Chapter 19 Probabilistic Risk Assessment and Severe Accidents

19.1 Introduction

This section describes the objectives of the design-specific Probabilistic Risk Assessment (PRA) and severe accident evaluations, and the corresponding regulatory requirements. This chapter is based upon the PRA model that represents the standard ESBWR design, and is thus considered to be the “Design Certification PRA.” The Design Certification PRA is used to develop the site-specific PRA, which is referred to as the “Site Baseline PRA.” Throughout this document, the “PRA” or “PRA model” are used in general terms to describe the general application of PRA. Distinctions between “Design Certification” and “Site Baseline” are made, as appropriate, to clarify specific applications.

19.1.1 Regulatory Requirements for PRA and Severe Accidents

Advanced nuclear power plant designs, like the ESBWR, are designed to achieve a higher standard of severe accident safety performance than previous designs. In an effort to provide this additional level of safety in the design of advanced nuclear power plants, guidance and goals have been developed for events that are beyond what is typically referred to as the design basis of the plant. For the ESBWR, severe accident issues are addressed during the design stage. This allows the design to take full advantage of the insights gained from such input as probabilistic risk assessments, operating experience, severe accident research, and accident analysis, by designing features to reduce the likelihood that severe accidents will occur and, to mitigate the consequences of severe accidents.

10 CFR Part 52, "Early Site Permits; Standard Design Certifications; and Combined Licenses for Nuclear Power Plants," requires that a design-specific PRA be submitted as part of an application for standard design certification. The ESBWR PRA is contained in Licensing Topical Report NEDO-33201, (Reference 19.1-1) which is docketed as part of the ESBWR DCD application.

Specifically, 10 CFR 52.47 requires an application for design certification to include the following:

- Demonstrate compliance with any technically relevant portions of the Three Mile Island (TMI) requirements given in 10 CFR 50.34(f).
- Propose technical resolutions of those unresolved safety issues and medium- and high-priority generic safety issues which are identified in the version of NUREG-0933 current on the date 6 months prior to application and which are technically relevant to the design.
- Contain a description of the design-specific PRA and its results.

Information on compliance with the TMI requirements is provided in Appendix 1A. Information on relevant unresolved safety issues is provided in Section 1.11.

This chapter provides an overview of the design-specific PRA. It also presents the assumptions and insights obtained from the PRA that are important to maintaining acceptable risk due to severe accidents in the ESBWR.

19.1.2 **Objectives**

The objectives of the plant-specific PRA and severe accident evaluations are to demonstrate that the ESBWR has been designed with state-of-the-art safety features, incorporating highly reliable and available passive safety functions with significant redundancy and diversity.

The design-specific PRA results and insights are compared against the following goals (note: these are goals and not regulatory requirements) and address how the plant features properly balance severe accident prevention and mitigation:

- Demonstrate how the risk associated with the design compares against the Commission's goals of less than 1E-4/yr for core damage frequency (CDF).
- Demonstrate how the risk associated with the design compares against the Commission's goals of less than 1E-6/yr for large release frequency (LRF).
- A deterministic goal that containment integrity be maintained for approximately 24 hours following the onset of core damage for the more likely severe accident challenges.
- A probabilistic goal that the conditional containment failure probability (CCFP) be less than approximately 0.1 for the composite of at-power core damage sequences assessed in the PRA.

In addition, the design-specific PRA process encompasses the following objectives:

- Identify and address potential design features and plant operational vulnerabilities, where a small number of failures could lead to core damage, containment failure, or large releases (e.g., assumed individual or common-cause failures could drive plant risk to unacceptable levels with respect to the Commission's goals, as presented above).
- Reduce or eliminate the significant risk contributors of existing operating plants that are applicable to the new design by introducing appropriate features and requirements.
- Select among alternative features, operational strategies, and design options.
- Identify risk-informed safety insights based on systematic evaluations of the risk associated with the design, construction, and operation of the plant such that the COL Holder can identify and describe the following:
    - The design's robustness, levels of defense-in-depth, and tolerance of severe accidents initiated by either internal or external events.
    - The risk significance of specific human errors associated with the design, including a characterization of the significant human errors that may be used as an input to operator training programs and procedure refinement.
- Assess the balance of preventive and mitigative features of the design, including consistency with the Commission's guidance in SECY-93-087 and the associated Staff Requirements Memorandum.

- Demonstrate whether the plant design, including the impact of site-specific characteristics, represents a reduction in risk compared to existing operating plants.
- Demonstrate that the design addresses known issues related to the reliability of core and containment heat removal systems at some operating plants (i.e., the additional TMI-related requirements in 10 CFR 50.34(f)).

The results and insights of the PRA are used to support other programs as follows:

- Support the process used to demonstrate whether the Regulatory Treatment of Non-Safety Systems (RTNSS) is sufficient and, if appropriate, identify the structures, systems, and components (SSCs) included in RTNSS.
- Support, as a minimum, regulatory oversight processes, and programs that are associated with plant operations, e.g., Technical Specifications, reliability assurance, human factors, and Maintenance Rule (10 CFR 50.65) implementation.
- Identify and support the development of specifications and performance objectives for the plant design, construction, inspection, and operation, such as an Inspections, Tests, Analyses and Acceptance Criteria (ITAAC); the Reliability Assurance Program (RAP); Technical Specification; and Combined License (COL) action items and interface requirements.

The ESBWR PRA uses the information that is available from the ESBWR plant design, Technical Specifications, and procedures at the time of the DCD application submittal. Component failure data and initiating event frequencies are based on generic industry data with consideration of the ESBWR design.

19.1.3 **Report Structure**

This chapter provides a summary of the ESBWR PRA results and insights. The most up to date PRA, reflecting the as-built, as-operated plant is developed (in appropriate phases) and retained by the COL Holder. It shall be available for NRC review when the information contained is used in risk-informed applications. Table 19.1-1 is a list of systems and functions modeled in the PRA.

Section 19.2 provides an overview of the ESBWR PRA and summarizes how the objectives are met. The overview includes a discussion of the uses of the PRA models, as well as PRA analysis of internal and external events for at-power and shutdown operating modes.

Section 19.3 summarizes the ESBWR design features for the prevention and mitigation of severe accidents. This section addresses the relevant portions of SECY-93-087, which contains the NRC's positions pertaining to evolutionary and passive Light Water Reactor (LWR) design certification policy severe accident issues. Preventive feature issues addressed in SECY-93-087 relating to the ESBWR include the following:

- Anticipated transient without scram (ATWS)
- Station blackout

- Fire protection
- Intersystem loss-of-coolant accident

Mitigative feature issues addressed in SECY-93-087 relating to the ESBWR include the following:

- Combustible gas control
- Core debris coolability
- High-pressure core melt ejection
- Containment performance
- Equipment survivability

Section 19.4 provides a description of the process and procedures that the COL Holder will use to maintain and update the PRA to ensure it reasonably reflects the as-built, as-operated plant, and its scope, level of detail, and technical adequacy are appropriate for the applications in which it is used.

The overall conclusions of the PRA and severe accident evaluations are presented in Section 19.5.

19.1.4 COL Information

None.

19.1.5 References

19.1-1 GE-Hitachi Nuclear Energy, “ESBWR Certification Probabilistic Risk Assessment,” NEDO-33201, Revision 6, October 2010.

Table 19.1-1 Systems and Functions Modeled (Sheet 1 of 3)

System	PRA Function
Basemat Internal Melt Arrest Coolability (BiMAC) Device	Mitigate potential core-concrete interaction. The Gravity-Driven Cooling System (GDCS) deluge valves provide a flow path from the GDCS pools to the BiMAC device upon initiation signal of high lower drywell temperature indicative of a core melt-through.
Balance of Plant Power Conversion	The preferred method of heat transfer following a transient including: Turbine Bypass Valves, Main Steam Lines, Circulating Water Pumps, Feedwater (FW) pumps, Condensate pumps.
Containment Isolation Valves	Isolate Breaks in Feedwater, Isolation Condenser System, Main Steam, or Reactor Water Cleanup/Shutdown Cooling Lines. Containment isolation valves close to limit radiological releases.
Containment Vent	When no containment heat removal system is available, the pressure in the containment will rise. The actuation of this function provides for containment pressure reduction by opening a venting path from the wetwell airspace that provides a scrubbed, controlled release of containment atmosphere to prevent or mitigate severe accidents.
Control Rod Drive (CRD) System	Rapid control rod insertion (scram). CRD Suction is taken from the condensate storage tank. CRD pumps supply high pressure makeup water to the reactor when the normal makeup supply (feedwater) is unable to prevent reactor water level from falling below the normal water range.
Diverse Protection System (DPS)	Provide diverse control signal for safety functions that could be affected by common cause failures of digital controls.
Drains	Floor drains and sumps are located in major buildings to remove process water and leakage to prevent flooding of components.
Fuel and Auxiliary Pools Cooling System (FAPCS)	Following an accident after the reactor has been depressurized to provide reactor makeup water for accident recovery. In this mode the FAPCS pump takes suction from the suppression pool and pumps it into the reactor vessel via Reactor Water Cleanup/Shutdown Cooling (RWCU/SDC) loop B and then Feedwater loop A. After successful Reactor Pressure Vessel (RPV) depressurization, FAPCS can accomplish the core cooling function when configured in the RPV injection mode. It is manually actuated and it is necessary to inhibit containment isolation signals if any are present. One of the FAPCS trains that is not operating in spent fuel pool cooling mode is placed in the suppression pool cooling mode as necessary during normal plant operation. Water drawn from the suppression pool is cooled and cleaned and then returned to the suppression pool in the suppression pool cooling mode of operation. This mode, without filter cleanup, is automatically initiated in response to a high suppression pool temperature signal and may be manually initiated following an accident. An additional motor-driven RPV makeup pump is capable of providing injection from the FPS tank to the FAPCS low pressure injection mode.
Feedwater System	Feedwater injection is successful if one of four feedwater pumps and one of four condensate pumps are available to supply water to the RPV during high or low pressure conditions.
Feedwater Runback	The feedwater pumps are run-back to zero flow to limit power production in the short term following the accident, in order to keep the pressure spike in the RPV within acceptable limits.

Table 19.1-1 Systems and Functions Modeled (Sheet 2 of 3)

System	PRA Function
Fire Protection System (FPS) Diesel and Motor Driven Pumps	Provide makeup for reactor water inventory control, Isolation Condenser/Passive Containment Cooling System(IC/PCCS) pool level control, and spent fuel pool make-up through connection to FAPCS.
Gravity-Driven Cooling System (GDCS)	GDCS provides emergency core cooling after any event that reduces the reactor coolant inventory. Once the reactor has been depressurized the GDCS is capable of injecting large volumes of water into the depressurized RPV to keep the core covered for at least 72 hours following a Loss-of-Coolant-Accident (LOCA). The GDCS injection function provides water from all three GDCS pools to the RPV via eight injection lines. If the RPV level decreases to 1 m above the top of the active fuel, squib valves are actuated in each of four GDCS equalizing lines. The open equalizing lines leading from the suppression pool to the RPV make long-term coolant makeup possible. An equalization valve delay time ensures that the GDCS injection function from the GDCS pools has had time to drain to the RPV and that the initial RPV level collapse as a result of the blowdown does not open the equalizing line.
Isolation Condenser System (ICS)	Removes post-reactor isolation decay heat with three out of four ICs operating and reduces reactor pressure and temperature to safe shutdown conditions. Automatic initiation of this function occurs on either low RPV water level, closure of Main Steam Isolation Valves (MSIVs), or high RPV pressure. Each ICS train contains a condensate reservoir that provides sufficient water to the RPV following a loss of feedwater to ensure that the setpoint for low vessel level injection is not reached.
Instrument Air, Service Air, High-Pressure Nitrogen Supply	Valve Motive Power.
Lower Drywell Hatches	The position of the lower drywell hatches must be controlled during shutdowns to ensure that they will close on demand to provide a containment flood-up boundary.
Nitrogen Inerting	Containment inerting is utilized to ensure that hydrogen and oxygen levels do not reach combustion levels.
Nuclear Boiler System	During an Anticipated Transient Without Scram (ATWS), RPV pressure is challenged by the unmitigated reactor power. Following a transient with loss of the power conversion system and ICS, RPV pressure rises, which causes one or more Safety Relief Valves (SRVs) to lift at their pressure setpoint. It is necessary for all lifted SRVs to reclose to prevent an inadvertent loss of coolant through a stuck-open relief valve. Manually depressurizes the RPV by opening SRVs to permit effective FAPCS injection to the RPV. Automatically or manually actuated SRVs and Depressurization Valves (DPVs) reduce reactor pressure to allow for low pressure injection. The Automatic Depressurization System (ADS) actuation logic initiates the depressurization.
Passive Containment Cooling System (PCCS)	The PCCS loops receive a steam-gas mixture supply directly from the drywell. The PCCS loops are initially driven by the pressure difference created between the containment drywell and the suppression pool during a LOCA and then by gravity drainage of steam condensed in the tubes. Enough water is present during operation to remove decay heat for at least 24 hours. A connection to the refueling well in the upper reactor building will automatically open to extend this inventory to at least 72 hours. PCCS vent fans are operated after 72 hours to redistribute the non-condensable gases from the wetwell to the drywell so that overall containment pressure is reduced.

Table 19.1-1 Systems and Functions Modeled (Sheet 3 of 3)

System	PRA Function
Plant Service Water System (PSWS)	Component Cooling
Power Distribution	Alternating current (AC) Power, Uninterruptible AC Power, direct current (DC) Power
Reactor Component Cooling Water System	Component Cooling for Reactor Building
Reactor Protection System (RPS)	The alternate rod insertion (ARI) function of the CRD system provides a backup means of actuating a hydraulic scram that is diverse and independent from the RPS logic and components. The same signals that initiate ARI simultaneously actuate the FMCRD motors to insert the control rods electrically. The RPS provides actuation logic for rapid control rod insertion (scram) so that no fuel damage results from any anticipated operational occurrence. Manual RPS actuation by the operators during an initiating event.
RWCU/SDC Mode	RWCU/SDC provides decay heat removal in response to transients. After an ATWS, RWCU/SDC is isolated to prevent filtering out boron. After an ATWS, RWCU/SDC may be manually restarted to supply shutdown cooling.
Standby Liquid Control (SLC) System	For ATWS events, the failure of control rods to insert in response to a valid trip demand is assumed and SLC automatically initiates. Operator action - failure to successfully control power during an ATWS.
Standby AC Power	Standby Diesel Generators, Ancillary Diesel Generators, and associated electrical buses.
Switchyard	The switchyard transmits AC power to and from the grid.
Turbine Component Cooling Water System	Provide component cooling for condensate and feedwater pumps.
Vacuum Breakers	The containment steam suppression function uses vacuum breakers that must be initially closed during the LOCA blowdown to allow steam condensation in the pool. Vacuum breakers must also subsequently open if drywell pressure decreases relative to the wetwell pressure to avoid negative pressure failures. Vacuum breaker is provided with redundant proximity sensors and temperature sensors to detect its closed position. PCCS effectiveness in containment heat removal requires that a pressure differential exist between the drywell and wetwell. To this end, the vacuum breakers between the drywell and wetwell must maintain this drywell-to-wetwell pressure differential. During a LOCA, the vacuum breakers open to allow the flow of gas from wetwell to drywell to equalize the wetwell and drywell pressure. If they subsequently do not completely close, as detected by proximity sensors or temperature sensors, a control signal will close the upstream isolation valves to prevent bypass leakage and therefore maintain the pressure suppression capability of the containment.

19.2 PRA Results and Insights

19.2.1 Introduction

This section provides an overview of the ESBWR PRA and a summary of the PRA results. The overview includes the internal and external events analyses, the shutdown PRA, the severe accident progression analysis and the offsite consequence analysis. The ESBWR PRA (Reference 19.1-1) is a full scope (Level 1, 2, and 3) PRA, that covers both internal and external events, for at-power and shutdown operations. Where applicable, ASME-RA-Sb-2005 (References 19.2-2 thru 19.2-4) capability category 2 attributes are included in the analysis. Obviously, some of these attributes are not achievable at the design certification stage of a nuclear power plant. For example, many aspects of assessing human actions cannot be analyzed in absence of a physical, operating plant and operation staff. In these cases, a bounding approach is taken to encompass all potential sites, configurations, and operating organizations. In addition, any analyses requiring site-specific characteristics that are not yet available are treated in a bounding manner.

In cases where detailed design information is not available, or when it can be shown that detailed modeling does not provide additional risk-significant information, bounding assumptions are made. Table 19.2-3 is a list of significant PRA insights and assumptions regarding how the design features affect the risk profile, and how uncertainties affect the PRA model in representing an estimate of the risks of the plant. A systematic method is used to identify PRA insights and assumptions, and to distinguish those that could have a significant effect on the PRA results if alternative assumptions were used. In order to ensure that this information is incorporated into the design process, the PRA insights and assumptions are categorized as follows:

Design Requirement: an assumption that requires specific design details be preserved to maintain its validity. If a future design change affects a design requirement, the PRA model is analyzed to determine the significance of the change. Each Design Requirement is referenced to an applicable section in the UFSAR.

Operational Program: an assumption that requires specific operational programs, such as procedures or training be preserved to maintain its validity. Development of operating and maintenance procedures is the responsibility of the COL Holder in accordance with COL Item 13.5-2-A. Other operational programs that address PRA insights and assumptions are the Maintenance Rule, Technical Specifications, and development of the Site Baseline PRA model.

Insight: an assumption that provides significant information about the PRA model or its results, but does not require design details or operational programs to maintain its applicability. Insights should be maintained in the Site Baseline PRA model development and should be considered when developing conclusions regarding risk-informed decisions.

In order to maintain a PRA model that reasonably reflects the as-built and as-operated characteristics of the plant, controls are implemented to develop the Site Baseline PRA, as described in Section 19.4.

19.2.2 Uses of PRA

19.2.2.1 Design Phase

The PRA supports the design through assessing risks using key parameters such as core damage frequency (CDF), large release frequency, and importance measures such as Fussell-Vesely and risk achievement worth (RAW) for major component functions. In particular, the ESBWR design certification PRA shows that the design meets the objectives stated in Section 19.1.

The ESBWR PRA defines potentially risk-significant SSC and operator errors that contribute to CDF and LRF using thresholds of Fussell-Vesely greater than or equal to 0.01, and RAW greater than or equal to 5.0 for individual basic events and a RAW greater than or equal to 50.0 for common cause failure events. The objective of the human reliability analysis and human factors engineering operational analysis in Chapter 18 is to ensure that the means are provided in the plant design to keep the quantitative risk importance of all potentially risk-important human interactions modeled in the PRA as low as practical. For the purpose of human reliability analysis, a human interaction with a Fussell-Vesely value greater than or equal to 0.01 or a RAW value greater than or equal to 5.0 is considered important to risk. This classification of risk-significance is consistent with the PRA. The human reliability analysis ensures that information for identifying, planning and implementing the needed action within the time permitted is provided in the design or is provided by automated support to carry out the needed action. For example, the operator can identify the need for manual actions through procedures and training and implement with tools as needed.

