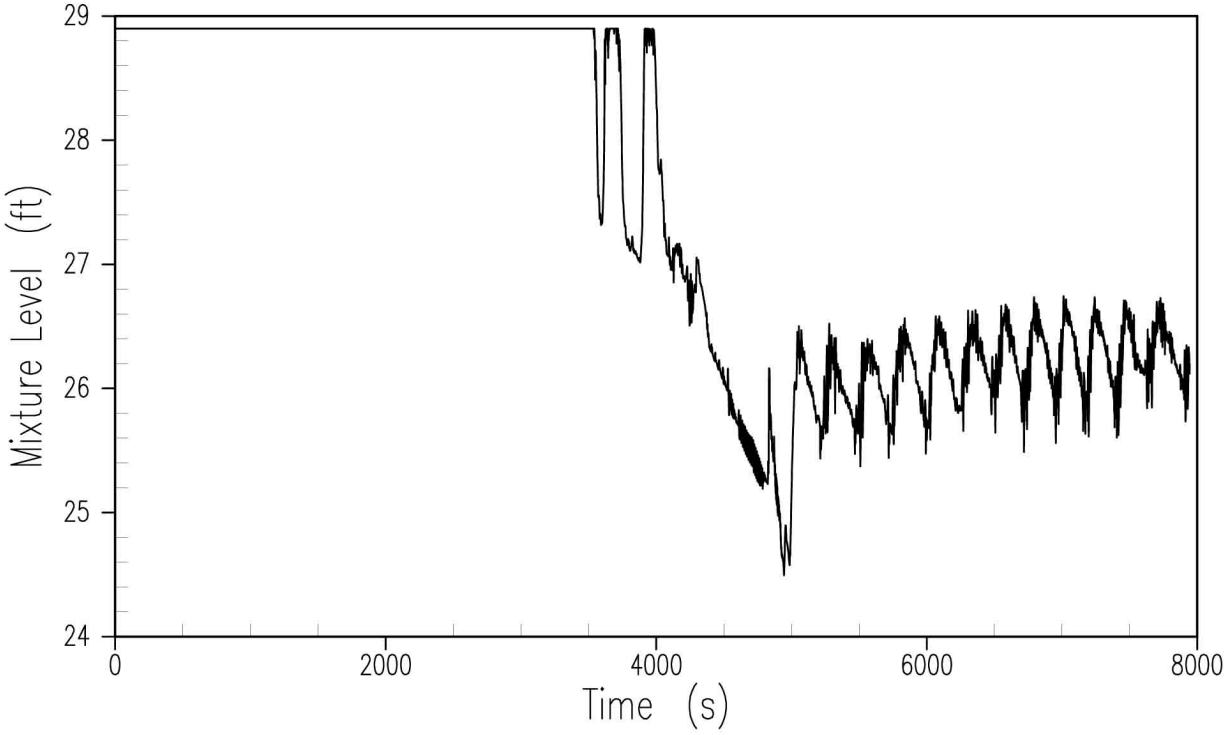

Figure 19E.4.8-29 Core Stack Mixture Level, Loss of RNS in Mode 5 with RCS Open

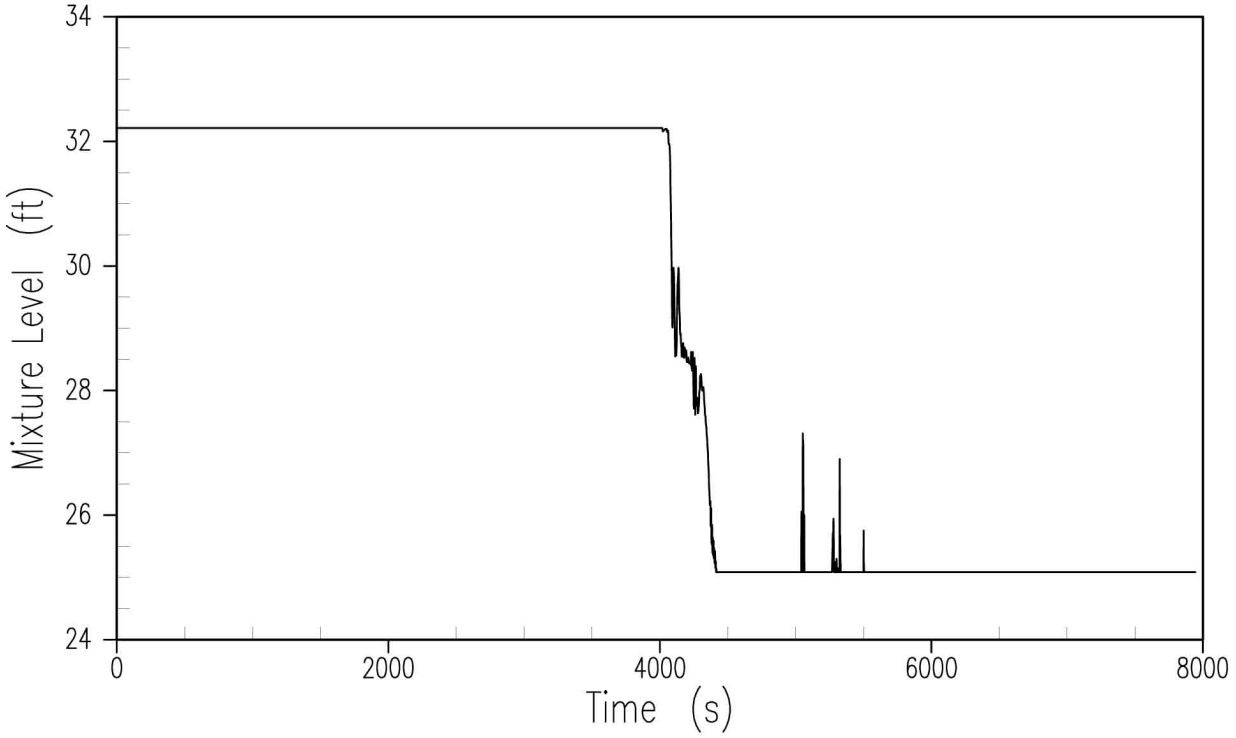