19.2.2.1.1 Use of PRA in Support of Design

In the design phase, various aspects of probabilistic analyses are employed to enhance the ESBWR and reduce the overall risk profile. At the conceptual design phase, qualitative risk analyses are used to ensure that vulnerabilities of existing boiling water reactors (BWRs) have been addressed in the ESBWR design.Table 19.2-1 contains a comparison of ESBWR design features versus design issues in BWRs.

The diversity and redundancy level of certain systems has been established, in part, by qualitative risk insights. Consistent with other conceptual design methods, the risk insights applied at the conceptual design phase are not explicitly documented in the PRA. Table 19.2-2 lists design features that have been applied to the conceptual design of the ESBWR to reduce risk. Extensive use of operating experience in the design phase has led to significant improvements, over conventional BWRs, in the plant's ability to respond to severe accidents. Significant design improvements include:

1. The ESBWR front-line safety functions are passive and, therefore, have significantly less reliance on the performance of supporting systems or operator actions. In fact, ESBWR does not require operator actions for successful event mitigation until 72 hours after the onset of an accident.

2. The ESBWR design reduces the reliance on alternating current (AC) power by using 72-hour batteries for several components. Diesel-powered pumping has been added as a diverse makeup system. The core can be kept covered without any AC sources for the first 72 hours following an initiating fault. This ability significantly reduces the consequences of a loss of preferred (offsite) power initiating fault.
3. ATWS events are low contributors to plant CDF because of the improved scram function and passive boron injection.
4. The ESBWR design reduces the frequency and consequences of LOCAs in large diameter piping by removing the recirculation system altogether.
5. The design of the ESBWR reduces the possibility of a LOCA outside the containment by designing, to the extent practical, all piping systems, major system components (pumps and valves) and subsystems connected to the reactor coolant pressure boundary (RCPB) to an ultimate rupture strength at least equal to the full RCPB pressure.
6. The probability of a loss of containment heat removal is significantly reduced because the PCCS is highly reliable due to redundant heat exchangers and passive component design.
7. The ESBWR is designed to minimize the effects of direct containment heating, ex-vessel steam explosions, and core-concrete interaction. The ESBWR containment is designed to a higher ultimate pressure than conventional BWRs.

Insights from the ESBWR PRA have already been used to implement several design enhancements. The following is a summary of several PRA-based changes that have been incorporated into the ESBWR design, and consequently, have contributed to a significant improvement in nuclear safety:

1. Added redundant, physically separated flow paths to the low pressure injection and suppression pool cooling lines in response to fire analysis.
2. Determined the loads to be served by the DPS, which supplies diverse control signals to safety functions.
3. Improved the design of digital controls to reduce the likelihood of inadvertent actuation of specified systems.
4. Added redundant supply valves for IC/PCCS pool makeup.
5. Added redundant drain line valves for ICS to eliminate a dependency on power supplies.
6. Changed the routing of fire suppression piping to reduce the likelihood of room flooding.
7. Determined the appropriate placement of control and instrumentation cabinets and power supplies to ensure physical separation.
8. Added the BiMAC device to reduce the consequences of severe accidents.

During the initial design, formal risk assessment methods are employed to ensure that the risk goals are met and to enhance the safety in the design. This analysis is submitted in a topical report as part of the design certification of the ESBWR. In addition, the design certification PRA is used to:

- Identify the systems that should have enhanced regulatory oversight (Appendix 19A).
- Provide an independent assessment of the set of surveillance intervals and allowed outage times in the technical specifications (Chapter 16).
- Identify the most important operator action categories in support of the man-machine interface (Chapter 18).
- Assist in identifying the most appropriate level of defense-in-depth and diversity for the instrument and control systems (Chapter 7).

Finally, the design team has used the PRA to assist in reducing the likelihood of accidents and transients and to enhance operational performance.

19.2.2.1.2 Consideration of Potential Design Improvements

Potential design improvements have been identified, in a systematic method, and evaluated on a cost-benefit basis. The evaluation is documented in topical report NEDO-33306 (Reference 19.2-5), and has determined that there are no practical and cost-beneficial design enhancements that should be considered.

19.2.2.2 COL Application Phase

19.2.2.2.1 Use of PRA in Support of COL Holder Programs

The PRA in the COL phase is used in support of COL Holder programs such as the maintenance rule, the human factors engineering program (Chapter 18), and the severe accident management program.

19.2.2.2.2 Risk-Informed Applications

No risk-informed applications are being implemented in the COL application.

19.2.2.3 Construction Phase

19.2.2.3.1 Use of PRA in Support of COL Holder Programs

The PRA in the Construction phase is used in support of COL Holder programs, such as the maintenance rule, the human factors engineering program (Chapter 18), and the severe accident management program.

19.2.2.3.2 Risk-Informed Applications

There are no plans for risk-informed applications to be implemented in the construction phase.

19.2.2.4 Operational Phase

19.2.2.4.1 Use of PRA in Support of COL Holder Programs

The PRA in the operational phase is used in support of COL Holder programs, such as the maintenance rule, the human factors engineering program (Chapter 18), interface with the reactor oversight program, and the severe accident management program. The reactor oversight program relies on the plant-specific PRA model that is maintained by the COL Holder.

19.2.2.4.2 Risk-Informed Applications

There are no plans for risk-informed applications to be implemented in the operational phase.

19.2.3 Evaluation of Full Power Operations

The focus of this subsection is to provide the insights of the plant-specific PRA for full power operations for internal and external events.

19.2.3.1 Risk from Internal Events

Identification of Internal Initiating Events

Internal initiating events are those events that occur either as a direct result of equipment failure, or as the result of errors while performing maintenance, testing, or other operator actions. These events occur during normal power operations. The DCD PRA uses generic initiating event frequencies based on operating plant history. These are considered to be bounding for the ESBWR. No attempt is made in this report to reduce the generic frequencies by taking into account ESBWR-specific scram reduction features or the enhanced reliability of mechanical and control systems.

Individual initiating events are grouped into categories that cause the same plant response. The initiating event categories are identified below.

- Transients
  - General Transient
  - Loss of Feedwater
  - Loss of Preferred Power
  - Loss of the Plant Service Water system
  - Inadvertent Opening of a Relief Valve
- LOCAs

  LOCAs are divided into different classes based on the size and elevation of the break. In particular, the breaks in the reactor coolant pressure boundary have been classified with respect to location as follows:

- Liquid breaks for pipes connected to the RPV above the top of fuel
- Steam breaks for pipes connected to the RPV above the top of fuel
- Breaks in pipes connected to the vessel below the top of fuel

The sizes of the breaks are classified as follows:

- Large breaks fully depressurize the plant through the break alone
- Small and medium breaks require SRVs or DPVs to fully depressurize
- Small liquid breaks can be mitigated with CRD as the only injection source
- Medium liquid breaks are larger than CRD capacity
- Breaks Outside Containment in lines containing the reactor coolant pressure boundary
- Interfacing Systems LOCA

• ATWS

ATWS events are not unique initiating events, but are extensions of transients with a subsequent failure to scram.

In some cases, applicable initiating events are grouped with other initiating events that elicit a similar plant response. The General Transient category consists of initiating events that result in a reactor trip and are caused by nonsafety-related systems that involve power productions. For example, the Transient with the Power Conversion System Unavailable, and the Transient due to Complete Loss of Air Systems are grouped with the Loss of Feedwater Transient for this reason. Also, the Interfacing Systems LOCA initiating event is grouped with the Break Outside Containment in Feedwater Line A initiator.

Acceptance Criteria for Internal Events

The acceptance criteria for the critical safety functions that are used in analyzing safe plant operation are described below:

• Reactivity Control
  - The acceptance criterion is to achieve sub-criticality and maintain the reactor in a sub-critical state.

• RPV Overpressure Protection
  - A pressure of 150 percent of the reactor coolant pressure boundary design pressure is defined as the acceptance criterion for the RPV overpressure protection.

• Core Cooling
  - A peak cladding temperature of 1200°C (2200°F) is defined as the criterion for establishing the adequacy of core cooling.

- Containment Heat Removal
  - The acceptance criterion for the containment cooling function is to maintain the pressure below the ultimate containment failure pressure, which is provided in Appendix 19C.

Core damage is assumed to occur directly from conditions that challenge the core cooling acceptance criterion, and indirectly due to conditions that challenge the other criteria.

Event Tree Development of Internal Events

The event tree methodology is used to represent the possible sequences of events following any one of the initiating event groups defined above. Each event tree sequence depicts a possible combination of system and operator action successes or failures leading to either a successful cooling of the core or to core damage according to the acceptance and success criteria. The event trees developed in the ESBWR internal events PRA are:

- General Transient
- Loss of Feedwater Transient
- Loss of Preferred Power Transient
- Loss of Service Water System
- Inadvertent Opening of a Relief Valve
- ATWS from Generic Transient
- ATWS from Transient with Loss of Feedwater System
- ATWS from Transient with Loss of Preferred Power
- ATWS from Transient with Loss of Service Water System
- ATWS from Inadvertent Opening of a Relief Valve
- ATWS from Transient with LOCA
- Large Steam LOCA
- Large LOCA on Feedwater Line A
- Large LOCA on Feedwater Line B
- Medium Liquid LOCA
- Small and Medium Steam LOCA
- Small Liquid LOCA
- Reactor Vessel Rupture
- Break Outside of Containment on Main Steam Lines
- Break Outside of Containment on Feedwater Line A
- Break Outside of Containment on Feedwater Line B

- Break Outside of Containment on RWCU/SDC Line
- Break Outside of Containment on Isolation Condenser Line

Systems Analysis of Internal Events

As part of the systems analysis, fault trees are developed for all the safety-related systems and several nonsafety-related systems whose operation could mitigate the effects of an accident. The fault tree analysis provides modeling of the major components in the plant. Failures on demand and during the mission of the component are both modeled. Common cause failure is treated for components used in redundant applications. The human actions that are modeled include both pre-initiator failures and post-initiator failures. Test and maintenance unavailability is also included explicitly in the systems analysis. Table 19.1-1 provides a list of the systems and functions that are included in the PRA model.

19.2.3.1.1 Significant Core Damage Sequences of Internal Events

There are important commonalities in the dominant accident sequences that play a key role in contributing to core damage. In addition to requiring a scram, each initiating event in the dominant sequences causes a loss of a key mitigating function. For example, Feedwater injection is unavailable in a Loss of Feedwater initiating event, and an inadvertent opening of a relief valve event indirectly results in the loss of the ICS. The dominant sequences typically do not contain multiple independent component failures. Instead, they consist of common cause failures that disable entire mitigating functions. And, it is important to note that multiple mitigating functions must fail in the dominant sequences, so a single common cause event is insufficient to directly result in core damage. The ATWS sequences are dominated by an assumed failure of the control rods to insert into the core due to mechanical binding. Core damage in ATWS accident sequences results from the inability to maintain a lowered RPV water level prior to achieving subcriticality. While the DPVs are challenged in a majority of the accident sequences, they are successful in most cases.

Important operator actions involve recognizing the need for depressurization or providing low pressure injection in particular scenarios and recognizing the need to make up to the IC/PCCS pools. Information on important operator actions is incorporated into the human factors engineering program, as discussed in Subsection 19.2.2.1.

The dominant sequences are described below, on a functional level. This distillation of the PRA accident sequences is intended to represent the important insights that represent the behavior of the ESBWR design in response to postulated accidents.

- General Transient with ATWS
    - Scram fails
    - SLCS fails
- Inadvertent Opening of a Relief Valve

  - Scram is successful
  - High Pressure Injection fails
  - Depressurization is successful
  - Low Pressure Injection fails
- Inadvertent Opening of a Relief Valve
  - Scram is successful
  - High Pressure Injection fails
  - Depressurization fails
- Medium Liquid LOCA
  - Scram is successful
  - Vacuum Breakers Pressure Suppression is successful
  - Depressurization is successful
  - Low Pressure Injection fails
- General Transient with ATWS
  - Scram fails
  - One or more SRVs sticks open
  - Failure to maintain RPV water level
- Medium Liquid LOCA
  - Scram is successful
  - Vacuum Breakers Pressure Suppression is successful
  - Depressurization is successful
  - Low Pressure Injection fails
- Medium Liquid LOCA
  - Scram is successful
  - Vacuum Breakers Pressure Suppression is successful
  - Depressurization fails
- Small Steam LOCA
  - Scram is successful
  - Vacuum Breakers Pressure Suppression is successful
  - Depressurization is successful
  - Low Pressure Injection fails

  - CRD Injection fails
- Small Liquid LOCA
  - Scram is successful
  - Isolation Condensers are successful
  - Depressurization is successful
  - Vacuum Breakers Pressure Suppression is successful
  - Low Pressure Injection fails
  - CRD Injection fails
- Small Steam LOCA
  - Scram is successful
  - Feedwater isolates on High Drywell Pressure
  - Automatic and Manual Depressurization fail
  - CRD Injection fails

19.2.3.1.2 Significant Large Release Sequences of Internal Events

The ESBWR has a low potential for generating large releases. The sequences that would have this result are unlikely and involve large uncertainties. Therefore a bounding, rather than best estimate, method is used for assessing containment performance.

The Risk Oriented Accident Analysis Methodology (ROAAM) has been developed for the purpose of resolving containment performance issues that are difficult to address in a purely probabilistic framework. Principal ingredients of ROAAM include: (a) identification of uncertainties; (b) conservative treatment of uncertainties in parameters and scenarios that are beyond the reach of any reasonably verifiable quantification; and (c) the use of external experts in a review, rather than in a quantification capacity.

Three phenomena are important for the ESBWR containment. These are ex-vessel steam explosions, ex-vessel debris cooling, and long term containment over pressurization.

In the ESBWR, ex-vessel steam explosions (EVE) originating in deep (> 2.0 m [6.6 ft]) subcooled pools of water in the lower drywell can potentially challenge the containment. Ex-vessel phenomena in shallow or saturated pools do not generate loads sufficient to affect the containment, so the ESBWR design is optimized to minimize the water that accumulates in the lower drywell while the core is retained in the reactor pressure vessel. Emergency operating procedures are optimized to preserve this feature.

The sequences that can lead to significant EVE involve medium liquid LOCAs or breaks in pipes connected to the vessel below the elevation of the core. The ROAAM analysis does not place significance on the details of how the LOCA proceeds to the EVE, but significant sequences can be

inferred from the Level 1 results. The significant sequence for EVE starts as a medium liquid LOCA (e.g., GDCS line break), followed by successful reactor scram, and all injection systems fail to keep the core covered. The LOCA itself causes the deep pool of water in the lower drywell. Eventually, the core relocates to the lower plenum of the reactor vessel and proceeds to drop into the water pool in the lower drywell. The resulting steam explosion is sufficient to challenge the integrity of the containment. Under the ROAAM process, this challenge is conservatively treated as a containment failure.

Ex-vessel debris coolability has been studied for many years, yet there remain considerable uncertainties as to which configurations are coolable by an overlying pool of water and which are not. ESBWR design includes the BiMAC to eliminate the uncertainties of ex-vessel coolability. This feature is described in Subsection 19.3.2.6.

The only significant potential for release due to ex-vessel coolability phenomena is associated with the uncertainty of the thermal performance of the BiMAC device. As in the EVE discussion, the details of the sequences that lead to this type of release are not relevant. This phenomena is applicable to all severe accident sequences, so the important level 1 sequences described in Subsection 19.2.3.1.1 are applicable here as well. In these postulated events, it is assumed that significant core concrete interaction occurs in spite of the BiMAC device. The containment could fail due to the generation of non-condensable gasses or later by erosion of the basemat by the core debris. In either case, the release would occur very late following core damage.

The final important phenomenon is the over-pressurization of the containment due to system failures. For this phenomenon there is some dependence on the core damage sequence progression because of common support systems for the containment functions. The general accident sequence for over pressurization begins with a transient with successful scram, failure of ICS, and failure of high pressure injection such that depressurization is required, but is not successful. Eventually, the water in the core boils away and the core melts. The result is a high pressure melt eject event, which does not provide any significant challenge to the containment, but the containment heat removal functions are required for long term cooling. The containment ultimately fails or is vented when the containment pressure exceeds the ultimate strength (Appendix 19C). In either case, a large release is assumed to occur, but beyond 24 hours following a representative over-pressure event.

Finally, because the overall CDF is very low, certain events that have historically been treated as negligible are found to have a small, but relatively measurable contribution to LRF due to the failure of passive design features.

The most important large release initiating events are %ML-L and %LL-S-FDWB, which represent a Medium Liquid LOCA and a Large LOCA in Feedwater Line B. This is due to the impact the LOCAs have on mitigating functions that become disabled.

19.2.3.1.3 Significant Offsite Consequences of Internal Events

The offsite consequence analysis for each source term is calculated and the results are multiplied by the annual release frequency for each source term, and then summed to obtain the risk-weighted mean consequence results. Based on this process, the whole-body dose at 805m (0.5 mile) over the entire dose spectrum from 0.1 Sv (10 rem) to >100 Sv (10,000 rem) is well below 1E-6/yr.

19.2.3.1.4 Summary of Important Results and Insights of Internal Events

The risk due to internal events is several orders of magnitude lower than the NRC safety goals that are discussed above. The internal events risk profile is balanced, such that there are no initiating events, component failures, or operator actions that dominate the results. The accident sequences with the highest risk typically consist of failures of multiple mitigating systems, so that there is no single component failure or single common cause failure that leads directly to core damage.

The ESBWR front-line safety functions are passive and, therefore, have significantly less reliance on the performance of supporting systems or operator actions. In fact, ESBWR does not require operator actions for successful event mitigation until 72 hours after the onset of an accident. The ESBWR design reduces the reliance on AC power by using 72-hour batteries for several components. Diesel-driven pumping has been added as a diverse makeup system. The core can be kept covered without any AC sources for the first 72 hours following an initiating fault. This ability significantly reduces the consequences of a loss of preferred (offsite) power initiating fault.

ATWS events are low contributors to plant CDF because of improvements in the scram function and passive boron injection.

The ESBWR design reduces the frequency and consequences of LOCA due to large diameter piping by removing the recirculation system altogether.

The probability of a loss of containment heat removal is significantly reduced because the PCCS is highly reliable due to redundant heat exchangers and passive component design.