Figure 19E.4.8-30 Downcomer Mixture Level, Loss of RNS in Mode 5 with RCS Open

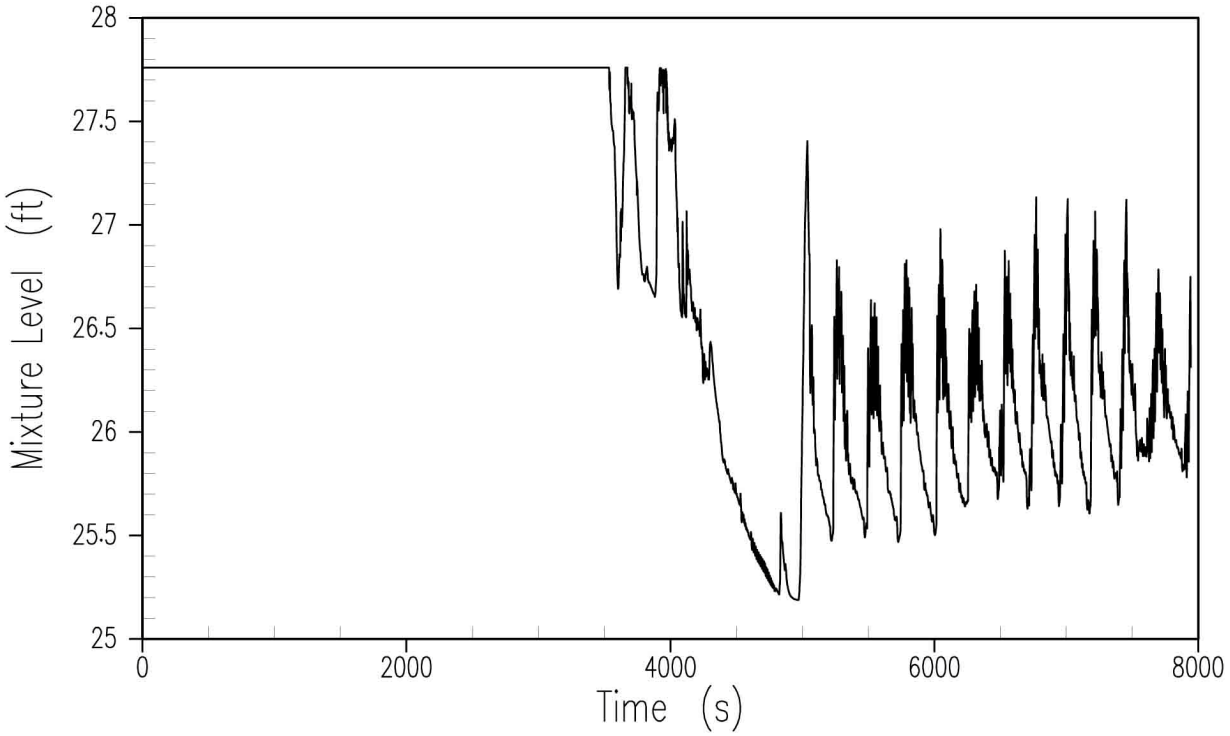

Figure 19E.4.8-31 Loop 1 Hot-Leg Mixture Level, Loss of RNS in Mode 5 with RCS Open

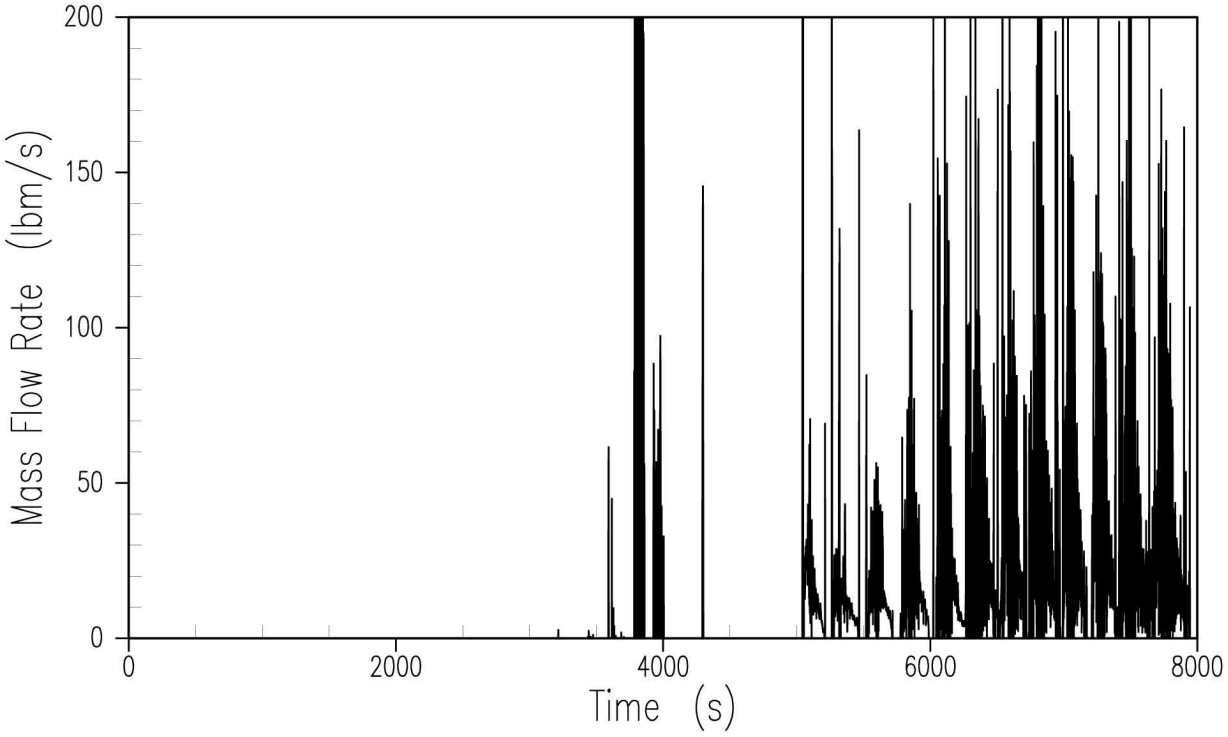

Figure 19E.4.8-32 ADS Stage 4 Vapor Flow, Loss of RNS in Mode 5 with RCS Open

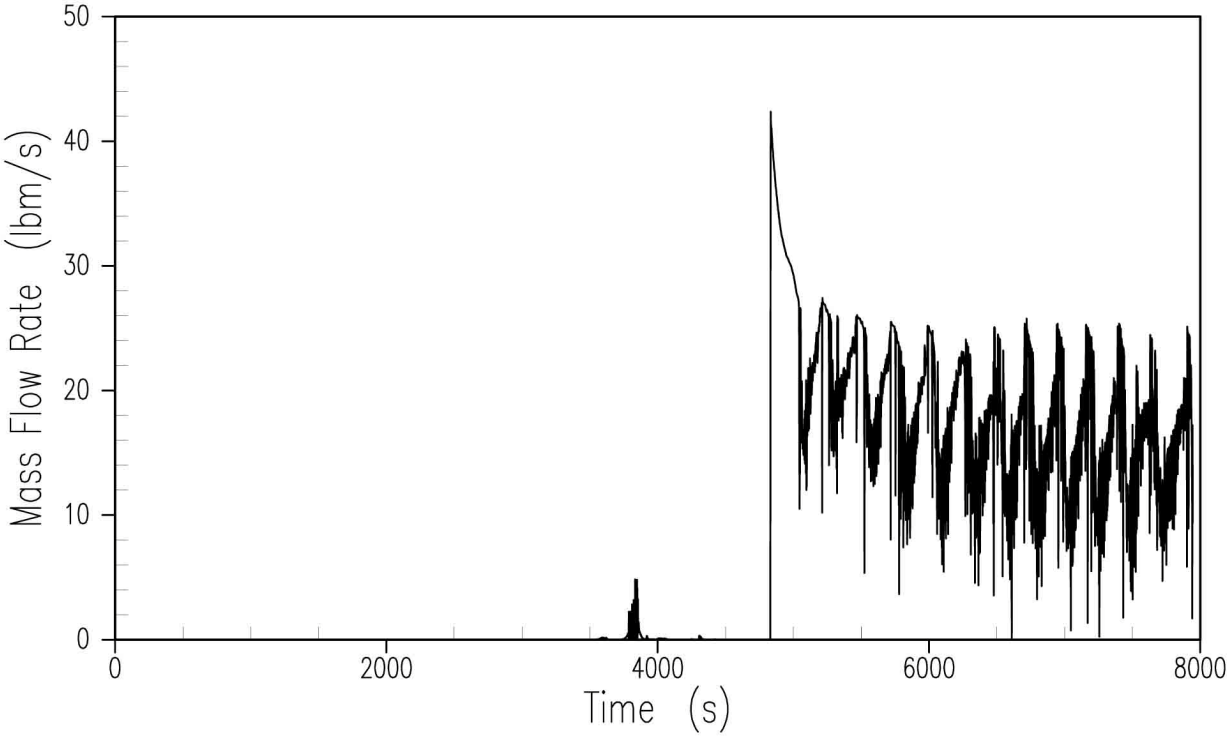

Figure 19E.4.8-33 ADS Stage 4 Liquid Flow, Loss of RNS in Mode 5 with RCS Open

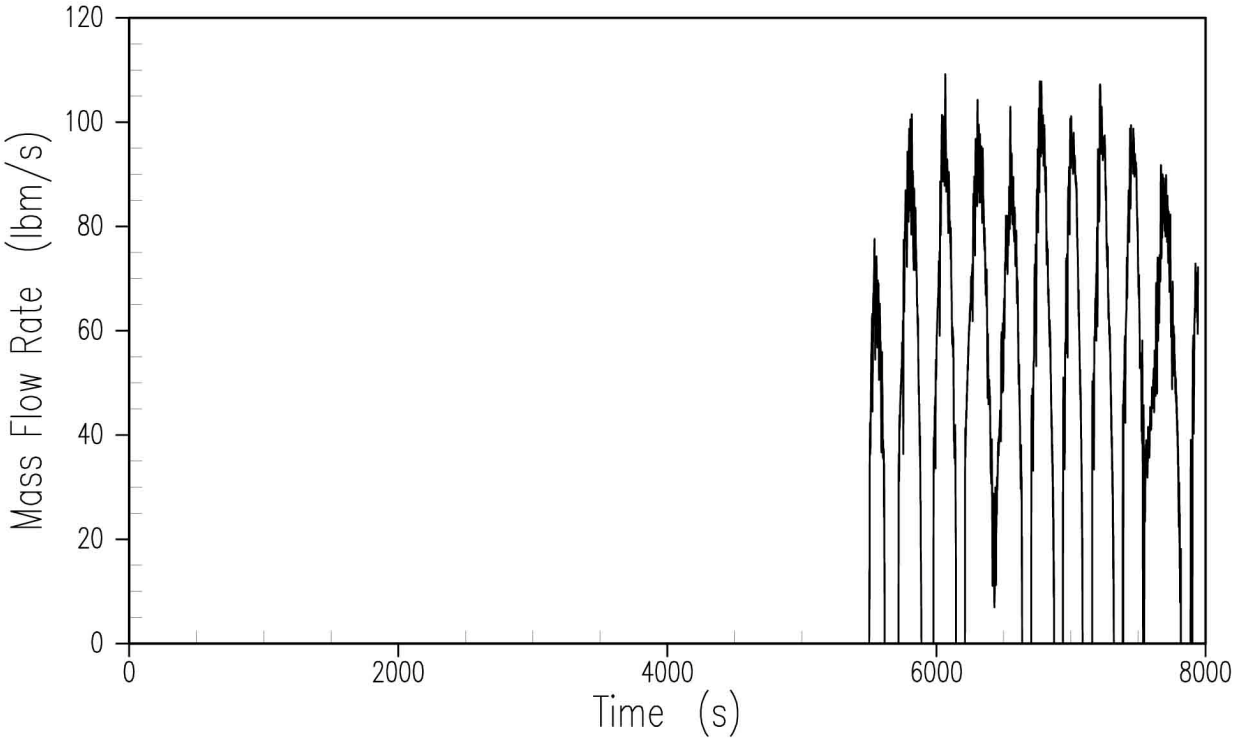

Figure 19E.4.8-34 IRWST Injection Flow, Loss of RNS in Mode 5 with RCS Open

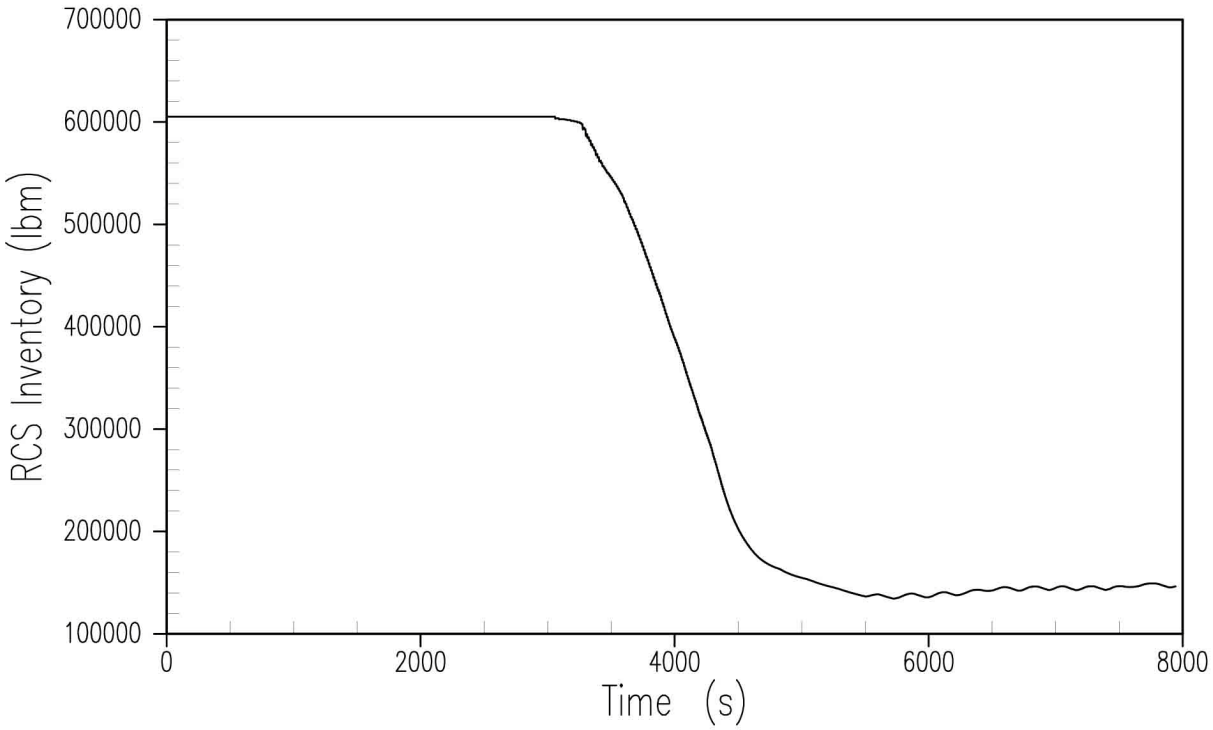

Figure 19E.4.8-35 Primary Mass Inventory, Loss of RNS in Mode 5 with RCS Open

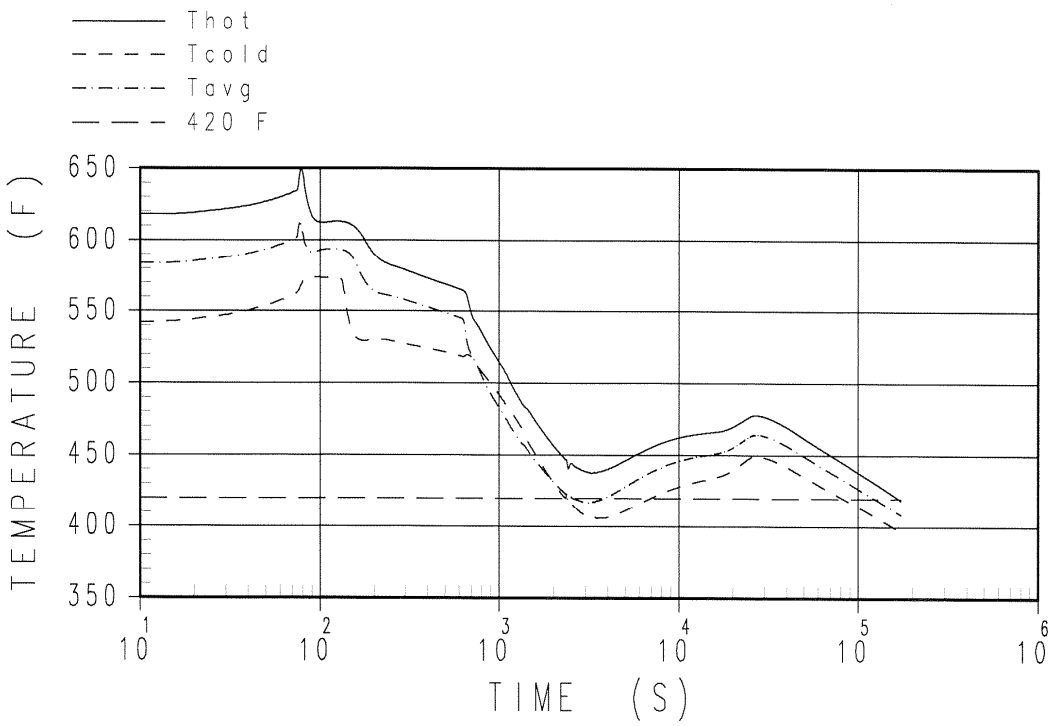

Figure 19E.4.10-1 Shutdown Temperature Evaluation, RCS Temperature

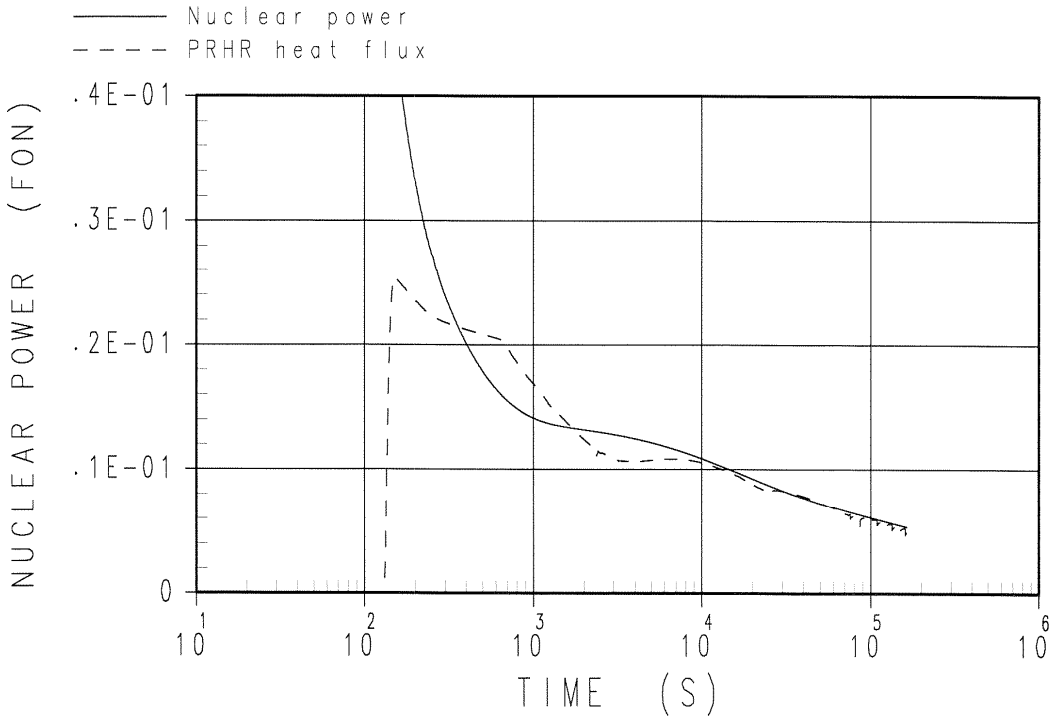

Figure 19E.4.10-2 Shutdown Temperature Evaluation, PRHR Heat Transfer

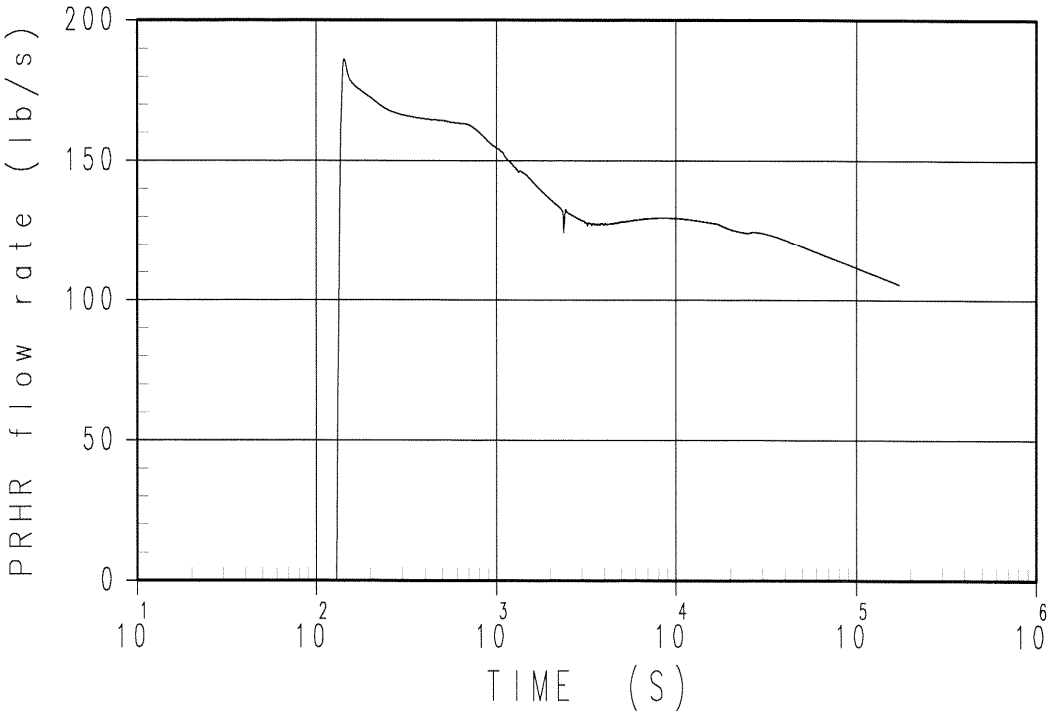

Figure 19E.4.10-3 Shutdown Temperature Evaluation, PRHR Flow Rate

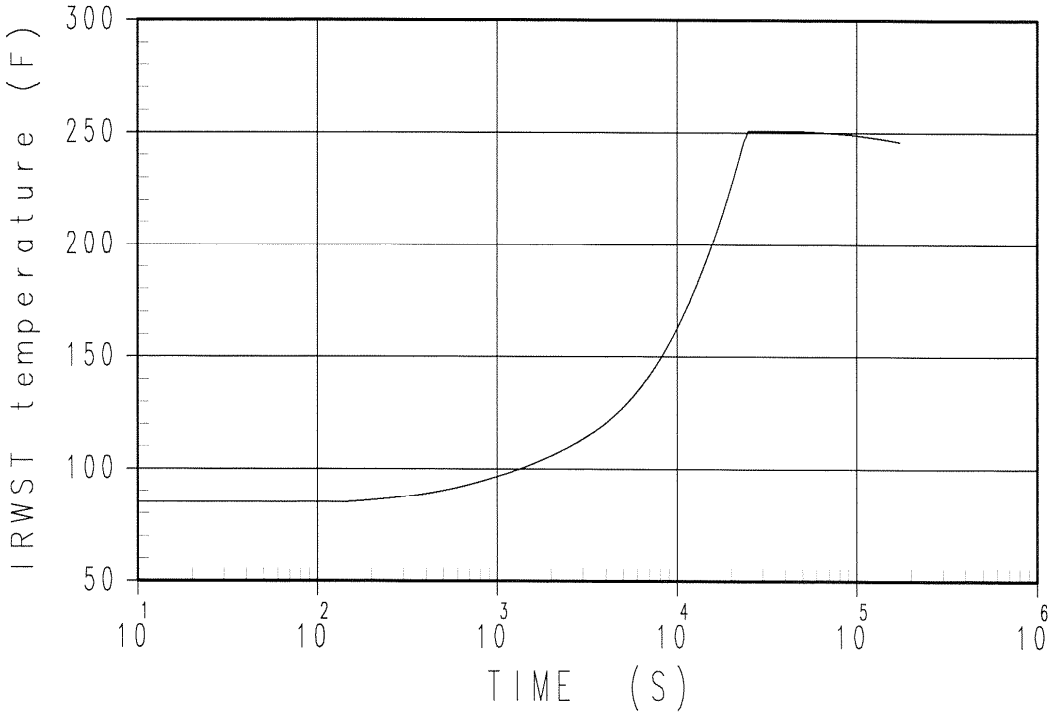

Figure 19E.4.10-4 Shutdown Temperature Evaluation, IRWST Heatup

Appendix 19F Malevolent Aircraft Impact

19F.1 Introduction and Background

A design-specific assessment of the effects on the AP1000 of the beyond design basis impact of a large commercial aircraft has been performed in accordance with 10 CFR 50.150(a) to identify design features and functional capabilities that demonstrate with reduced use of operator actions: (i) the reactor core remains cooled, the containment remains intact, and (ii) spent