19.2.3.2 Risk from External Events Evaluation of External Event Fire

19.2.3.2.1 External Event Fire

The probabilistic fire analysis is performed taking into account that the specifics of cable routings, ignition sources, and target locations in each zone of the plant are not known at this stage of the plant design. Because of this limitation, a simplified conservative and bounding approach is used in this analysis. For example, the probabilistic fire analysis assumes the worst effects of fire on all the equipment and systems located in each group of fire areas, that is, any fire in any fire area will cause the worst damage, and a fire ignition in any fire area continues to grow unchecked into a fully-developed fire without credit for fire suppression. The results of the analysis show that CDF due to fire is a low contributor to ESBWR core damage risk.

The fire risk analysis uses the same PRA models as the internal events evaluation. The specific fire location determines which of the internal events sequences are applicable. These are modified to take into account the effects of specific fires and include the possibility of fire propagation through potentially failed fire barriers. Bounding fire initiating event frequencies are used in the analysis, consistent with the nature of the fire analysis.

Significant Core Damage Sequences of External Event Fire

There are no fire-initiated core damage sequences that have a significant contribution to CDF. Typical fire accident sequences result in the loss of one division of SSCs and a transient initiating event with a very low CDF. Even when the failure of fire barriers is considered, the CDF values for fire accident sequences are not significant.

The most important fire-induced initiated events involve fires in the cable tunnels that disable either Plant Investment Protection (PIP)-A or PIP-B control signals and power supplies. Postulated fire propogation between the N-DCIS A room and the DPS room also has a relatively higher contribution because it disables both the PIP-A and DPS controls. Other noteworthy fire-induced initiating events include the fires in the switchyard that result in loss of preferred power, and in the Reactor Building that disable Division I or II electrical equipment.

The analysis of fire in the control room assumes that the fire forces control room evacuation; as such, no credit is given to manual actuations that must be performed from within the control room. However, it is assumed that automatic signals are not affected because they are generated in panels located outside the control room.

Recovery of the actuation of certain systems is credited due to the existence of remote shutdown panels located outside the control room. However, the operators are not required to perform any actions at the remote shutdown panels; the plant proceeds to a safe shutdown without the need for operator intervention. If automatic actuations fail, the operators may manually perform the necessary actuations from the remote shutdown panels.

Significant Large Release Sequences of External Event Fire

The calculated large release frequency for fire-initiated events is also very low. The important fire sequences do not challenge any of the passive containment cooling systems or the BiMAC.

Significant Offsite Consequences of External Event Fire

The estimated offsite consequences due to external events under at-power and shutdown conditions are less than the defined dose limits.

Summary of Important Results and Insights of External Event Fire

The main conclusion that can be drawn from the ESBWR probabilistic internal fires analysis is that the risk from internal fires is acceptably low. The estimated CDF for each of the analyzed scenarios, even when using a conservative analysis, is lower than the internal events CDF.

The ESBWR is inherently safe with respect to internal fire events. All potential fires have been analyzed and it has been shown that the plant can be safely shut down at low risk to plant personnel and the general public.

19.2.3.2.2 Evaluation of External Event Flood

Introduction

The objective of the ESBWR internal probabilistic flood analysis is to identify and provide a quantitative assessment of the CDF due to internal flood events. It models potential flood vulnerabilities in conjunction with random failures modeled as part of the internal events PRA. Through this process, flood vulnerabilities that could jeopardize core integrity are identified.

The floods may be caused by large leaks due to rupture or cracking of pipes, piping components, or water containers such as storage tanks. Other possible flooding causes are the operation of fire protection equipment and human errors during maintenance.

The internal probabilistic flood analysis is performed taking into account that piping layout specifics are not known. Therefore, a simplified probabilistic flooding approach is employed using general design assumptions to identify potential flooding vulnerabilities.

Significant Core Damage Sequences of External Event Flood

The most important flood sequences involve leaks in the Turbine Building – Main Condenser area, the Electrical Building general area, the Turbine Building's first floor, and Service Water Pumphouse. The cutsets associated with these sequences involve the common cause software failures on the digital control systems, and failures of the same single components that disable the AC power supplies or the IC/PCCS pool makeup.

Operator actions are not significant contributors to the full power internal flooding risk profile.

During the initial phase of the ESBWR design, a significant flood risk in the Control Building due to a break in Fire Protection System pipes was identified. Based on this PRA insight, the design specifications now require that the FPS pipes and fire hose stations are located in the Control Building stairwells and the standpipes are located external to the Control Building such that a piping failure does not result in a significant flood.

Significant Large Release Sequences of External Event Flood

The important flooding sequences do not impose additional challenges to any of the passive containment cooling systems or the BiMAC. Therefore the internal events containment performance insights can be directly used for external event flood sequences.

Significant Offsite Consequences of External Event Flood

The estimated offsite consequences due to external events under at-power and shutdown conditions are less than the defined individual, societal, and radiation dose limits.

Summary of Important Results and Insight of External Event Flood

Due to the low CDF and LRF values for flooding events, there are no additional results or insights.

19.2.3.2.3 Evaluation of External Event High Wind

Introduction to Evaluation of External Event High Wind

The ESBWR high wind analysis explicitly quantifies accident sequences initiated by hurricanes and tornado winds. Straight winds are lesser velocity winds that pose minimal challenges to the plant design. Due to the strength of construction of the ESBWR Category I buildings, the effects of high winds are limited to Loss of Preferred Power events with a potential loss of the Condensate Storage Tank. Overall risk from high winds is further minimized by design features such as the motor driven pump, powered by the ancillary diesel generator, for alternate RPV injection, and the direct current (DC) batteries with a 72-hour operational life.

Significant Core Damage Sequences of External Event High Wind

The high winds at-power risk assessment does not produce significant core damage sequences or insights that are different than the internal events at-power loss of preferred power results.

Significant Large Release Sequences of External Event High Wind

Due to the low CDF value and because the high winds do not affect any containment systems, high wind-induced external events do not result in any additional significant contributors to large release frequency.

Significant Offsite Consequences of External Event High Wind

The estimated offsite consequences due to external events under at-power and shutdown conditions are less than the defined individual, societal, and radiation dose limits.

Summary of Important Results and Insights of External Event High Wind

Due to the low CDF and LRF values for high wind events, there are no additional results of significance. There is one insight from the analysis that is included below in the shutdown risk discussion.

19.2.3.2.4 Evaluation of External Event Seismic

Introduction to Evaluation of External Event Seismic

The seismic risk analysis is performed to assess the impacts of seismic events on the safe operation of the ESBWR plant. A PRA-based seismic margins analysis is performed for the ESBWR to calculate high confidence low probability of failure (HCLPF) accelerations for important accident sequences and accident classes. The seismic margin earthquake for the PRA-based seismic margin assessment for ESBWR is the ESBWR Certified Seismic Design Response Spectra (CSDRS). The ESBWR seismic margins HCLPF accident sequence analysis concludes that the ESBWR is inherently capable of safe shutdown in response to beyond design basis earthquakes and has a plant level HCLPF of at least 1.67 times the peak ground acceleration of a safe shutdown earthquake (SSE), where SSE is the ESBWR CSDRS, in compliance with SECY 93-087 (Reference 19.2-7) requirement *"PRA insights will be used to support a margins-type assessment of seismic events. A PRA-based seismic margins 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."*

Table 19.2-4 contains the systems evaluated in the ESBWR and contains minimum HCLPF ratio for these systems.

Significant Core Damage Sequences of External Event Seismic

A PRA-based Seismic Margins Analysis is used to derive seismic vulnerability insights. The COL Holder will identify a milestone for completing a comparison of the as-built SSC HCLPFs to those assumed in the ESBWR seismic margin analysis shown in Table 19.2-4. Deviations from the HCLPF values or other assumptions in the seismic margins evaluation shall be analyzed to determine if any new vulnerabilities have been introduced. A minimum HCLPF value of 1.67*SSE will be met for the SSCs identified in Table 19.2-4 (COL 19.2.6-1-A). Therefore, there are no CDF calculations performed. The Seismic Margins Analysis concludes that the most significant HCLPF sequences are seismic-induced loss of DC power and seismic-induced ATWS due to seismic-induced failure of the fuel channels and seismic-induced failure of the SLC tank.

Based on previous industry seismic analyses, seismic risk is dominated by seismic-induced SSC failures, and not by random SSC failures or human actions. Human actions are typically not necessary until the long-term. **[START COM 19.2-001]** As-built SSC High Confidence Low

Probability of Failures (HCLPFs) will be compared to those assumed in the ESBWR seismic margin analysis shown in Table 19.2-4. Deviations from the HCLPF values or other assumptions in the seismic margins evaluation will be analyzed to determine if any new vulnerabilities have been introduced. This comparison and analysis will be completed prior to fuel load. **[END COM 19.2-001]**

Significant Large Release Sequences of External Event Seismic

A PRA-based Seismic Margins Analysis is used to derive seismic vulnerability insights. Therefore, there are no LRF calculations performed.

Significant Offsite Consequences of External Event Seismic

A PRA-based Seismic Margins Analysis is used to derive seismic vulnerability insights. Therefore, there are no off-site consequence calculations performed. Due to the bounding method that is used to calculate the seismic margin, it is considered to be unnecessary to extrapolate offsite consequences.

Summary of Important Results and Insights of External Event Seismic

The ESBWR seismic margins HCLPF accident sequence analysis highlights the following results regarding the seismic capability of the ESBWR:

- The ESBWR is inherently capable of safe shutdown in response to strong magnitude earthquakes.
- The most significant HCLPF sequences are seismic-induced loss of DC power and seismic-induced ATWS due to seismic-induced failure of the fuel channels and seismic-induced failure of the SLC tank.

19.2.4 Evaluation of Other Modes of Operation – Shutdown

The focus of this subsection is to provide the qualitative results and insights of the plant-specific PRA for the shutdown mode of operation. The internal events model covers operations in Modes 1 through 4 (Power Operation, Startup, Hot Shutdown, Stable Shutdown). The shutdown model covers Modes 5 and 6 (Cold Shutdown and Refueling). A detailed PRA is performed to determine the CDF during shutdown. Loss of the Reactor Water Cleanup/Shutdown Cooling System, Loss of Reactor Component Cooling Water System, Loss of Plant Service Water System, and Loss of Preferred Power are all investigated. Additionally, the CDF due to drain-down of the RPV or LOCAs during shutdown is evaluated. Fault trees and event trees are used to determine the shutdown CDF for each event analyzed. The evaluation encompasses plant operation in shutdown modes. This evaluation addresses conditions for which there is fuel in the RPV. It includes the NSSS and systems that support operation of the NSSS.

19.2.4.1 Significant Core Damage Sequences During Shutdown Mode

19.2.4.1.1 Internal Events During Shutdown

The greatest contribution to shutdown risk comes from breaks in lines connected to the vessel below TAF. In these cases, the lower drywell equipment hatch or personnel hatch is likely to be open to facilitate work in the lower drywell. Although the frequency of these events is very low, there is only one method for mitigation – manual closure of the hatch(es).

Besides lower drywell LOCA events, RPV draindown events have the next largest impact on the shutdown PRA results. The significant cases for draindown events result in RWCU isolation due to the leak, followed by a failure to provide alternate decay heat removal. The highest contributing RPV draindown cases are during Mode 6 Unflooded.

The most important operator actions in the ESBWR shutdown analysis are to close the lower drywell hatches upon the detection of a break in the reactor coolant system (RCS), and failure to recognize the need for low pressure makeup after depressurization.

Random failures of individual SSCs are not significant contributors to internal events during shutdown CDF.

19.2.4.1.2 Fire During Shutdown

The most important fire-initiated shutdown events are loss of RWCU/SDC due to fire in Turbine Building – Modes 5, 5 Open and 6-Unflooded; and, loss of preferred power due to fire in the switchyard – Modes 5, 5 Open and Mode 6-Unflooded.

There are two additional operator actions that are important for Shutdown external events, both of which involve fire-initiated events. They involve failure to initiate CRD injection, and failure to open two SRVs for depressurization.

19.2.4.1.3 Flooding During Shutdown

The most important flood-initiated shutdown events are a break in the Makeup Water System at the Reactor Building elevation 17500 mm during Modes 5 and 5 Open; a break in the Fire Protection System in the Turbine Building; and, Service Water Building PSW Line Break. Similar to the at-power flooding PRA, operator actions are not significant contributors to the shutdown internal flooding risk profile. Accounting for this conservatism and the low CDF and LRF values, there are no significant PRA results or insights from flooding during shutdown.

19.2.4.1.4 High Winds During Shutdown

Similar to the full power risk profile, the shutdown risk for high winds are limited to Loss of Preferred Power events with a potential loss of the Condensate Storage Tank. The high winds shutdown risk assessment does not produce significant core damage sequences or insights that are different than the internal events shutdown loss of preferred power results.

Operator actions are non-significant contributors to the shutdown high wind risk profile. Random failures of systems, structures or components are not significant contributors to the internal events shutdown CDF.

It is assumed that the plant is not in a Mode 6 Unflooded condition when a hurricane strike occurs. There is sufficient time, prior to a hurricane strike, for transitioning to another mode so that long term cooling is more available. In Mode 6 Unflooded, the containment is open, the reactor vessel is open and the water above the core will not keep the core cool for an extended period of time without additional mitigating systems.

19.2.4.1.5 Seismic Events During Shutdown

Similar to the full power risk profile, seismic risk during shutdown is dominated by seismic-induced SSC failures, and not by random SSC failures or human actions.

19.2.4.1.6 Shutdown PRA Assumptions

Compared to the Residual Heat Removal System in BWRs, the RWCU/SDC in the ESBWR does not have the potential for diverting RPV inventory to the suppression pool through the suppression pool suction, return, or spray lines.

The arrangement for preventing vessel draining through the design of the control rod drive mechanism (CRDM) is the same as the one used in the ABWR. Therefore, the ESBWR design does not introduce a new challenge to vessel inventory relative to CRDMs.

It is assumed that both RWCU/SDC trains are running, because the time periods in which only one is running occurs when the reactor well is flooded. Consequently, failure of one of the trains is not considered an initiating event.

Any break above level L3 does not constitute an initiating event, as RWCU/SDC will continue to ensure normal core cooling.

19.2.4.2 Significant Large Release Sequences of Shutdown Mode

Because the majority of the shutdown CDF occurs during times when the containment is open, shutdown modes are not analyzed for large release frequency. Shutdown core damage events can be conservatively assumed to be large releases.

19.2.4.3 Significant Offsite Consequences of Shutdown Mode

Due to the bounding method that is used to calculate shutdown CDF and LRF, it is considered unnecessary to extrapolate offsite consequences. The source terms for containment bypass events may not fall below the early fatality threshold until approximately eight days after shutdown; however, the frequency of shutdown containment bypass events is very low. As a result the offsite consequences, which are the product of the source term risk and the shutdown containment bypass frequency, are not significant.

19.2.4.4 Summary of Important Results and Insights of Shutdown Mode

The greatest contribution to shutdown risk in the internal events PRA comes from breaks in lines connected to the vessel below TAF. In these cases, the lower drywell equipment hatch or personnel hatch is likely to be open to facilitate work in the lower drywell. Although the frequency of these events is very low, there is only one method for mitigation – manual closure of the hatches. The dominant risk contributor with respect to shutdown modes is “Mode 6 Unflooded.” This is consistent with the baseline shutdown CDF results since the isolation condenser system is not credited in the Mode 6 Unflooded event trees. Therefore, it is necessary to ensure the operability of the systems critical to the decay heat removal function during this mode.

Shutdown risk due to external events is considered to be less significant due to the bounding approaches that are used in the fire, flooding and high winds assessments. For example, no credit is taken for operator intervention to mitigate fires or isolate flooding sources. The CDF and LRF values for these events are very low; therefore, there are no significant PRA results or insights from shutdown external events.

19.2.5 Summary of Overall Plant Risk Results and Insights

The ESBWR front-line safety functions are passive and, therefore, have significantly less reliance on the performance of supporting systems or operator actions than previous BWRs. In fact, ESBWR does not require operator actions for successful event mitigation until 72 hours after the onset of an accident. The dominant accident sequences typically do not contain independent component failures. Instead, they consist of common cause failures that disable entire mitigating functions. And, it is important to note that multiple mitigating functions must fail in the dominant sequences, so a single common cause event is insufficient to directly result in core damage.

The containment provides a highly reliable barrier to the release of fission products after a severe accident, with the dominant release category being that defined by nominal allowed leakage (identified as variable TSL).

The Level 3 results indicate that the offsite consequences due to internal at-power events are negligible. The results, including sensitivity studies, demonstrate that the estimated offsite consequences are less than the defined dose limits by several orders of magnitude.

19.2.6 COL Information

19.2.6-1-A Seismic High Confidence Low Probability of Failure Margins

This COL Item is addressed in Subsection 19.2.3.2.4.

19.2.7 References

19.2-1 NUREG-1560, Individual Plant Examination Program: Perspectives on Reactor Safety and Plant Performance, September 1997.

19.2-2 ASME RA-S-2002, “Standard for Probabilistic Risk Assessment for Nuclear Power Plant Applications,” ASME, New York, New York, April 5, 2002.

19.2-3 ASME RA-Sa-2003, “Standard for Probabilistic Risk Assessment for Nuclear Power Plant Applications,” Addendum A to ASME RA-S-2002, ASME, New York, New York, December 5, 2003.

19.2-4 ASME RA-Sb-2005, “Standard for Probabilistic Risk Assessment for Nuclear Power Plant Applications,” Addendum B to ASME RA-S-2002, ASME, New York, New York, December 30, 2005.

19.2-5 GE-Hitachi Nuclear Energy, NEDO-33306, “Severe Accident Mitigation Design Alternatives,” Revision 4, October 2010.

19.2-6 NUMARC 91-06, “Guidelines for Industry Actions to Assess Shutdown Management,” December 1991.

19.2-7 SECY-93-087, “Policy, Technical and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs,” April 2, 1993.