fuel pool integrity is maintained. The specific assumptions regarding the aircraft impact were based on guidance provided by the NRC and the Nuclear Energy Institute, including the loading function derived from the aircraft impact characteristics for use in assessments of aircraft impact effects.

This appendix describes those design features and functional capabilities identified in the assessment, and discusses how the identified design features and functional capabilities show that with reduced use of operator actions, the reactor core remains cooled and the containment remains intact, and spent fuel pool integrity is maintained. In the following discussion, the identified design features are designated as “key design features.”

19F.2 Scope

The evaluation of plant damage caused by the impact of a commercial aircraft is a complex analysis problem involving phenomena associated with structural impact, shock-induced vibration, and fire effects. The assessment of the aircraft impact also considers structural damage, such as that caused by the impact/penetration of hardened components (e.g., engine rotors, landing gear).

An assessment of the effects of aircraft fuselage and wing structure is also performed.

An assessment of the effects of shock-induced vibration on systems, structures, and components is performed.

An assessment of the impact/penetration of hardened aircraft components, such as engine rotors and landing gear is performed.

Perforation of analyzed structural components, including the containment vessel and the spent fuel pool liner, is not predicted; therefore, realistic assessments of the damage to internal systems, structures, and components caused by 1) burning aviation fuel and 2) secondary impacts are not required.

19F.3 Assessment Methodology

Methods described in NEI 07-13, Revision 7 (Reference 1) were followed to assess the effects on the structural integrity of the primary containment and spent fuel pool, and to assess the physical, fire, and vibration effects of the aircraft impact on the core cooling capability of the existing and enhanced design. In accordance with the recommendation set forth in subsection 2.4.1(4) of NEI 07-13, Revision 7, an analytical evaluation and experimental verification has been performed for the first of a kind steel-concrete modular design feature subjected to the aircraft impact loading.

19F.4 Results/Conclusions

A detailed aircraft impact assessment was performed for AP1000 in accordance with the guidance in NEI 07-13 (Reference 1). The assessment concludes that an aircraft impact would not inhibit AP1000’s core cooling capability, would not impact containment integrity, and would not impact spent fuel pool integrity based on best-estimate calculations.

The assessment resulted in the identification of the following design features and functional capabilities; changes to which are evaluated and reported in accordance with 10 CFR 50.150(d).

19F.4.1 Shield Building and Spent Fuel Pool

The shield building, as described in Chapter 3, is a key design feature for the protection of the safety systems located inside containment from the impact of a large commercial aircraft. The assessment concludes that a strike upon the shield building would not result in perforation of the shield building so damage to the containment vessel would not occur. Therefore, the systems and equipment within the containment vessel are not damaged from the impact or from exposure to jet fuel.

The assessment finds that safety-related components inside containment, including the reactor pressure vessel and passive core cooling system, remain intact and maintain their intended capabilities following the shock-induced vibrations resulting from the impact of a large commercial aircraft based on applying the methodology in Reference 1.

This assessment also concludes that a strike upon the auxiliary building would not result in loss of spent fuel pool liner integrity. Both the structural design of the shield building and the auxiliary building, as described in Chapter 3, are considered key design features.

19F.4.2 Site Arrangement

The assessment credits the design and arrangement of certain building features, depicted in Figures 3.7.2-12 and 3.7.2-19, to limit the effects of a potential aircraft impact on the auxiliary building. These key features are as follows:

- The design of the wall along the south end of the turbine building at column line 11.2, as described in Subsection 3.7.2.8.3, is a key design feature for the protection of the auxiliary building from the impact of a large commercial aircraft.

- The design of the wall along the east side of the annex building at column line E, as depicted in Figure 3.7.2-19, is a key design feature for the protection of the auxiliary building from the impact of a large commercial aircraft.

- The design and location of the spent fuel pool in the southern portion of the auxiliary building, as depicted in Figure 3.7.2-12 and described in Subsection 9.1.2.2, is a key design feature for the protection of the spent fuel from the effects of an impact of a large commercial aircraft. The spent fuel pool is located in area 6 of the auxiliary building. The spent fuel pool liner is protected from the east, south, and west by a minimum of 7 feet, 3 inches of concrete and from the north by the location of the shield building. Therefore, the liner is not impacted and the spent fuel pool integrity is maintained.