Table 19.2-1 Comparison of ESBWR Features With Existing BWRs (Sheet 1 of 3)

NUREG-1560 Key Observations	ESBWR Features
General Observation The variation in the CDFs is driven by plant design differences (primarily in support systems such as cooling water, electrical power, ventilation, and air systems). BWRs require several large motors for pumps and valves in continuous or cyclic duty for successful event mitigation. These motors require AC or DC power, and cooling.	ESBWR front-line safety functions have significantly less reliance on supporting systems and are not sensitive to variations in supporting system reliability.
AOOs (transients) Important contributor for most plants because of reliance on support systems; failure of such systems can defeat redundancy in front-line systems. Noted variability in the probability that an operator will fail to depressurize the vessel for low pressure injection in BWRs Susceptibility to harsh environment affecting the availability of coolant injection capability following loss of decay heat removal. Ability to cross-tie systems to provide additional redundancy.	ESBWR passive features have significantly less reliance on supporting systems. ESBWR does not require operator actions for successful event mitigation until 72 hours, thus there is significantly less reliance on successful operator actions. Harsh environment primarily affects motors and pump seals in BWRs and is therefore less important to ESBWR risk. In ESBWR, the cross-tie potential has been identified at the design stage as an integral part of the design, not requiring complicated recovery actions.
Loss of Preferred Power Significant contributor for most plants, with variability driven by: • Length of battery life; • Number of redundant and diverse emergency AC power sources; • Availability of alternative offsite power sources; and • Availability of firewater as a diverse injection system for BWRs.	The ESBWR design addresses battery life by adding 72-hour batteries for several components. Motor-driven pump powered by ancillary diesel generator has been added as a diverse makeup system. The core can be kept covered without any AC sources, which results in loss of preferred power (LOPP) initiated CDF that is very much lower than existing BWRs.
ATWS Normally a low contributor to plant CDF because of reliable scram function and successful operator responses.	A low contributor to plant CDF because of reliable scram function (e.g., removal of scram discharge volume, use of FMCRD run-in) and passive standby liquid control.
Internal Floods Small contributor for most plants because of the separation of systems and compartmentalization in the reactor building, but significant for some because of plant-specific designs. Largest contributors involve service water breaks.	Also a small contributor for the same reasons. BWRs with direct service water cooling to plant loads are more susceptible to line breaks. The ESBWR segregates the service water from the plant loads by closed component cooling water systems.

Table 19.2-1 Comparison of ESBWR Features With Existing BWRs (Sheet 2 of 3)

NUREG-1560 Key Observations	ESBWR Features
LOCAs BWRs generally have lower LOCA CDFs than PWRs for the following reasons: • BWRs have more injection systems; and • BWRs can more readily depressurize to use low-pressure systems.	ESBWR retains BWR LOCA response features and enhances them by adding passive Emergency Core Cooling System (ECCS). The reliability of depressurization and injection functions is significantly improved, with no reliance on operator action. ESBWR reduces the potential for LOCA by removing the recirculation system altogether.
ISLOCA Small contributor to plant CDF for BWRs and PWRs because of the low frequency of initiator.	Also a small contributor to ESBWR CDF. The design of the ESBWR reduces the possibility of a LOCA outside the containment by designing to the extent practical all piping systems, major system components (pumps and valves), and subsystems connected to the reactor coolant pressure boundary (RCPB) to an ultimate rupture strength at least equal to the full RCPB pressure.
Early Containment Failure Overpressure failures (primarily from ATWS), fuel-coolant interaction, and direct impingement of core debris on the containment boundary are important contributors to early failure for BWR containments. The higher early structural failures of BWR Mark I containments versus the later BWR containments are driven to a large extent by drywell shell melt-through.	The ESBWR is designed to minimize the effects of direct containment heat, ex-vessel steam explosions, and core-concrete interaction. The ESBWR containment is designed to a higher ultimate pressure.
Containment Bypass Bypass is generally not important for BWRs.	Bypass is not important for ESBWRs due to the reliability of the containment isolation functions.
Late Containment Failure Overpressurization when containment heat removal is lost is the primary cause of late failure in most PWR and some BWR containments. High pressure and temperature loads caused by core-concrete interactions are important for late failure in BWR containments. Containment venting is important for avoiding late uncontrolled failure in some Mark I containments.	The probability of a loss of containment heat removal is significantly reduced because the PCCS is highly reliable due to redundant heat exchangers and passive component design. The BiMAC device is designed to prevent core-concrete interactions. Containment venting is possible in the ESBWR, but the importance has been minimized by the PCCS reliability.

Table 19.2-1 Comparison of ESBWR Features With Existing BWRs (Sheet 3 of 3)

NUREG-1560 Key Observations	ESBWR Features
Human Actions Only a few specific human actions are consistently important for either BWRs or PWRs as reported in the Individual Plant Examination submittals. For BWRs, the actions include manual depressurization of the vessel, initiation of standby liquid control during an ATWS, containment venting, and alignment of containment or suppression pool cooling. Manual depressurization of the vessel is more important than expected, because most plant operators are directed by the emergency operating procedures to inhibit the automatic depressurization system (ADS) and, when ADS is inhibited, the operator must manually depressurize the vessel.	No operator actions are required for safety function success in the ESBWR for the first 72 hours of an event. Several of the manually initiated actions in BWRs and PWRs are automatically actuated in the ESBWR (e.g., ADS, ADS inhibit, SLC, Suppression Pool Cooling). In PRA modeled events with multiple failures, operator actions based on monitoring the progression of the event, emergency procedures and training can be taken at any time within the first 72 hours of an event when operators select a more optimal path to shutdown, restart, managing the operating point or providing barrier protection than would be achieved with reliance only on the automated systems. For example, many important actions can be actuated or inhibited either manually or automatically. Example actions include depressurization, use of standby liquid control, and alignment for suppression pool cooling. The use of manual operator actions as a back up to automatic systems also reduces the risk associated with failure of such systems.
Station Blackout With the SBO rule implemented, the average SBO CDF is approximately 9E-6/yr. Although the majority of the plants that implemented the SBO rule have achieved the goal of limiting the average SBO contribution to core damage to about 1E-5/yr, a few plants are slightly above the goal.	Implementing the design requirements in the EPRI Utility Requirements Document has significantly reduced the SBO contribution to core damage for ESBWRs.

Table 19.2-2 ESBWR Design Features That Reduce Risk

Reactor Vessel
Increased volume of water in vessel
No recirculation loops minimizes Large LOCA potential
Only smaller diameter piping connected to vessel below core elevation

Isolation Condenser System
Redundant and Diverse active components
Cooling Pools vs. shell-side heat exchangers
In-line condensate reservoirs

Gravity-Driven Cooling System
Eliminate reliance on pumps and motor-operated valves

Passive Containment Cooling System
No active components for safety-related heat removal

Standby Liquid Control System
Two pressurized tanks of sodium pentaborate
No pumps required for injection to vessel

Reactor Water Cleanup/Shutdown Cooling
Uses larger RWCU heat exchangers for backup decay heat removal
Full pressure shutdown cooling capability

Fuel and Auxiliary Pools Cooling System
LPCI mode for backup coolant injection
Automatic Suppression Pool Cooling mode

Control Rod Drive System
Provides high pressure, high capacity injection to vessel

ATWS Prevention/Mitigation
Scram Discharge Volume eliminated
Fine Motion CRDs provide diverse backup
Automatic, safety-related SLC
Alternate Rod Insertion (ARI)

Instrumentation and Control
Multiple diverse systems to minimize common cause failures

Severe Accident Mitigation
BiMAC device added to eliminate the uncertainty of ex-vessel debris coolability and core-concrete interaction gas generation
Firewater injection capable of arresting core melt in-vessel (not modeled in PRA)
Inert containment prevents hydrogen combustion
High ultimate rupture strength of containment

Loss of Preferred Power
Plant capable of “island mode” of operation in the event of loss of grid (not modeled in PRA)
Standby Diesel Generators and Ancillary Diesel Generators supply short-term and long-term safety loads

Table 19.2-3 Risk Insights and Assumptions(Sheet 1 of 6)

Insight or Assumption	Disposition
The containment provides a highly reliable barrier to the release of fission products after a severe accident, with the dominant release category being that defined by nominal allowed leakage. The ESBWR is designed to minimize the effects of pressurization due to direct containment heating (suppression pool – Subsection 6.2.1.1), ex-vessel steam explosions (GDCS spillover pipes – Subsection 6.2.1.1.10.2), and core-concrete interaction (BiMAC – Subsection 19.3.2.6). The ESBWR containment is designed to a higher ultimate pressure than previous BWR containment designs.	Insight
The Level 3 results indicate that the offsite consequences due to internal at-power events are negligible. The results, including sensitivity studies, demonstrate that the estimated offsite consequences are less than the defined individual, societal, and radiation dose limits by several orders of magnitude.	Insight
The ESBWR incorporates redundancy and diversity in its design principles, and has used PRA insights during development to identify potential risks and to address them in the design phase. As such, the risks of core damage and offsite radiological consequences are very low. In addition, the risk profile is balanced such that there are no individual component failures or operator errors that contribute a proportionally significant risk. The relative risk significance of individual risk contributions from ESBWR SSCs and operator actions are very low, and are on the same order of magnitude, in some cases, of events that were previously excluded in LWR PRAs.	Insight
The design of the ESBWR reduces the possibility of a LOCA outside the containment by designing to the extent practical all piping systems, major system components (pumps and valves), and subsystems connected to the reactor coolant pressure boundary (RCPB) to an ultimate rupture strength at least equal to the full RCPB pressure.	Insight
Sensitivity study results indicate that changes in test and maintenance unavailability do not significantly impact the CDF or insights.	Insight
LOCA frequencies. For each pipe group, the number of lines, the number of sections (assessed on the basis of layout drawings), the frequency apportionments, and the final averaged frequencies. Sensitivity study results indicate that changes in the LOCA frequencies have the potential to impact CDF, but still maintain significant margin below the NRC safety goal guidelines.	Operational Program – Site Baseline PRA
Sensitivity study results indicate that changes in the human error failure probabilities, particularly pre-initiators, have the potential to impact CDF, but still maintain significant margin below the NRC safety goal guidelines.	Operational Program – Human Factors Engineering
Sensitivity study results indicate that squib valve failure rate estimates have the potential to impact CDF, but still maintain significant margin below the NRC safety goal guidelines.	Operational Program – Maintenance Rule
If automatic isolation fails to isolate an RWCU/SDC line break outside of containment, manual action to isolate the line is modeled in sequences that allow successful low pressure injection.	Operational Program – Procedure Development

Table 19.2-3 Risk Insights and Assumptions(Sheet 2 of 6)

Insight or Assumption	Disposition
If the containment is breached or is vented, GDCS injection fails to be sustained in long-term sequences because condensate make-up to GDCS from PCCS is not available. An external injection source must be available in these sequences to ensure adequate core cooling.	Operational Program – Procedure Development
The design certification PRA uses conservative assumptions in the treatment of ATWS conditions. The following failures are assumed to lead directly to core damage: • Feedwater runback • ADS Inhibit • Level control using Feedwater or CRD injection • SLC The Site Baseline PRA will be refined to reflect operating procedures that will be developed to address the response to ATWS conditions.	Operational Program – Site Baseline PRA
Q-DCIS and N-DCIS are designed to high standards for reliability, including very reliable hardware and high quality software. The most dominant failure modes reside in the uncertainty in the treatment of software faults, including common cause software failures that either cause demanded actions to fail, or cause spurious actions.	Operational Program – Site Baseline PRA
GDCS faults are dominated by common cause failures of the check valves or the squib valves in the injection and equalize lines.	Operational Program – Maintenance Rule
CRD injection is assumed to be functional following a containment overpressurization failure due to the separation between the dominant containment failure locations (Appendix 19C) and the location of CRD pumps and lines. This is an important assumption, based on the containment failure analysis, that supports the use of CRD in these sequences.	Operational Program – Site Baseline PRA
The following operator actions have the highest risk importance: • Fail to recognize the need for IC/PCCS pool makeup • Fail to recognize the need for makeup after depressurization • Fail to close Lower Drywell Hatches after a LOCA during Shutdown These operator actions are based on conservative modeling methods and none are considered to be dominant contributors to CDF or LRF.	Operational Program – Human Factors Engineering
FAPCS, internal and external, injection capability provide adequate core cooling for transients given successful DPV or ADS valve operation, even if containment pressure is at the ultimate containment pressure.	Design Requirement (Subsection 9.1.3.2)
The DPS cabinet is assumed to be located in a separate fire area in the control building. A preliminary fire PRA analysis model with DPS cabinet located inside room 3301 shows that the fire risk in fire area F3301 would be the dominant contributor to all fire risks due to the high failure probability of common cause failure of software for the safety–related system, the failure of DPS, and multiple nonsafety-related systems impacted by a fire in room 3301. With a separate fire area for the proposed DPS cabinet in the detailed design, the fire risk can be significantly reduced.	Design Requirement (Figure 1.2-4)

Table 19.2-3 Risk Insights and Assumptions(Sheet 3 of 6)

Insight or Assumption	Disposition
The exposure of the distributed control and information systems (Q-DCIS and N-DCIS) equipment to heat and smoke caused by a fire in a single fire area does not cause spurious actuations that could adversely affect safe shutdown.	Design Requirement (Subsection 9.5.1.12)
The communication links between the main control room (MCR) and the Q-DCIS and N-DCIS rooms do not include any copper or other wire conductors that could potentially cause fire-induced spurious actuations that could adversely affect safe shutdown.	Design Requirement (Subsection 9.5.1.10)
It is assumed that the doors that connect the Control and Reactor Buildings with the Electrical Building galleries are watertight, for flooding of the galleries up to the ground level elevation.	Design Requirement (Subsection 3.4.1.4.3)
The Drywell Floor Drain Sump channels, which allow leakage on the lower drywell floor to flow into the sump, will prevent any molten debris, which reaches the inlet, from entering the sump.	Design Requirement (Subsection 6.2.1.1.10.2)
Closure of both the equipment hatch and the personnel hatch can be performed from outside the lower drywell/containment.	Design Requirement (Section 1.0, Figure 1.2-2)
The IC/PCCS Pool valves that provide make-up water from the equipment storage pool have DPS controls and are powered from a reliable source of power, which is capable of long-term support.	Design Requirement (Table 7.8-3 and Subsection 5.4.6.2.2)
Control logic cabinets for each of the containment vacuum breaker isolation valves must be located in separate fire zones.	Design Requirement (Subsection 6.2.1.1.2)
Because of the high consequence of a RWCU/SDC line break outside containment this system is designed with an additional diverse, nonsafety-related valve that is used for line isolation. This valve is controlled by the nonsafety-related DCIS system and closes on the same signals that provide the safety-related isolation.	Design Requirement (Subsection 5.4.8.1.2)
Power operated equipment and valves on lines attached to the RPV that require maintenance have maintenance valves installed such that freeze seals will not be required.	Design Requirement (Subsection 5.2.3.1.1)
Separate common cause failure groups are assumed in the PRA model for safety-related versus nonsafety-related batteries and inverters.	Design Requirement (Subsection 7.1.1)
A pneumatic accumulator and check valve are required to support the remote-manual and ADS-activated functions of the valve. The accumulator and check valve ensures that the valve opens via the pneumatic operator following a failure of the pneumatic pressure source.	Design Requirement (Subsection 5.2.2.2.2)
The composition of the layer of protective material on the lower drywell floor that covers the BiMAC piping is designed, for the more likely severe accident sequences, to prevent melt impingement due to corium ablation, and also to prevent noncondensable gas generation in quantities that would lead to exceeding the containment ultimate pressure.	Design Requirement (Subsection 19.3.2.6)

Table 19.2-3 Risk Insights and Assumptions(Sheet 4 of 6)

Insight or Assumption	Disposition
The ATWS sequences experience core damage at high pressure because ADS is inhibited as part of the core damage mitigation effort. However, it is assumed that Emergency Operating Procedures (EOPs) will instruct the operator to depressurize after core damage has occurred in an attempt to preserve containment. The frequency of ATWS sequences experiencing RPV rupture at high pressure is negligible, so only failures at low pressure were analyzed.	Operational Program – Procedure Development
Venting is assumed to occur when the containment pressure reaches 90% of the ultimate containment strength.	Operational Program – Procedure Development
During shutdown conditions, a continuous fire watch is required for the following scenarios with breached fire barriers for maintenance activities: • The breaching of the fire door between fire areas F1152 and F1162 (the reactor building fire areas that house RWCU pumps) and between fire areas F4250 and F4260 (the turbine building fire areas that house the RCCW pumps). • The simultaneous breaching of multiple fire barriers that can open fire areas F3301 and F3302 (the N-DCIS room fire areas) to fire area F3100 (the corridor fire area) at the same time. • The simultaneous breaching of multiple fire barriers that can open fire areas F5350 and F5360 (the PIP electric equipment room fire areas) to fire area F5100 (the corridor fire area) at the same time. Shutdown fire risks related to the fire barriers are evaluated and managed in accordance with the outage risk management program of 10 CFR 50.65(a)(4).	Operational Program – Maintenance Rule
All LOCAs below TAF during shutdown require closure of lower drywell hatch. The hatch can be opened during shutdown. If a break occurs in the lower drywell and the hatch is not closed, core damage is assumed to occur (once the water level reaches the bottom of the hatch, it is assumed that the door can not be closed and the leak not isolated).	Operational Program – Procedure Development
An important recovery action during shutdown is to recover at least one train after loss of both operating RWCU/SDC system trains. This is the primary method of residual heat removal. In the limiting case of loss of cooling, there are approximately four hours before boiling would occur. Therefore, there is ample time to restore RWCU/SDC or its supporting systems, such as Service Water or Reactor Component Cooling Water.	Operational Program – Procedure Development
During Mode 5, while preparing to remove the RPV head, RPV water level is raised to provide additional shielding for the personnel removing the head bolts. In BWRs, level is raised to approximately the level of the flange to maximize shielding. In the ESBWR, with its additional RPV height to accommodate the chimney, water level could be raised to a point below the vessel flange to achieve equivalent shielding protection for the workers. In addition, if water level is raised to below the ICS inlet lines, ICS can still be used to remove decay heat, in the event that shutdown cooling is lost during this time period. The duration of this configuration is estimated to be small, around 12 hours, so the overall risk contribution is small.	Operational Program – Procedure Development

Table 19.2-3 Risk Insights and Assumptions(Sheet 5 of 6)

Insight or Assumption	Disposition
The plant should not be in a Mode 6 Unflooded condition when a hurricane strike occurs. This is because in Mode 6 Unflooded the containment is open, the reactor vessel is open and the water above the core will not keep the core cool for an extended period of time.	Operational Program – Procedure Development
A dominant risk contributor with respect to shutdown modes is Mode 6 Unflooded. This is consistent with the baseline shutdown CDF results since the isolation condenser system is not credited in the Mode 6 Unflooded event trees. Therefore, it is necessary to ensure the operability of the systems critical to decay heat removal function during this mode.	Operational Program – Maintenance Rule
It is assumed that the watertight doors are normally closed at power. Opening of the doors would generate an alarm in the Control Room, and procedures direct their immediate closure upon receipt of an alarm.	Operational Program – Human Factors Engineering (alarm), Procedure Development (response)
It is assumed that, during shutdown, manual and Automatic Depressurization System (ADS) of the vessel are available while the vessel head is in place.	Operational Program - Technical Specification LCO 3.5.3
It is assumed that the actuation of the GDCS due to an RPV Level 1 water level signal is available during shutdown PRA Mode 5 and Mode 6 Unflooded.	Operational Program - Technical Specification LCO 3.5.3
Procedures have provisions to prohibit coincident removal of the control rod and CRD of the same assembly.	Operational Program – Procedure Development
Contingency procedures provide core and spent fuel cooling mitigative actions during FMCRD replacement with fuel in the vessel.	Operational Program – Procedure Development
During shutdown conditions, in preparation for refueling, both trains of RWCU/SDC are running while the unit is in either Mode 5 or Mode 6 until the reactor cavity is flooded.	Operational Program – Procedure Development
The outage planning and control program is consistent with NUMARC 91-06.	Operational Program – Procedure Development
The FAPCS vessel injection manual isolation valve is a locked-open valve. While its open position is assured by administrative controls, it is an important valve whose failure to remain open could disable two active low pressure injection functions: FAPCS and FPS through FAPCS.	Operational Program – Human Factors Engineering
The PCCS pool drain line maintenance valves are locked-open manual valves with position indication in the Main Control Room.	Operational Program – Human Factors Engineering
A fire in the lower drywell that damages all equipment in the area can significantly impact the CDF. These fires have been screened from the Fire PRA analysis. The area is inert during power operations. During shutdown, the screening is based on engineering judgment. The components that lead to the high risk significance are RWCU/SDC equipment and containment isolation valves. The judgment to screen this from analysis is based on the physical separation of the components, the limited number of ignition sources in the area, and the limited combustible material in the area.	Operational Program – Site Baseline PRA

Table 19.2-3 Risk Insights and Assumptions(Sheet 6 of 6)

Insight or Assumption	Disposition
There are implicit assumptions in the high winds risk assessment that (1) the plant will go to Mode 4 and will not de-inert in Mode 4 when the plant shuts down in anticipation of a hurricane strike, and (2) in anticipation of a hurricane strike, the plant will ensure that equipment credited in the high winds PRA is available.	Operational Program – Procedure Development

Table 19.2-4 ESBWR Systems and Structures in Seismic Margins Analysis with Plant Level HCLPF not less than 1.67*SSE[1](Sheet 1 of 2)

PLANT STRUCTURES

- Reactor Building
- Containment
- RPV Pedestal
- Control Building
- RPV Support Brackets
- Firewater Service Complex

DC POWER

- Batteries
- Cable trays
- Motor control centers

REACTIVITY CONTROL SYSTEM

- Fuel assembly
- CRD Guide tubes
- Shroud support
- CRD Housing
- Hydraulic control unit

SRV

- SRV

STANDBY LIQUID CONTROL

- Accumulator Tank
- Check valve
- Squib valve
- Piping
- Valve (motor operated)

Table 19.2-4 ESBWR Systems and Structures in Seismic Margins Analysis with Plant Level HCLPF not less than 1.67*SSE[1](Sheet 2 of 2)

ISOLATION CONDENSER

- Piping
- Heat exchanger
- Valve (motor operated)
- Valve (nitrogen operated)

DPV

- DPV

GRAVITY-DRIVEN COOLING

- Check valve
- Squib valve
- Piping

VACUUM BREAKERS

- Vacuum breaker valve

PASSIVE CONTAINMENT COOLING

- Heat Exchanger
- Piping

IC/PCCS POOL INTERCONNECTION

- Valve (motor operated)

FIRE PROTECTION WATER SYSTEM

- Pump (diesel driven)
- Tank
- Piping

Note:

1. A minimum HCLPF value of 1.67*SSE will be met for the structures and equipment shown. SSE is the ESBWR Certified Seismic Design Response Spectra (CSDRS) as provided in Figures 2.0-1 and 2.0-2. Where applicable, differential building displacement is part of piping failure modes evaluation.

19.3 Severe Accident Evaluations

19.3.1 Severe Accident Preventive Features

19.3.1.1 Anticipated Transients Without Scram (ATWS)

For ATWS prevention and mitigation, the ESBWR is designed with the following features:

- An ARI system that utilizes sensors and logic that are diverse and independent of the RPS.
- Electrical insertion of Fine Motion Control Rod Drives (FMCRDs) that also utilize sensors and logic that are diverse and independent of the RPS.
- Automatic feedwater runback under conditions indicative of an ATWS.
- Automatic initiation of SLC under conditions indicative of an ATWS.
- Elimination of the scram discharge volume in the CRD system.

Subsection 15.5.4 provides details on the effectiveness of these design features for addressing ATWS concerns. Given these features, the ESBWR PRA demonstrates that ATWS provides an insignificant contribution to CDF and LRF.

19.3.1.2 Mid-Loop Operation

Not applicable to the ESBWR.

19.3.1.3 Station Blackout

The response of the ESBWR to Station Blackout is addressed in Subsection 15.5.5. The on-site AC electric power system includes four redundant load divisions. Sufficient independence is provided between redundant load divisions to ensure that postulated single active failures affect only a single load division and are limited to the extent of total loss of that load division. The 6.9 kV PIP buses are normally energized from the normal preferred power supply. When the normal preferred power supply is lost, an automatic transfer from the normal preferred power supply to the alternative preferred power supply occurs. When a LOCA occurs without a loss of preferred power (LOPP) there is no effect on the electrical distribution system. The plant remains on either source of preferred power.

During a total loss of off-site power, the safety-related electrical distribution system is automatically powered from the on-site nonsafety-related diesel generators. If, however, these diesel generators are not available, each division of the safety-related system independently isolates itself from the nonsafety-related system, and power to safety-related loads of each safety-related load division is provided uninterrupted by the safety-related batteries of each division. The divisional batteries are sized to provide power to required loads for 72 hours. In addition, devices that monitor the input voltage and frequency from the nonsafety-related system, and automatically isolate the division on degraded conditions, protect each division of the safety-related system. The combination of these factors in the design minimizes the probability of losing electric power from on-site power supplies

as a result of the loss of power from the transmission system or any disturbance of the nonsafety-related AC system.

Because of the nature of the passive safety-related systems in the ESBWR, station blackout events are not significant contributors to CDF or LRF.

19.3.1.4 Fire Protection

The Fire Protection System (FPS) serves as a preventive feature for severe accidents in two ways; (1) by reducing or eliminating the possibility of damaging fire events that could induce transients, damage mitigation equipment, and hamper operator responses; and (2) as a means for long-term makeup to the upper containment pools, which may be required after the first 72 hours of an accident requiring passive heat removal.

Subsection 9.5.1 provides details on the fire prevention design elements of FPS. The risk significance of fire is relatively low, due to the design features incorporated in the ESBWR. The fire PRA is summarized in Subsection 19.2.3.2.1 above.

19.3.1.5 Intersystem Loss-of-Coolant Accident

An Intersystem Loss of Coolant Accident (ISLOCA) is postulated to occur when a series of failures or inadvertent actions occur that allow the high pressure from one system to be applied to the low design pressure of another system, which could potentially rupture the pipe and release coolant from the reactor system pressure boundary. This may also occur within the high and low pressure portions of a single system. The design of the ESBWR reduces the possibility of a LOCA outside the containment by designing to the extent practicable all piping systems, major system components (pumps and valves), and subsystems connected to the reactor coolant pressure boundary (RCPB) to an ultimate rupture strength at least equal to the full RCPB pressure.

Due to these design features of the ESBWR, ISLOCA is not a significant contributor to initiating events or accidents.

19.3.1.6 Fire Water Addition System

The FPS not only plays an important role in preventing core damage, but it is the backup source of water for flooding the lower drywell should the core become damaged and relocate into the containment (the primary source is the deluge subsystem pipes of the Gravity Driven Cooling System). The primary injection path is from the dedicated FAPCS pump through the feedwater line and into the reactor pressure vessel. This system must be manually aligned. This is appropriate because the sequences in which FPS is useful are slow to develop and easy to identify.

19.3.1.7 Vessel Depressurization

The ESBWR reactor vessel is designed with a highly reliable depressurization system. The nitrogen supply and battery capacity are sufficient to allow depressurization after potential ICS failures. This system plays a major role in preventing core damage.

19.3.1.8 Isolation Condenser System

The ESBWR ICS is described in Subsection 5.4.6. It is designed to automatically limit the reactor pressure and preclude SRV operation when the reactor becomes isolated following a scram during power operations. The ICS, together with the water stored in the RPV, conserves sufficient reactor coolant volume to avoid automatic depressurization caused by low reactor water level. ICS removes excess sensible and core decay heat from the reactor, in a passive way and with minimal loss of coolant inventory from the reactor, when the normal heat removal system is unavailable, after any of the following events:

- Sudden reactor isolation from power operating conditions
- Station blackout (unavailability of all AC power)
- Anticipated Transient Without Scram (ATWS)
- Loss-of-Coolant-Accident (LOCA)

The ICS is designed as a safety-related system to remove reactor decay heat following reactor shutdown and isolation. It also prevents unnecessary reactor depressurization and operation of other Engineered Safety Features that can also perform this function. In the event of a LOCA, the ICS provides additional liquid inventory from an in-line condensate reservoir upon opening of the condensate return valves to initiate the system.

19.3.2 Severe Accident Mitigative Features

19.3.2.1 Hydrogen Generation and Control

The potential for containment failure due to hydrogen generation is addressed by considering physical characteristics of the containment, notably the inerted condition and containment structural capability, as well as the reliability of passive systems engineered to perform the containment functions of isolation, vapor suppression, and heat removal. Containment failure due to combustible gas deflagration in the drywell and wetwell airspace is shown to be negligible considering the inerted containment and time period required to generate enough oxygen to create a combustible gas mixture. In addition, ICS and PCCS components are designed to maintain their integrity for combustible gas deflagration that may occur in design basis accidents and severe accidents.

Because the ESBWR containment is inerted, the prevention of a combustible gas deflagration in the drywell and wetwell airspace is assured in the short term following a severe accident. In the longer term, there is an increase in the oxygen concentration resulting from the continued radiolytic decomposition of the water in the containment. Because the possibility of a combustible gas

condition is oxygen-limited for an inerted containment, it is important to evaluate the containment oxygen concentration versus time following a severe accident to assure that there will be sufficient time to implement recovery actions. It is desirable to have at least a 24-hour period following an accident to allow for actions with a high likelihood of success. This subsection discusses the rate at which post-accident oxygen will be generated by radiolysis in the ESBWR containment following a severe accident, and establishes the period of time that would be required for the oxygen concentration in containment to increase to a value that would constitute a combustible gas condition (5% oxygen by volume) in the presence of a large hydrogen release.

The rate of gas production from radiolysis depends upon the power decay profile and the amount of fission products released to the coolant. Analysis results have been developed in a manner consistent with the guidance provided in SRP 6.2.5 and Regulatory Guide 1.7. There are unique design features of the ESBWR that are important with respect to the determination of post-accident radiolytic gas concentrations. In the post-accident period, the ESBWR does not utilize active systems for core cooling and decay heat removal. For a design-basis LOCA, ADS depressurizes the reactor vessel and GDCS provides gravity-driven flow into the vessel for emergency core cooling. The core coolant is subcooled initially and then it is saturated, resulting in steam flow out of the vessel and into the containment. The PCCS heat exchangers remove the energy by condensing the steam.

A similar situation exists for a severe accident that results in core melt followed by reactor vessel failure. In this case, the GDCS coolant covers the melted core material in the lower drywell, with an initial period of subcooling followed by steaming. The PCCS heat exchangers remove the energy in the same manner as described above for a design basis LOCA.

Each PCCS heat exchanger has a vent line that transfers non-condensable gases to the suppression pool vapor space, driven by the drywell to suppression pool pressure differential. In this way, the majority of the non-condensable gases will be in the suppression pool. The accumulation of combustible noncondensable gases in the PCCS and ICS heat exchangers is discussed below. A vent fan is installed in each vent line to redistribute the non-condensable gases from the wetwell to the drywell when deemed appropriate during long-term (post 72-hour) recovery actions.

The calculation of post-accident radiolytic oxygen generation accounts for this movement of non-condensable gases to the suppression pool after they are formed in the drywell. In addition, the effect of the core coolant boiling, which strips dissolved gases out of the liquid phase resulting in a higher level of radiolytic decomposition, is accounted for in the analysis.

Analysis Assumptions

The analysis of the radiolytic oxygen concentration in containment is performed consistent with the methodology of Appendix A to SRP 6.2.5 and Regulatory Guide 1.7. Some of the key assumptions are as follows:

- Reactor power is 102% of rated
- $G(O_2)$ = 0.25 molecules/100eV
- Initial containment O_2 concentration = 4%
- Allowed containment O_2 concentration = 5%
- Stripping of drywell non-condensable gases to wet-well vapor space
- Fuel clad-coolant reaction up to 100%
- Iodine release up 100%
- Adequate gas mixing throughout containment
- Passive Auto-catalytic Recombiners are not credited

Analysis Results

The analysis results show that the time required for the oxygen concentration to increase to the de-inerting value of 5% is significantly greater than 24 hours for a wide range of fuel clad-coolant interaction and iodine release assumptions up to and including 100%. Thus, the containment failure due to combustible gas deflagration in the drywell and wetwell airspace is shown to be unrealistic considering the inerted containment and time period required to generate enough oxygen to create a combustible gas mixture.

Combustible Gas Accumulation in PCCS and ICS

Radiolytic generation of combustible gases occurs in all light water reactors. The generation of hydrogen and oxygen gases occurs in a stoichiometric ratio at a rate proportional to the core decay heat. During a LOCA, these gases escape into the containment, resulting in very dilute concentrations of combustible gases in the drywell (below concentrations that could result in ignition).

PCCS condensers are designed to receive the drywell atmosphere during an accident, (which is a mixture of steam and noncondensable gases); to condense the steam; and to return the condensate back to the drywell. Each PCCS condenser consists of two modules submerged in a pool of cooling water. Each module contains an upper and lower drum connected by an array of tubes. Gases from the drywell pass up a central supply line that feeds both upper drums. The steam component of the gases condenses as it moves downward through the tube array (transferring its heat to the pool water) and condensate collects in the lower drum and drains back to the drywell by gravity. The pool water level drops slowly over the course of the accident as water boils off. The leftover noncondensable gases exit the PCCS condenser through a vent line that connects the lower drum to the wetwell. As steam and noncondensable gases enter the condenser, the vent operates passively to bleed the gases from the lower drum using the pressure differential between the drywell and wetwell as the driving force. In this way, something close to an equilibrium

state is reached in which noncondensable gases remain in the condenser while small amounts continue to come in with the steam and go out through the vent.

In the initial stage of a LOCA, the majority of the noncondensable gas in the drywell is nitrogen. This gas is eventually forced into the wetwell by the depressurization of the RPV. Over time, the primary noncondensable gases in the drywell are radiolytically generated hydrogen and oxygen. Analytical modeling shows that noncondensable gases accumulate in the lower portions of the tubes and lower drum. When this gas transitions from mostly nitrogen to a stoichiometric mixture of hydrogen and oxygen, a combustible concentration may exist.

PCCS components have been evaluated to determine the effects of radiolytically generated hydrogen and oxygen based on a range of mixture concentrations. A bounding detonation pressure for a pure stoichiometric mixture of hydrogen and oxygen is calculated using the highest peak pressures during a LOCA. It is then applied statically using dynamic load factors in a finite element model for the PCCS condenser. The calculated stresses for the detonation load are combined with those from seismic and LOCA thermal loads. The acceptance criterion for components subject to detonation is based on the ability of those components to retain their pressure integrity without plastic deformation.

Two postulated detonation scenarios have been analyzed in the finite element model: a detonation in one tube and a detonation in the lower drum. The finite element analyses determine the necessary thicknesses for the PCCS tubes and lower drum that satisfy the acceptance criteria for elastic-plastic analysis. Therefore, the thickness of downstream piping and components is sized to accommodate the resulting detonation loads. The magnitude of the detonation loads on the downstream components is minimized by igniters in each lower drum, and safety-related catalyst modules at the entrance of each vent pipe in the condenser lower drum. By recombining hydrogen and oxygen as it reaches the PCCS lower drum, the igniters prevent excessive oxygen from accumulating to a combustible mixture during severe accident conditions. The catalyst modules keep hydrogen concentrations in the PCCS vent below levels at which detonation events can occur.

During plant transients in which the RPV is isolated, ICS removes heat, while the condenser vent lines keep the units continuously purged of noncondensable gases. The ICS vent valves automatically open on a time delay after ICS is initiated, regardless of system pressure. Once open, the vent lines bleed steam and noncondensable gases from the condensers to the suppression pool, keeping the steam fraction in the lower drums at high levels throughout the event. The vent valves are designed to fail open on a loss of power to provide additional reliability for this function. A flow orifice in the vent line limits the maximum flow rate to minimize the amount of water inventory lost from the reactor as a result of the constant flow through the vent lines.

During a LOCA, ICS initiates in order to supply the additional condensate stored in its drain piping to the RPV to assist in keeping the core covered during a design basis accident. The actual heat removal through the ICS condenser is relatively small during a LOCA. However, if the condensers

are not isolated, there is potential for condensation to occur, and given enough time, a combustible gas concentration accumulates in the ICS condenser following a LOCA. In order to prevent this buildup from occurring, the ICS containment isolation valves automatically close after receiving an indication that the depressurization valves on the RPV have opened.

ICS and PCCS components are designed to maintain their integrity for postulated design basis accidents as well as severe accidents. This includes the consideration of combustible gas accumulation in the condensers under transient or LOCA conditions.

19.3.2.2 Core Debris Coolability

In the event of a severe accident in which the core melts through the reactor vessel, it is possible that the containment could be breached if the molten core is not sufficiently cooled. In addition, interactions between the core debris and concrete can generate large quantities of non-condensable gases, which could contribute to eventual containment failure.

The ESBWR design incorporates mitigating features to enhance core debris coolability. The lower drywell floor is designed with sufficient floor space to enhance debris spreading, and also contains the BiMAC device to protect the containment liner and basemat. The core debris coolability analysis shows that the BiMAC device is effective in containing the potential core melt releases from the RPV in a manner that assures long-term coolability and stabilization of the resulting debris. Therefore, the possibility of corium-concrete interaction is negligible.

Subsections 19.3.2.5 and 19.3.2.6 describe the function of the deluge system and the BiMAC.

19.3.2.3 High-Pressure Core Melt Ejection

The set of potential High-Pressure Core Melt Ejection (HPME) accidents that lead to Direct Containment Heating (DCH) consists of those involving core degradation and vessel failure at high primary system pressure. A necessary condition for this is that a minimum of 2 out the 4 isolation condensers (IC) have failed due to either water depletion on the secondary side, or due to failure to open the condensate return valves that keep the isolation condensers isolated during normal operation. In addition, all 8 of the squib activated, reactor depressurization valves, and all 10 of the ADS Safety Relief Valves must fail to operate.

The probability of a high-pressure core melt is significantly reduced due to the highly reliable depressurization system. In addition, the following ESBWR containment design features mitigate the possible effects of high-pressure core melt:

- The containment is segregated into an upper drywell and a lower drywell, which communicate directly, but the ability of high-pressure core melt, ejected within the lower drywell, to reach the upper drywell is mitigated by this design.
- The upper drywell atmosphere can vent into the wetwell through a large vent area and an effective heat sink.