- The locations of the main control room (MCR), remote shutdown station, and secondary diverse actuation system (DAS) panel are a key design feature for the protection against the physical and fire damage resulting from the impact of a large commercial aircraft. The detailed aircraft impact assessment shows that an aircraft impact cannot destroy all three of these locations due to the number of barriers associated with these locations. The main control room is located in room 12401, the remote shutdown station is located in room 12303, and the secondary DAS panel is located in room 12554. The assessment determined that any impact scenario would not destroy all three of these locations, and from any one of these locations, passive safety injection and recirculation for long-term core cooling can be initiated.

Security-Related Information, Withhold Under 10 CFR 2.390d

- The design of the five oversized doors located on the east wall of room [ ]SRI, the east wall of room [ ]SRI, the shield building wall on the west side of room [ ]SRI, east wall of room [ ]SRI and the shield building wall on the west side of room]SRI are key design features for the protection against the physical and fire damage resulting from the impact of a large commercial aircraft. These doors and their connections to the walls are considered key design features because they are designed with a thickness that provides impact resistance equivalent to that of the wall. The doors at the east wall of room [ ]SRI, the shield building wall on the west side of room [ ]SRI, east wall of room [ ]SRI, and the shield building wall on the west side of room [ ]SRI are normally thicker than what is required for impact resistance due to radiation shielding. The door on the east wall of room [ ]SRI is calculated to have a thickness of at least 5" steel to meet the impact resistance requirement. The walls are considered key design features for protecting containment integrity and core cooling.

19F.4.3 Core Cooling and Containment Integrity

If necessary, core cooling can be maintained by actuating the passive safety injection portion of the Passive Core Cooling System (PXS) and Reactor Coolant System (RCS) as described in Section 6.3. The portions of the PXS and RCS required for safety injection are located inside containment and are key design features. Their location protects them from damage due to an aircraft impact because the containment vessel remains intact and has no structural damage. The following valves are key design features and need to actuate for passive safety injection and recirculation for long-term core cooling:

- ADS Stage 4 squib valves, RCS-V004A/B/C/D (3 of 4)
- In-containment refueling water storage tank (IRWST) injection line squib valves, PXS-V123A/B and PXS-V125A/B (1 of 4)
- Recirculation line squib valves, PXS-V118A/B and PXS-V120A/B (1 of 4)

The steel containment vessel is protected by the shield building and is a key design feature. Based on beyond design basis calculations, the steel containment vessel is not impacted as a result of an aircraft impact on the shield building. If necessary, containment integrity is maintained by portions of the Passive Containment Cooling System (PCS). Containment integrity is maintained via air-only cooling by the passive containment cooling system. As discussed in Section 19.40, with air-only cooling (without design basis cooling), containment failure within 24 hours is predicted to be highly unlikely.

For design basis accidents, containment cooling is provided by water cooling of containment. Water cooling is distributed onto the containment vessel by the PCS water distribution bucket located above the containment vessel. Although the water distribution bucket is predicted to be unnecessary following an aircraft impact, an assessment has been performed on the water distribution bucket and predicts the support structure to be intact.

Redacted Information, Withheld Under 10 CFR 2.390d

SRI

19F.4.4 Reactor Trip

The reactor trip equipment is a key design feature. This equipment includes the sensors and manual inputs, protection and safety monitoring system cabinets, and reactor trip switchgear as described in Subsection 7.2.1. In the event of an aircraft impact, it is likely that ac power will be lost. On a loss of ac power, the control rods are de-energized and fall by gravity into the reactor core. If ac power is not lost, plant shutdown will be controlled by the intact protection and safety monitoring system or initiated manually from the main control room, remote shutdown room, or reactor trip switchgear. Additionally, if PMS is not intact as a result of the impact, the reactor trip breakers will open due to undervoltage. This results in the control rods being de-energized and falling into the reactor core. If the reactor trip switchgear or rod drive motor-generator sets are not intact, the rods also are de-energized and fall by gravity into the reactor core.

19F.4.5 Supporting Power, Instrumentation, and Control Equipment

The supporting equipment for the main control room, remote shutdown station, and secondary DAS panel are key design features. These include the class 1E batteries, the supporting PMS control and instrumentation cabinets and cabling for the equipment identified in Subsection 19F.4.3, the transfer switch to isolate the MCR and transfer controls to the remote shutdown room, and the DAS cabling for the squib valve control cabinet. These key design features enable the actuation of safety injection through operation of the squib valves. The functional capabilities of the secondary DAS panel are described in Subsection 7.7.1.11 and is referred to as the DAS squib valve control cabinet. These key design features are protected by their spatial separation as described in Subsection 19F.4.2.

19F.4.6 Fire Barriers

The design and location of 3-hour fire barriers within the auxiliary building are key design features for the protection of equipment needed to manually actuate the systems and equipment potentially required for core cooling following the impact of a large commercial aircraft. The assessment credited the design and location of fire barriers (including doors), as described in Appendix 9A, to limit the effects of fire damage created by the impact of a large commercial aircraft. Penetrations through

specific barriers in the auxiliary building are rated to withstand a differential pressure of 5 psid based on the methodology in Reference 1. These barriers are identified in Subsection 9.5.1.2.1.1.

19F.5 References

1. NEI 07-13, Revision 7, “Methodology for Performing Aircraft Impact Assessments for New Plant Designs.”