- The containment steel liner is structurally backed by reinforced concrete, which cannot be structurally challenged by DCH.

19.3.2.4 Containment Performance

A spectrum of potential containment failure modes has been evaluated for the ESBWR, including the potential for a break outside of containment, potential ex-vessel steam explosion, direct containment heating and basemat penetration challenges. In this subsection, the focus is on the containment challenges associated with potential combustible gas deflagration, over-pressurization and bypass. The potential for containment failure due to these challenges is addressed by considering physical characteristics of the containment, notably the inerted condition and containment structural capability, as well as the reliability of passive systems engineered to perform the containment functions of isolation, vapor suppression and heat removal. The containment response has been evaluated for a 24-hour period following the onset of core damage. To provide additional insight, containment effectiveness will be quantified to demonstrate that the containment provides a reliable barrier to radionuclide release after a severe accident.

Analysis of the ultimate strength of the containment indicates that the drywell head is the most likely failure location if the containment were to over-pressurize. The pressure capability of the containment's limiting component is higher than the pressure that would be experienced if assuming a 100 per cent fuel clad-coolant reaction.

The deterministic analysis for containment pressure capability is presented in Appendix 19B and the probabilistic analysis for containment pressure fragility in Appendix 19C.

Because of the ESBWR design and reliability of containment systems, the most likely containment response to a severe accident is associated with successful containment isolation, vapor suppression and containment heat removal. As a result, the containment provides a highly reliable barrier to the release of fission products after a severe accident, with the dominant release category being that defined by the nominal allowed leakage variable, TSL. This conclusion is based on the following insights:

1. The combustible gas generation analysis indicates that a combustible gas mixture within the drywell and wetwell airspace of containment would not occur within 24 hours after the occurrence of a severe accident. Thus, containment failure by this mechanism is not considered further. Combustible gas generation within the ICS and PCCS heat exchangers is controlled by the means discussed in Subsection 19.3.2.1.
2. Containment bypass, which results in a direct path between the containment atmosphere and environment, has been evaluated. A containment penetration screening evaluation indicates that there are two systems, main steam and feedwater that require isolation to prevent significant offsite consequences. The probability of the bypass failure mode is dominated by a common cause failure of the RPS MSIV isolation signal resulting in a

calculated frequency of containment bypass two orders of magnitude lower than the TSL release category.

3. Containment over-pressurization has been evaluated in terms of early and late loss of containment heat removal, as well as the loss of the vapor suppression function. Overpressure failure is found to be about three orders of magnitude less likely than the TSL release category after a severe accident, specifically:
   a. The frequency of loss of containment heat removal in the first 24 hours after accident initiation is approximately four orders of magnitude lower than the TSL release category.
   b. The frequency of loss of containment heat removal in the period between 24 and 72 hours after accident initiation is about three orders of magnitude lower than the TSL release category.
   c. The frequency of vacuum breaker failure, which would result in the shortest time to containment over-pressurization because of the loss of the vapor suppression function, is approximately four orders of magnitude lower than the TSL release category.
4. The need for controlled filtered venting in the 24-hour period after onset of core damage has been evaluated. The evaluation considers loss of containment heat removal for the spectrum of applicable accident classes. In each representative sequence, operator controlled venting could be implemented to control the containment pressure boundary and potential leak path. However, venting is found not to be necessary to prevent containment failure within 24 hours after onset of core damage for scenarios in which containment heat removal is lost.

19.3.2.5 GDCS Deluge Subsystem

The lower drywell (LDW) deluge subsystem of GDCS provides automatic flow to the lower drywell if core debris discharge from the reactor vessel is detected. This subsystem is actuated on a high lower drywell floor temperature profile that is unique to a core debris discharge. Supply lines connect each of the GDCS water pools to the deluge headers, which are isolated by squib valves. The deluge headers provide water to the Basemat Internal Melt Arrest and Coolability (BiMAC) device embedded into the lower drywell floor to cool the ex-vessel core-melt debris. Temperature sensors in the BiMAC device provide the actuation signal to open the squib valves. This permits flooding the lower drywell after there has been a discharge of core material, which is significant because it minimizes the consequences of steam explosions that would occur if the lower drywell floor had been flooded prior to core discharge. Subsequent coverage of the core melt provides for debris cooling and scrubbing of fission products released from the debris. The deluge lines are sized to accommodate a single line failure, so that flow from the functional lines would be sufficient to ensure proper BiMAC operation; that is, capable to operate in the natural circulation mode within 5 minutes from corium melt arrival on the LDW floor.

19.3.2.6 Basemat Internal Melt Arrest and Coolability Device

The BiMAC device is a passively-cooled barrier to core debris on the LDW floor. This boundary is provided by a series of side-by-side inclined pipes, forming a jacket, which is passively cooled by natural circulation when subjected to thermal loading. Water is supplied to the BiMAC device from the GDCS pools by squib valves that are activated on the deluge lines. The timing and flows are such that cooling becomes available immediately upon actuation, and the chance of flooding the LDW prematurely, to the extent that this opens up a vulnerability to steam explosions, is remote. Analyses have shown that the containment will not fail by basemat melt-through or by overpressurization as long as the BiMAC functions. The detection and activation system is designed as a two-train system that is completely independent of core damage prevention systems. The BiMAC device is illustrated in Figure 19.3-1. Important considerations in the design are as follows:

1. Pipe inclination angle. The inclined pipes are designed with consideration of critical heat fluxes generated by the molten corium, to permit natural circulation flow.
2. Protective layer. The material located on top of the BiMAC pipes protects against melt impingement during the initial corium relocation event. This also allows an adequate, but short, time period for diagnosing that conditions are appropriate for flooding, which minimizes the chance of inadvertent, early flooding. The material is selected to have high structural integrity and high resistance to melting, and low generation capability for non-condensable gases to prevent containment over-pressurization.
3. Cover plate. A supported steel plate above the LDW floor, and the BiMAC device, serves as a floor for refueling operations. The plate is made to sit on top of normal floor grating, which is supported from below by steel columns. The cover plate is designed so that debris will penetrate it in a short period of time while providing protection for the BiMAC from CRD housings falling from the vessel.
4. Lower Drywell Cavity. The space available at the BiMAC device is sufficient to accommodate the full core debris. The entire volume available, up to a height of the vertical segments of the BiMAC pipes, amounts to approximately 400% of the full-core debris. Thus there is no possibility for the melt to remain in contact with the LDW liner. The two sumps needed for detecting leakage flow during normal operation (the Equipment Drain Sump, located above the LDW floor; and the Floor Drain Sump located in the LDW outside of the BiMAC pipes), are positioned and protected in the same manner as the rest of the LDW liner (Figure 19.3-1). The Floor Drain Sump will have channels at floor level to allow water, which falls onto the LDW floor, to flow into the sump. The channels will be long enough that any molten debris which reaches the inlet will freeze before it exits and spills into the sump. The channels will be designed consistent with ABWR DCD Tier 2, Section 19ED (Reference 19.3-4).

19.3.2.7 Containment Isolation

The ESBWR containment design minimizes the number of penetrations. This affects the severe accident response by minimizing the probability of containment isolation failure. Lines that originate in the reactor vessel or the containment have dual barrier protection that is generally obtained by redundant isolation valves. Lines that are considered nonsafety-related in mitigating an accident isolate automatically in response to diverse isolation signals. Lines which may be useful in mitigating an accident have means to detect leakage or breaks and may be isolated should this occur.

Because of the high consequence of a RWCU/SDC line break outside containment, this system is designed with a third, diverse nonsafety-related valve that is used for line isolation. This valve is controlled by the nonsafety-related DCIS system and closes on the same signals that provide the safety-related isolation.

19.3.3 Containment Vent Penetration

In accordance with the guidance in SECY-93-087 (Reference 19.3-2), Section I, Issue K, Dedicated Containment Vent Penetration, "… passive plant design features that address the containment overpressure challenge include highly reliable, redundant, and diverse passive safety-grade decay heat removal, automatic depressurization, and containment cooling." Therefore, the NRC recommended that, "the containment performance criteria proposed in Section I.J of this enclosure will serve as the basis for the staff's review of containment integrity and the need for containment vent." The containment performance goal in SECY-93-087, Issue I.J is met. Details are found in Appendix 19B and 19C.

The ESBWR design includes highly reliable, redundant, and diverse passive safety-grade decay heat removal, automatic depressurization, and containment cooling functions. In addition, use of containment venting is not credited in the calculation of LRF. Therefore, the nonsafety-related, active vent is acceptable.

19.3.4 Equipment Survivability Analysis

A severe accident is an event that progresses beyond the postulates of a design-basis accident. The capability to place the plant in a controlled, stable state after a severe accident provides an additional measure of risk reduction. To assess this capability, a four-step process has been implemented to evaluate equipment survivability in a severe accident:

- Identify the functional requirements needed to place the plant in a controlled, stable state. The functions necessary to place the plant in a stable configuration are those that are required to terminate the severe accident progression and limit potential challenges to the containment as the final barrier to radionuclide release. The resultant plant condition must be monitored to allow appropriate accident management.

- After establishing the mitigative functions, the equipment necessary to achieve these functions is identified. The term “equipment” is applied to structures, components and instrumentation necessary to achieve the function.
- The severe accident environment is then established to provide the framework for evaluating equipment survivability. The severe accident environment may present pressure, temperature or radiation conditions that exceed those associated with design-basis accidents. The severe accident environment is established by considering the spectrum of severe accidents identified in the PRA as well as a hypothetical 100% metal-water reaction of zirconium in the fuel cladding.
- Finally, equipment capabilities are evaluated in terms of the severe accident environment. As discussed in References 19.3-1 and 19.3-2, there must be “reasonable assurance” that the required mitigative features can operate in the severe accident environment over the time span in which they are needed.

19.3.4.1 Functional Requirements During Severe Accident

By definition, severe accidents have progressed beyond the conditions postulated in design-basis accidents. At a minimum, core cooling has been lost for a period long enough to introduce the potential for fuel damage. The severe accident may be arrested in the RPV (“in-vessel” severe accident) or it may progress to RPV failure (“ex-vessel” severe accident). Both types of severe accidents may pose a greater challenge than design-basis accidents to containment as the final barrier to radionuclide release. It is from this perspective that the mitigative functions necessary to place the ESBWR in a stable, controlled configuration after a severe accident have been identified. The severe accident mitigative functions are summarized below:

- Reactivity control is required to terminate the nuclear reaction, thus limiting the core energy to decay heat.
- Depressurization of the RPV is required to allow the ESBWR gravity-feed core cooling systems to function. If the RPV is depressurized prior to RPV failure, the damaged core could be cooled and stabilized within the RPV.
- Core cooling, if provided prior to RPV failure, could limit the progression of a severe accident so that a damaged core is retained in the RPV.
- Cooling of the lower drywell debris bed is required for severe accidents in which the RPV has failed, thus, introducing corium into the lower drywell. Debris bed cooling limits basemat penetration, radiated heat and non-condensable gas generation due to core-concrete interaction.
- Cooling of the upper drywell debris bed is required for severe accidents in which the RPV has failed at high pressure, which may result in corium dispersal into the upper drywell. The upper drywell cooling requirements are limited by the quantity and dispersal of potential debris in the upper drywell.

- Containment isolation is required to establish the containment as a fission product boundary to the environment.
- Containment pressure control is required to assure that containment integrity is maintained in the presence of the steam or non-condensable gas generation that may occur in a severe accident.
- Combustible gas control is required to prevent containment challenges due to the effects of deflagration or detonation.
- Post-accident monitoring of plant conditions is required to assess the accident progression and determine the need for mitigating measures and emergency actions.

19.3.4.2 Equipment Required for Severe Accident Mitigation

To implement the severe accident mitigative functions, a successful response of plant equipment, including structures, support components and associated instrumentation, is required. This section addresses the plant equipment, at a system level, that must survive in the severe accident environment to implement each safety function. The ESBWR design provides the flexibility to achieve mitigative functions with alternative methods that are not discussed here.

19.3.4.2.1 Reactivity Control

Reactivity control in a severe accident could be required if a degraded core were in a critical configuration and adequately moderated; this circumstance is exceedingly unlikely. In a degraded core configuration, reactivity control could be accomplished by the Standby Liquid Control (SLC) system. Key aspects of the SLC system are described in Section 9.3.5.

19.3.4.2.2 RPV Depressurization

The RPV may be depressurized by the Automatic Depressurization System (ADS) through use of the safety relief valves (SRVs) or depressurization valves (DPVs). Key aspects of the ADS are described in Subsection 6.3.2.8.

19.3.4.2.3 Core Cooling

Core cooling in a severe accident can be accomplished by the Gravity-Driven Cooling System, which is part of the Emergency Core Cooling System. The system supplies water to the RPV by gravity feed if the RPV is depressurized. The supply of water to the RPV, in either the short-term mode (from the GDCS pools) or the long-term mode (from the Suppression Pool) requires no external AC electrical power source or operator intervention. Key aspects of the GDCS are described in Subsection 6.3.2.7.

19.3.4.2.4 Cooling of Debris (Lower Drywell)

Cooling of the debris bed in the lower drywell can be accomplished in a severe accident by flooding the area. The GDCS, operating in the deluge mode, is the primary means for lower drywell flooding and requires no external AC electrical power source or operator intervention. Water is distributed in the lower drywell through the BiMAC. The deluge system and BiMAC are described in Subsections 19.3.2.5 and 19.3.2.6, respectively.

19.3.4.2.5 Cooling of Debris (Upper Drywell)

Debris in the upper drywell is postulated only if the RPV fails at high pressure, which is a very unlikely severe accident scenario. The upper drywell cooling requirements are limited by the quantity and dispersal of potential debris in the upper drywell.

19.3.4.2.6 Containment Isolation

Containment isolation is established early in an accident sequence by valves and control signals to isolate lines penetrating the containment. The Leak Detection and Isolation System (LD&IS) is designed to NRC requirements, including post-TMI requirements, as indicated in Appendix 1A, Table 1A-1 (Item II.E.4.2). Key aspects of containment isolation valves are described in Subsection 6.2.4; the LD&IS system is described in Subsection 7.3.3.

19.3.4.2.7 Containment Pressure Control

Containment pressure control can be accomplished by removing the heat energy accumulating within containment during a severe accident or venting to reduce pressure.

Containment Heat Removal

Containment heat removal can be accomplished by the Passive Containment Cooling System (PCCS). The system is part of the containment boundary as indicated in Appendix 1A, Table 1A-1 (Item III.D.1.1). Key aspects of the PCCS are described in Subsection 6.2.2.

Containment Venting

If the severe accident generates pressure that threatens containment integrity, the ESBWR design includes a controlled vent path to terminate the pressure rise. The vent path takes suction from the suppression pool airspace, which forces escaping fission products through the suppression pool to provide significant fission product scrubbing prior to release as summarized in Subsection 6.2.5.4.

19.3.4.2.8 Combustible Gas Control

Combustible gas control is achieved in the ESBWR by maintaining an inert containment atmosphere and by controlling combustible gas concentrations in the ICS and PCCS heat exchangers. The containment is inerted during normal operation; thus, there are no active system requirements necessary to achieve combustible gas control during a severe accident. Further, analysis summarized in Subsection 6.2.5.5 indicates that the time to generate a combustible gas

environment is so long that there would be a high likelihood of successful recovery actions, if required. Finally, a passive autocatalytic recombiner will limit the concentration of combustible gases after a severe accident. Combustible gas generation within the ICS and PCCS heat exchangers is controlled by the means discussed in Subsection 19.3.2.1.

19.3.4.2.9 Post Accident Monitoring

Monitoring of plant conditions is necessary to place the plant in a stable configuration. Consideration of regulatory requirements and the ESBWR severe accident functional response evaluation (including emergency procedure and severe accident guideline requirements), leads to the identification of variables that require monitoring in a severe accident. Such variables include indication of containment pressure, temperature, radiation and combustible gas conditions as well as indicators of mitigative system functioning.

19.3.4.3 Severe Accident Environment

References 19.3-1 through 19.3-3 provide the requirements that an applicant must address for postulated in-vessel and ex-vessel severe accidents. References 19.3-1 and 19.3-2 require that “credible” severe accidents be considered in a survivability evaluation. Reference 19.3-3 requires that survivability should consider an accident with the release of hydrogen generated by the equivalent of a 100 percent fuel-clad metal-water reaction. These considerations establish the ESBWR severe accident environment to be considered in the equipment survivability evaluation.

The resultant severe accident sequences address the credible accident scenarios as determined by the ESBWR PRA (summarized in Section 19.1) and the non-mechanistic scenario prescribed by the regulations:

- The PRA demonstrates that the sequences that dominate the core damage frequency are those with RPV failure at low pressure. Given the importance of low-pressure sequences to the core damage frequency, they will be evaluated in terms of in-vessel retention and ex-vessel accidents.
- LOCA sequences contribute a small fraction of the core damage frequency. Loss-of-coolant accidents may provide a different challenge to equipment survivability than transient sequences because the core energy is initially deposited directly to the drywell rather than to the suppression pool. Thus, a LOCA sequence, which progresses through RPV failure, is included in the survivability evaluation.
- As indicated above, consideration of a potential severe accident with the release of hydrogen generated by the equivalent of a 100% fuel-clad metal-water reaction is required by regulation. This is a non-mechanistic scenario that produces 100% fuel-clad reaction.

Sequences with RPV failure at high pressure are much less likely than those with RPV failure at low pressure. The ESBWR core damage frequency meets NRC safety goals with significant margin. Given the low probability of core damage for the ESBWR, and the small contribution of sequences

with RPV failure at high pressure, such sequences are not considered credible from the perspective of the ESBWR survivability evaluation.

19.3.4.4 Equipment Capability

As indicated in Reference 19.3-1, the requirements for “equipment survivability” differ from those that are applied to “equipment qualification,” a term which is generally applied to design-basis accidents. Specifically, the references indicate that the environmental qualification requirements of 10 CFR 50.49, the quality assurance requirements of 10 CFR 50 (Appendix B) and the redundancy/diversity requirements of 10 CFR 50.50 (Appendix A) need not be applied to features provided for severe accident protection. This conclusion is justified because of the significant differences in the likelihood of severe accidents in comparison to design basis accidents. Instead, there must be “reasonable assurance” that severe accident mitigative equipment will operate in the severe accident environment over the time span in which it is needed.

Several considerations were made in the survivability evaluation to demonstrate reasonable assurance of ESBWR equipment operability in a severe accident environment:

- Equipment physical location. The evaluation considers whether required equipment is exposed to the severe accident environment. Exposure occurs if the equipment is physically located in the primary containment. A specific location within containment may not be subject to the most severe conditions postulated in the accident, e.g., wetwell airspace conditions would be more benign than lower drywell conditions.
- The equipment design or qualification in comparison to the severe accident environment. The evaluation considers whether the severe accident environment exceeds equipment design and, if so, the significance of the equipment exposure to the severe accident environment.
- The timing of the required equipment function. The evaluation considers when the equipment function is required, notably if equipment performs its function before its design basis is exceeded.
- The nature of the required equipment function. The evaluation considers whether the equipment must change state (“active” component) within the severe accident environment, or must simply maintain (“passive” component) its position to achieve its mitigative function.
- The duration of the severe accident condition. The evaluation considers whether the severe accident effect on equipment is transitory or consistent over a long duration.
- Equipment material properties. The evaluation considers fundamental material properties, such as yield strength of steel, in relation to conditions predicted during a severe accident.

The survivability evaluation considers mechanical and electrical components, including associated support equipment and instrumentation.

19.3.4.5 Summary

ESBWR equipment capability was systematically evaluated in a potential severe accident environment determined by credible in-vessel and ex-vessel scenarios as well as a non-mechanistic 100% fuel-clad metal-water reaction. The evaluation identified key functions needed to place the plant in a controlled and monitored stable state. The evaluation process identified the equipment necessary to achieve these functions. The evaluation demonstrated that there is reasonable assurance that the ESBWR equipment necessary to achieve a controlled, stable plant state will function over the time span in which it is needed.

19.3.5 Improvements in Reliability of Core and Containment Heat Removal Systems

19.3.5.1 Core Heat Removal System Reliability Improvements

In addition to the conventional core heat removal methods that are retained in the plant design, the ESBWR design takes advantage of natural circulation core heat removal during at-power operations and passive heat removal by means of isolation condensers and the gravity-driven cooling system during anticipated operational occurrences (AOO) and accidents. These features provide a significant improvement in core heat removal reliability over existing BWRs due to passive features and redundant components that are not in the design of existing reactors. The Gravity-Driven Cooling System and Isolation Condenser System are described in detail in Subsections 6.3.2.7 and 5.4.6, respectively.

19.3.5.2 Containment Heat Removal System Reliability Improvements

Containment heat removal can be provided by either the PCCS or the suppression pool cooling mode of the FAPCS. For sequences with successful containment heat removal, the analysis assumes that the PCCS is available and that suppression pool cooling is not in a standby condition. This bounds the containment pressure response because the PCCS can only limit pressurization, while suppression pool cooling can limit and reduce containment pressure.

The PCCS receives a steam-gas mixture from the upper drywell atmosphere, condenses the steam using the PCCS pools as a heat sink, and returns the condensate to the GDCS pool. The non-condensable gas is drawn to the suppression pool through a submerged vent line by the pressure differential between the drywell and wetwell. The PCCS is designed to remove decay heat added to the containment after a LOCA, thus maintaining the containment within its pressure limits. Operation of the PCCS heat exchangers requires no support systems and there is adequate inventory in the PCCS pools to provide containment heat removal for 72 hours after the onset of core damage.

The Containment Inerting System bleed line has air-operated valves mounted on a line that connects the wetwell airspace to the reactor building heating, ventilation and air conditioning (HVAC) discharge. This system provides a scrubbed release path in the event that pressure in the

containment cannot be maintained below the structural limit. The path can be opened or closed at pressures up to the ultimate capability of the containment.

19.3.6 COL Information

None.

19.3.7 References

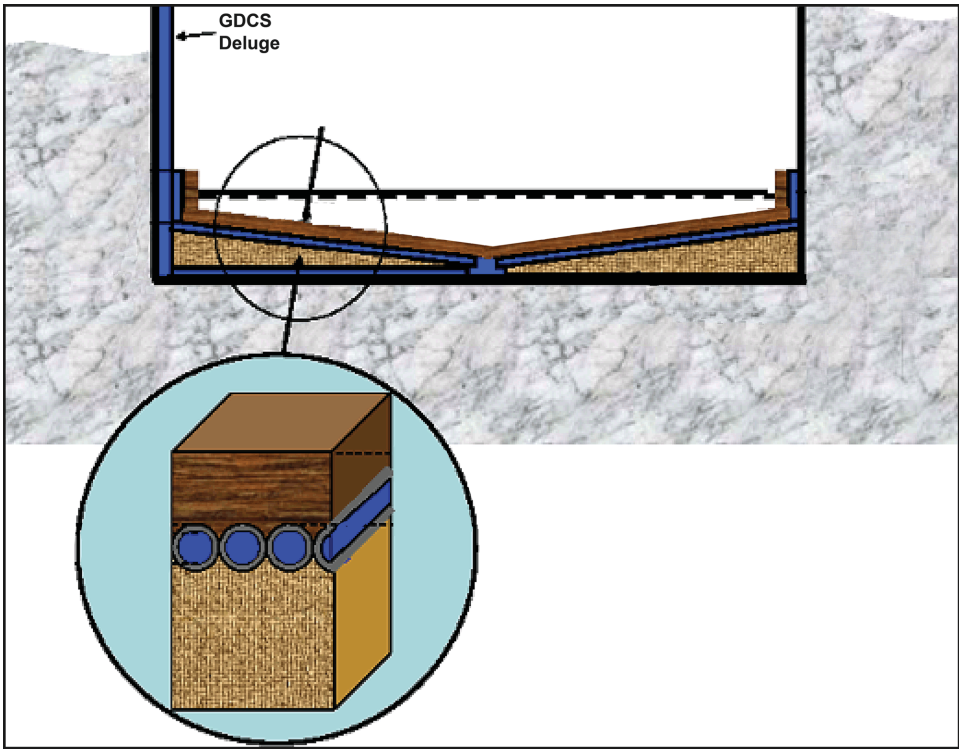
19.3-1 SECY-93-016, “Evolutionary Light Water Reactor (LWR) Certification Issues and Their Relationship to Current Regulatory Requirements”, January 12, 1990.

19.3-2 SECY-93-087, “Policy, Technical and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs”, April 2, 1993.

19.3-3 10 CFR 50.34, “Contents of Application; technical information”, Code of Federal Regulations.

19.3-4 ABWR Standard Safety Analysis Report, 23A6100, Revision 3, November 1993.

Figure 19.3-1 BiMAC Pipes and Protective Layer



19.4 PRA Maintenance

19.4.1 PRA Design Controls

PRA design controls consistent with the regulatory positions in Regulatory Guide 1.200 contain the following elements:

- Personnel performing PRA analyses possess sufficient expertise based on training and job experience to perform the tasks.
- Personnel performing technical reviews and independent verifications of PRA analyses possess sufficient expertise based on training and job experience to perform the tasks.
- Procedures are in place that control documentation, including revisions to controlled documents and maintenance of records.
- Procedures are in place that provide for independent verifications of calculations and information used in the PRA.
- Procedures are in place that address corrective actions if assumptions, analyses, or information used previously are changed or are found to be in error.

19.4.2 PRA Maintenance and Update Program

Chapter 19 is based upon the PRA model that represents the standard ESBWR design, and is thus considered to be the “Design Certification PRA.” The Design Certification PRA is used as a starting point to develop the site-specific PRA for each COL holder, which is referred to as the “Site Baseline PRA.” Throughout this document, the “PRA” or “PRA model” are used in general terms to describe the general application of PRA. Distinctions between “Design Certification” and “Site Baseline” are made, as appropriate, to clarify specific applications.

The PRA model is a controlled document containing the detailed information for the model. In order to maintain a PRA model that reasonably reflects the as-built and as-operated characteristics of the plant, administrative controls are implemented to:

- Monitor PRA inputs and collect new information
- Maintain and upgrade the PRA model to be consistent with the as-built and as-operated plant
- Ensure that cumulative impacts of pending changes are considered in PRA applications
- Evaluate the impact of PRA changes on previously implemented risk-informed applications
- Maintain configuration control of the computational methods used to support the PRA model
- Document the PRA model and the procedures that implement these controls

The update process addresses those activities associated with maintaining and upgrading the PRA model and documentation. PRA updates include a general review of the entire PRA model, incorporation of recent plant data and physical plant changes, conversion to new software versions,

implementation of new modeling techniques as appropriate, and documentation that facilitates review of PRA changes.

When reviewing pending changes, the impact on the CDF and LRF are estimated. As a result of the estimate, one of the following should occur:

- If the effect of the change is risk significant, a PRA model update is implemented promptly (commensurate with the safety significance of the pending change) without waiting for the normal update cycle.
- If the effect of the change is small the incorporation of the change occurs in the next scheduled model update. The identified change is documented in a change control process.
- If the change has no effect, then no further action is required.

The Site Baseline PRA will be upgraded to reflect plant design, operational, and PRA modeling changes, consistent with NRC-endorsed standards in existence 1 year prior to issuance of the update, which will be prior to initial fuel load, and then every four years. The key assumptions in the Site Baseline PRA as documented in Table 19.2-3 will be maintained or any departures shall be addressed. The COL Holder maintains this information in accordance with documentation and records retention requirements.

PRA updates are generally consistent with the positions established in Section 1.4 of Regulatory Guide 1.200.

Plant specific design, procedure, and operational changes are reviewed for risk impact. Additional reviews to identify information which could impact the Site Baseline PRA models are completed, including comparison of the PRA model with the knowledge of industry and plant experiences, information, and data with the purpose of identifying inputs pertinent to the PRA. This PRA information includes modeling errors discovered during routine use of the Site Baseline PRA or new information that could impact PRA modeling assumptions.

Various information sources are monitored on an ongoing basis to determine changes or new information that affect the model, model assumptions, or quantification. Information sources include operating experience, technical specification changes, plant modifications, maintenance rule changes, engineering calculation revisions, procedure changes, industry studies, and NRC information.

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 a comparison of the prior and the updated results portions delineating the significant changes in the PRA model elements with an associated explanation. The comparison of results provides reasonable assurance that the model update reflects the as-built and as-operated plant.

An independent review of the model or model elements by a qualified reviewer or reviewers is required as part of the update process. When major methodology changes or upgrades are made

during an update, 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 the configuration controls process. PRA upgrades receive a peer review for those elements 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 providing details of the assumptions made and their bases. PRA documentation is developed such that traceability and reproducibility is maintained.

Potential impacts to the PRA model (i.e., design changes, calculation revisions, and procedure changes) as well as any errors or potential errors found in the PRA model between periodic updates are documented in the configuration control process.

The configuration control process assures that the Site Baseline PRA is technically adequate for support to other COL Holder programs such as the Maintenance Rule.

19.4.3 Description of Significant Plant, Operational, and Modeling Changes

19.4.3.1 Design Phase Changes

Changes to the PRA model are expected in the design phase based on reliability assessments of the design details. This may be an iterative process, in which the design engineer builds quality and reliability into the SSC with feedback to the PRA model.

19.4.3.2 COL Application Phase Changes

Not Applicable.

19.4.3.3 Construction Phase Changes

The Site Baseline PRA will be completed one year prior to initial fuel load. It will include the Design Certification PRA, as a starting point, and any additional PRA modeling changes identified in the design certification process. The Site Baseline PRA will also be upgraded to reflect NRC-endorsed standards in existence 1 year prior to initial fuel load, and will be updated with plant-specific design information; insights from procedure development and operator training; and other PRA modeling changes that are identified subsequent to the completion of the Design Certification PRA.

19.4.3.4 Operational Update Phase Changes

Not Applicable.

19.4.4 COL Information

None.

19.4.5 References

None.

19.5 Conclusions

In accordance with 10 CFR 52.79(a)(46), this report is required to contain a description of the plant-specific PRA and its results. As part of the development of the certified design PRA, site and plant specific information were reviewed to determine if any changes from the certified design PRA were warranted. This review included consideration of site-specific information such as site meteorological data and site-specific population distributions, as well as plant-specific design information that replaced conceptual design information described in the UFSAR. Subsection 1.8.5 was also reviewed to determine if there were any departures affecting the PRA results. This review is summarized in Appendix 19AA

The review of site-specific information and plant-specific design information determined that: 1) the PRA bounds site-specific and plant-specific design parameters and design features and 2) these parameters and features have no significant impact on the DCD PRA results and insights. Therefore, based on this review, it is concluded that there is no significant change from the certified design PRA. In that there are no significant changes from the certified design PRA, incorporation of Chapter 19 into the UFSAR satisfies the requirement of 10 CFR 52.79(a)(46) for a description of the plant-specific PRA and its results.

The PRA and severe accident evaluations contained in this chapter demonstrate that the ESBWR is designed with state-of-the-art safety features that have high reliability and availability with significant redundancy and diversity.

The core damage frequency of internal and external events for operating and shutdown modes are significantly lower than the NRC's goal of less than 1E-4/yr. Likewise, the corresponding large release frequencies for the ESBWR are significantly lower than the NRC's goal of less than 1E-6/yr. The NRC's goals are also met with the additional constraint of crediting only the use of safety-related and RTNSS functions.

In fact, the ESBWR plant design, which considers potential effects of site-specific characteristics, represents a significant reduction in risk compared to existing operating plants. Tables 19.2-1 and 19.2-2 provide a comparison of existing BWR design features versus ESBWR design improvements, and ESBWR design features that reduce or eliminate significant risk contributors of existing operating plants.

The ESBWR design meets, with considerable margin, the goal that containment integrity be maintained for approximately 24 hours following the onset of core damage for the more likely severe accident challenges. The more likely severe accident challenges either do not result in containment failure, or result in containment failure after 72 hours. Severe accidents that result in containment failure in less than 24 hours have core damage frequencies low enough to be considered remote and speculative.

The conditional containment failure probability is approximately 0.1 for the composite of at-power core damage sequences assessed in the PRA. Although the shutdown core damage sequences

are assumed to result in direct containment bypass, their overall frequencies are significantly lower than the NRC goals.

The dominating accident sequences typically do not involve multiple independent component failures. Instead, they involve multiple, low probability, common cause failures that disable entire mitigating functions. Multiple mitigating functional failures are required to get to a core damage end state. Therefore, the ESBWR PRA does not contain significant accident sequences where a small number of failures could lead to core damage, containment failure, or large releases.

Risk-informed safety insights are derived from systematic evaluations of the risk associated with the design, construction, and operation of the plant. These insights confirm the design's robustness, levels of defense-in-depth, and tolerance of severe accidents initiated by either internal or external events. In addition, the risk significance of human errors is calculated to identify the significant human errors that may be used as an input to operator training programs and procedure refinement.

19.5.1 **COL Information**

None.

19.5.2 **References**

None.

19.6 Mitigative Strategies Descriptions and Plans

The Mitigative Strategies Description and Plans are submitted to the Nuclear Regulatory Commission as a separate licensing document in order to fulfill the requirements of 10 CFR 52.80(d). The Mitigative Strategies Description and Plans meet the requirements contained in 10 CFR 50.54(hh)(2) and will be maintained in accordance with the requirements of 10 CFR 52.98. The Mitigative Strategies Description and Plans are categorized as Security-Related Information and are withheld from public disclosure pursuant to 10 CFR 2.390.

Appendix 19A Regulatory Treatment of Non-Safety Systems

19A.1 Introduction

The purpose of this appendix is to demonstrate that the ESBWR design adequately addresses Regulatory Treatment of Non-Safety Systems (RTNSS) issues. A systematic process is used in the ESBWR design process to identify regulatory guidance and assess it relative to specified ESBWR design features to determine if additional regulatory treatment is warranted for structures, systems, or components (SSCs) that perform a significant safety, special event, or post-accident recovery functions.

The ESBWR is a passive, advanced light water reactor. In the ESBWR design, passive systems perform the required safety functions for 72 hours following an initiating event. After 72 hours, nonsafety-related systems, either passive or active, replenish the passive systems in order to keep them operating or performing post-accident recovery functions directly. The ESBWR design uses active systems to provide defense-in-depth capabilities for key safety functions. These active systems also reduce challenges to the passive systems in the event of transients or plant upsets. In general, these active defense-in-depth systems are designated as nonsafety-related.

The ESBWR design process includes the use of both probabilistic and deterministic criteria to achieve the following objectives associated with the Regulatory Treatment of Non-Safety Systems in passive plant designs:

1. Determine whether regulatory oversight for certain nonsafety-related systems is needed.
2. Identify risk important SSCs for regulatory oversight (if it is determined that regulatory oversight is needed).
3. Decide on an appropriate level of regulatory oversight for the various identified SSCs commensurate with their risk importance.

The following SECY-94-084 criteria are applied to the ESBWR design to determine the systems that are candidates for consideration of regulatory oversight:

A. SSC functions relied upon to meet beyond design basis deterministic NRC performance requirements such as 10 CFR 50.62 for anticipated transient without scram (ATWS) mitigation and 10 CFR 50.63 for station blackout (SBO).

B. SSC functions relied upon to resolve long-term safety (beyond 72 hours) and to address associated seismic capabilities.

C. SSC functions relied upon under power-operating and shutdown conditions to meet the NRC's safety goal guidelines of a core damage frequency (CDF) of less than 1.0E-4 per reactor year and large release frequency (LRF) of less than 1.0E-6 per reactor year.

D. SSC functions needed to meet the containment performance goal (SECY-93-087, Issue I.J), including containment bypass (SECY-93-087, Issue II.G), during severe accidents.

E. SSC functions relied upon to prevent significant adverse systems interactions.

Upon the identification of candidates for RTNSS consideration, the ESBWR design process evaluates each candidate to determine if RTNSS designation is made. Following selection of all equipment identified by the RTNSS process, a risk evaluation is performed to determine the appropriate regulatory controls.

In this chapter, and within other documents associated with the ESBWR RTNSS process, terms such as "RTNSS system" or "RTNSS function" are used. Although a "Regulatory Treatment of Non-Safety System system" is grammatically awkward, the term "RTNSS" is considered to be a demarcation of safety classification.

The following sections address Criteria A through E above by systematically identifying nonsafety-related systems that are potential candidates for regulatory oversight.

Criteria A, B and E are assessed using deterministic methods, including an assessment of containment performance. Criteria C and D are assessed probabilistically, by quantitative and qualitative methods based on information derived from the baseline PRA and also a focused PRA sensitivity study. The Design Certification PRA, described in Chapter 19 is a comprehensive analysis that is performed in conjunction with the design phase of the ESBWR. It is an integrated assessment of the ESBWR design as it applies to transient and accident conditions. It identifies areas where further improvement can reduce risk in the design and operational phases and it quantifies the risk estimates to assess the capability of the ESBWR design to meet the NRC safety goals of CDF less than 1.0 E-4 per year and LRF less than 1.0 E-6 per year. The focused PRA sensitivity study evaluates whether the passive systems are solely adequate to meet the NRC safety goals, that is, without the benefit of the available nonsafety-related active systems.

Systems that are identified as being significant with respect to these criteria are candidates for RTNSS. The candidate systems are then analyzed to reach a conclusion on whether they are RTNSS and to assign an appropriate level of regulatory oversight.

19A.2 Criterion A: Beyond Design Basis Events Assessment

19A.2.1 ATWS Assessment

The requirements of 10 CFR 50.62(c) state that each boiling water reactor must have:

- Equipment to trip the reactor coolant recirculating pumps automatically under conditions indicative of an ATWS.
- An alternate rod injection (ARI) system that is diverse from the reactor trip system.

- A Standby Liquid Control (SLC) system with the capability of injecting into the reactor pressure vessel a borated water solution at specified conditions.

The ESBWR functions that meet these requirements are:

- Automatic feedwater runback under conditions indicative of an ATWS
- An ARI system with sensors and logic that are diverse and independent of the RPS
- Automatic initiation of SLC under conditions indicative of an ATWS

With respect to the first criterion, the ESBWR design does not use recirculation pumps, so recirculation pump trip logic does not exist in the ESBWR. However, the ATWS automatic feedwater runback feature provides the analogous reduction in water level, core flow and reactor power, similar to recirculation pump trip “RPT” in a forced circulation BWR. This feature prevents reactor vessel overpressure and possible short-term fuel damage for ATWS events. The feedwater runback signal is generated in the safety-related ATWS/SLC processors. This signal is transmitted to the feedwater control system (described in Subsection 7.7.3) through the nonsafety-related DPS (described in Subsection 7.8.1). The portions of DPS that transmit the feedwater runback signal from the ATWS mitigation logic, and the portions of the feedwater control system that provide the pump runbacks are in the scope for RTNSS.

ARI, which hydraulically scrams the plant using the three sets of ARI valves of the Control Rod Drive System (CRD) (as described in Subsection 4.6.1) is also used for ATWS mitigation. The ARI logic is implemented by DPS. Therefore, the CRD ARI valves and the DPS ARI logic function are in the scope for RTNSS.

The ATWS/Standby Liquid Control System (SLC) mitigation logic provides a diverse means of emergency shutdown using the SLC for soluble boron injection. Automatic initiation of the SLC boron injection and ADS Inhibit on signals indicative of an ATWS are provided by safety-related controls and instrumentation. In addition, a diverse ADS Inhibit is provided by DPS logic. In order for SLC injection to be successful, both the safety-related and the nonsafety-related (DPS) ADS Inhibit logics must function. Therefore, the DPS actuated ADS Inhibit logic function is in the scope for RTNSS.

The SLC system does have nonsafety-related portions, which are the subsystem for nitrogen charging of the accumulators and the subsystem for boron mixing and makeup of the accumulators. These systems are not required for SLC to perform its safety-related function. They are used to maintain functional readiness and are not in the scope for RTNSS.

19A.2.2 Station Blackout Assessment

The ESBWR is designed such that no operator actions or AC power are required for a station blackout (SBO) event, for 72 hours. The analysis in Subsection 15.5.5 demonstrates that reactor water level is maintained above the top of active fuel by operation of the Isolation Condenser System (ICS), which is safety-related. With operation of the Passive Containment Cooling System

(PCCS), the containment and suppression pool pressures and temperatures are maintained within their design limits. Therefore, the integrity for containment is maintained. The ESBWR is designed to successfully mitigate an SBO event to meet the requirements of 10 CFR 50.63 using safety-related SSCs. There are no RTNSS candidates for SBO based on Criterion A.

19A.3 Criterion B: Long-Term Safety Assessment

19A.3.1 Actions Required Beyond 72 Hours

The safety functions required to be maintained in the long term are:

- Core cooling
- Containment integrity
- Control Room habitability
- Post-accident monitoring

The ESBWR is designed so that safety-related passive systems are able to perform all safety functions for 72 hours, after initiation of a design basis event, without the need for active systems or operator actions. After 72 hours, nonsafety-related systems are used to replenish the passive systems or to perform core cooling and containment integrity functions directly. Between 72 hours and seven days, the resources for performing safety functions must be available on-site. After seven days it is reasonable to assume that certain commodities can be replaced or replenished from offsite sources, e.g., diesel fuel. Each required safety function must be sustained to ensure that reactor and containment conditions are stable, the operating staff is protected, and the condition of the plant can be monitored.

RTNSS SSCs required to perform safety functions after 72 hours have augmented design requirements that provide reasonable assurance they will function when needed. RTNSS B SSCs have redundancy for the active components. They are designed to appropriate seismic design standards and are protected from high winds and flooding hazards. These SSCs that are subject to harsh environmental conditions are also able to perform in accident environmental conditions. Each safety function is analyzed below to identify nonsafety-related systems that are required after 72 hours. These systems are candidates for RTNSS.

To facilitate the distinctions in the following discussion, safety functions are described in terms of: 1) safety-related functions; and, 2) the RTNSS functions that perform or support the safety functions in the long term.

19A.3.1.1 Core Cooling

The core cooling safety function provides an adequate inventory of water to ensure that the fuel remains cooled and covered, with stable or improving conditions, for the duration of the accident.

The safety-related function is met by the Isolation Condenser System (ICS) for scenarios with the reactor coolant pressure boundary (RCPB) intact, and by the Gravity-Driven Cooling System (GDCS) injection function for scenarios with the RCPB open to containment, such as a LOCA. During shutdown conditions, either GDCS or the flooded-up refueling volume are sufficient to ensure core cooling. Once activated, neither power nor controls are required to maintain these functions. Cooling, which is provided by the IC/PCCS pools, is sufficient for at least 72 hours.

The inventory of water in the spent fuel pool is sufficient to provide passive heat removal in the pool for the first 72 hours following a loss of normal FAPCS spent fuel pool cooling (such as during an extended loss of preferred power event). Long term pool makeup is provided, as described below.

The RTNSS functions to support core cooling have permanently installed piping in FAPCS, which connects directly to the Fire Protection System (FPS). This allows the IC/PCCS pools and spent fuel pool to be filled with water from the FPS to extend the cooling period. Water stored in the FPS tank is sufficient to provide combined cooling from 72 hours through 7 days. The dedicated FPS equipment for providing makeup water and the flow paths to the pools is nonsafety-related. However, the piping that interfaces between FPS, FAPCS, and the pools is safety-related, as described in Subsection 9.1.3. These functions are manually actuated and can be performed without support systems. The diesel-driven FPS pump provides the driving force for the FPS makeup water. As described in Subsection 9.5.1.4, it is an air-cooled pump with skid-mounted auxiliaries and a gravity-drain fuel oil supply. The motor-driven FPS pump is self-cooled and is powered by ancillary AC power, which is described below. Water is supplied from the nonsafety-related, Seismic Category I, firewater storage tanks to the nonsafety-related, Seismic Category I, diesel-driven pump. The motor-driven pump is nonsafety-related, Seismic Category II. The nonsafety-related, Seismic Category I, fuel oil tank for the diesel-driven fire pump has a capacity based on supporting the RTNSS function of the fire pump to provide make up water to the IC/PCCS pools from 72 hours through 7 days after an accident. Refilling the pools is initiated manually and no remote controls or instrumentation are necessary.

19A.3.1.2 Containment Integrity

The containment integrity safety function removes reactor decay heat and controls containment pressure to maintain containment integrity for the duration of an accident. In addition, if the containment pressure approaches the design value during a LOCA, it is necessary to provide a means to rapidly reduce the pressure to an acceptably lower value and to maintain this low value.

The safety-related systems that provide the decay heat removal function are ICS, for non-LOCA conditions, and Passive Containment Cooling System (PCCS) for LOCAs. Both systems are capable of removing decay heat for at least 72 hours without the need for operator actions. The IC/PCCS pools must be refilled after 72 hours to support long-term cooling.

The ability to maintain containment pressure for the first 72 hours is provided by the decay heat removal capabilities of ICS and PCCS. Noncondensable gas accumulation causes the containment

pressure to trend upward; however, containment design pressure is not challenged until after 72 hours. Maintaining containment pressure after 72 hours is addressed by RTNSS functions.

After 72 hours, the RTNSS functions that require active support in order to maintain stable conditions in the containment are: 1) makeup water, which is provided from the Fire Protection System (FPS) via FAPCS piping to replenish the boil-off from the Spent Fuel Pool (SFP) and IC/PCCS pool; 2) mitigation of the containment pressure increase due to non-condensable gas generation to maintain stable long-term containment integrity; and 3) the ability to rapidly reduce containment pressure before it exceeds the design pressure.

Long-term makeup water to the IC/PCCS pools is accomplished by the FPS pumps and connections to FAPCS, as described in the discussion on core cooling (Subsection 19A.3.1.1).

Long-term containment pressure control is accomplished by a combination of passive auto-catalytic recombiners (PARs) in the containment airspaces and PCCS Vent Fans. The PARs (Subsection 6.2.5.1) remove hydrogen and oxygen generated by radiolysis. They do not require supporting power. The PCCS Vent Fans, (Subsection 6.2.2.2) redistribute the non-condensable gases from the wetwell to the drywell to reduce overall containment pressure to an acceptable level. The PCCS Vent Fans are powered from the ancillary AC power buses, and are manually aligned and operated.

Ancillary AC power (Subsection 8.3.1.1.9) is provided to RTNSS loads. Either of two nonsafety-related ancillary diesel generators provide post accident power to specified loads when no other sources of power are available. The air-cooled ancillary diesel generators are Seismic Category II, as are their associated auxiliaries, controls, electrical buses, and fuel oil storage and transfer systems. The diesel generators and associated equipment are housed in a Seismic Category II structure.

The ancillary diesel generators and associated buses are rated at 480 volts alternating current (VAC). These buses are also capable of being powered by offsite power or the onsite standby diesel generators through the PIP buses (Section 8.3). The ancillary diesels start automatically on a loss of offsite power. If an onsite standby diesel generator fails to start and provide power, the feed from the PIP bus to the ancillary diesel bus will be isolated and the ancillary diesel generator will power the associated ancillary diesel bus.

19A.3.1.3 Control Room Habitability

The control room habitability area must have adequate temperature controls during an accident to support operator actions. In addition, General Design Criterion 19 states that adequate radiation protection shall be provided to permit access to and occupancy of the control room under accident conditions, for the duration of the accident.

The safety-related function of controlling radiation dose is accomplished by the safety-related emergency filter unit (EFU) fans (Subsection 9.4.1), which automatically start and are powered by

safety-related Q-DCIS for the first 72 hours following an event. For longer-term operation, Q-DCIS is powered from the ancillary AC buses.

The safety-related cooling function is provided by the passive heat sink characteristics of the outer walls, floor and ceiling of the CRHA. In addition, if active room cooling is not functional, a safety-related trip of selected nonsafety-related displays in the control room is performed to eliminate their continued heat production.

Long-term operational activities in the control room are attributed to post-accident monitoring, which is discussed in Subsection 19A.3.1.4.

19A.3.1.4 Post-Accident Monitoring

Beyond the first 72 hours of an accident, operator actions are necessary to support continued operation of core cooling, containment integrity, and control room habitability functions, as discussed above. During this time, operators use information on the condition of the plant to support the functions needed for accident response. Therefore, post-accident monitoring safety functions include safety-related displays in the control room, emergency lighting, and control room cooling to remove heat generated by personnel and the monitoring equipment.

Safety-related post-accident monitoring is performed by instrumentation that is categorized as Reg Guide 1.97 Type A, B, or C (Sections 3.9, 3.10, 3.11). These are safety-related functions for the first 72 hours, and therefore are in the scope of RTNSS beyond 72 hours for long-term post-accident monitoring. Operability of the post-accident monitoring instrumentation is addressed in Technical Specification LCO 3.3.3.2, “Post-Accident Monitoring (PAM) Instrumentation.” Post-accident monitoring is provided by Q-DCIS, (Subsection 7.1.2.8) which is powered by uninterruptible power, including DC batteries that are designed to function for at least 72 hours. Emergency lighting is provided to support post-accident monitoring functions, and it is powered by 72-hour batteries. Passive cooling, provided by the Control Building and Reactor Building structures, maintains the equipment within acceptable temperature limits for at least 72 hours. Post 72 hours the CRHA air handling units and auxiliary cooling units maintain control room temperatures within limits.

Beyond 72 hours, it is necessary to provide power for the Q-DCIS components. Power for Q-DCIS and emergency lighting (Subsection 9.5.3) is supplied by ancillary AC power. In addition, cooling for the areas containing the DCIS components must be considered. The Q-DCIS cabinets and related components are either passively cooled, or, if necessary have localized cooling from the Control Room Habitability Area Ventilation System (CRHAVS) recirculation air handling units. Internal air conditioning provides cooling to the recirculation air handling units and heating is also available (Subsection 9.4.1). The recirculation air handling units are powered by ancillary AC power.

19A.3.2 Seismic Assessment

The seismic margins analysis described in Subsection 19.2.3.2.4 assesses the seismic ruggedness of safety-related plant systems and the nonsafety-related systems required for decay heat removal.

No accident sequence has a High Confidence Low Probability of Failure (HCLPF) ratio less than 1.67 times the peak ground acceleration magnitude of the safe shutdown earthquake (SSE). In addition, to address long-term safety functions, the structures and components that are in the scope of RTNSS Criterion B meet Seismic Category II design requirements. Therefore, there are no additional RTNSS candidates due to seismic events.

19A.3.3 Summary of RTNSS Findings for Criterion B

The following are representative SSCs that provide functions in the scope for RTNSS to address long-term safety and seismic requirements:

- Diesel Driven Fire Pump.
- Motor Driven Fire Pump.
- Fire Water Tank.
- Diesel Fire Pump Fuel Tank.
- Piping Required for Dedicated FPS Makeup Water Supplied to the Spent Fuel Pool (SFP) and IC/PCCS Pools.
- Passive Autocatalytic Recombiners.
- PCCS Vent Fans.
- Ancillary Diesel Generators.
- Ancillary Busses.
- Ancillary Diesel Generator Fuel Tanks.
- Ancillary Diesel Generator Fuel Transfer Pumps.
- Ancillary Diesel Building HVAC.
- Emergency Lighting Units.
- Control Room Air Handling Units.
- Air Conditioning for air handling unit coils and the Q-DCIS Room Local Coolers.

19A.4 Criterion C: PRA Mitigating Systems Assessment

Criterion C requires an assessment of safety functions that are relied upon at-power and during shutdown conditions to meet the NRC's safety goal guidelines. A comprehensive assessment to identify RTNSS candidates includes focused PRA sensitivity studies, an assessment of the effects of nonsafety-related systems on initiating event frequencies, and an assessment of uncertainties in these analyses, or that may be introduced by first of a kind passive components.

19A.4.1 Focused PRA Sensitivity Study

Focused PRA sensitivity studies are used to evaluate whether safety-related systems alone are adequate to meet the NRC safety goals of CDF less than 1.0 E-4 per year and LRF less than 1.0

E-6 per year. The Focused PRA studies, which encompass at-power and shutdown modes for internal and external events, retain the same initiating event frequencies as the baseline PRA models, and set the logic status of nonsafety-related systems to failed, while safety-related systems remain unchanged in the models. The Focused PRA models are evaluated using only the safety-related systems and RTNSS systems determined from Criterion A, those functions from Criterion B that are evaluated in the PRA models. Additional nonsafety-related systems are included only if they are required to meet the CDF or LRF goals.

The Focused PRA sensitivity studies include a baseline Focused PRA, (i.e., safety-related SSCs only) to determine if the safety goal guidelines are met without adding nonsafety-related SSCs. In addition, a RTNSS-based Focused PRA is created to determine which nonsafety-related systems are necessary to meet the safety goal guidelines. Success paths of the RTNSS functions from Criteria A and B are added to the baseline Focused PRA models because they receive regulatory oversight and their functions are modeled in the PRA. If the RTNSS-based Focused PRA results do not satisfy the NRC safety goal guidelines, then active functions are added to the RTNSS-based model until the goals are satisfied.

Once the NRC goals are met, there may be several combinations of SSCs that can satisfy them. In order to identify an optimal combination of SSCs, risk achievement worth importance values are calculated for each SSC in the RTNSS-based Focused PRA. The value of each SSC is determined by excluding one RTNSS function at a time. If the NRC goal cannot be met with an SSC out of service, then the SSC is considered to be highly significant.

The ESBWR baseline Focused PRA results determined that some models do not meet the CDF or LRF goals. The dominating failure mode in the baseline Focused PRAs is a common cause software failure that disables the controls to the safety-related functions. With the addition of DPS functions of GDCS injection mode and equalize mode actuation, ADS actuation, isolation of RWCU/SDC isolation valves, and opening of the IC/PCCS pool cross-connect valves, the safety goals are met.

Because these functions are required to meet the safety and containment performance goals, they are designated as High Regulatory Oversight, as discussed in Subsection 19A.8.1. The DPS functions that are not highly significant are still addressed in the Availability Controls Manual.

Assessment of Nonsafety Related Systems on Seismic Events

The focused PRA uses the internal and external events PRA models to quantify the effects of RTNSS SSCs on the safety goal guidelines. The effects of seismic events are evaluated deterministically, in accordance with the seismic margins analysis. The ESBWR plant and equipment are designed with a HCLPF of at least 1.67 times the peak ground acceleration of the safe shutdown earthquake (SSE). Only passive safety-related systems are credited in the seismic event tree. In addition, FPS is classified as nonsafety-related but is designed so that the diesel driven pump in the Fire Pump Enclosure (FPE), the FPS water supply, the FPS suction pipe from

the water supply to the pump, one of the FPS supply pipes from the FPE to the Reactor Building, and the FPS connections to the FAPCS remain operable following a seismic event. Piping and components completely separate from FAPCS pool cooling piping provide flow paths for post-accident make-up water transfer to the IC/PCCS pools and spent fuel pool. The piping and components are designed to meet Quality Group C and Seismic Category I requirements. Therefore, there are no seismic-related candidates for RTNSS consideration.

19A.4.2 Assessment of Uncertainties

The ESBWR PRA addresses passive system thermal-hydraulic uncertainty issues in a systematic process that identifies potential uncertainties in passive components or thermal-hydraulic phenomena and then applies an appropriate treatment to the component to ensure that the uncertainties are treated conservatively.

Passive system thermal-hydraulic uncertainties manifest themselves in the PRA model within failure probabilities and success criteria. Passive components that must rely on natural forces, such as gravity, have lower driving forces than conventional pumped systems so additional margin is incorporated into the design. Some passive functions are based on new engineering design, with limited operating experience to establish confidence in the failure rate estimates. The PRA models the effectiveness of passive safety functions in the failure rate estimated and success criteria that are factored into the event trees. Assessing the event tree success criteria in the PRA model identifies thermal-hydraulic uncertainties. Sensitivity studies show that the PRA results are not sensitive to changes in success criteria.

There are also uncertainties associated with the manual alignment and operation of long-term decay heat removal systems identified under RTNSS Criterion B. These uncertainties can influence the results such that there is a challenge to the CDF and LRF goals in transient sequences. This is not an issue for low frequency scenarios, such as large LOCA or seismic events.

In order to address uncertainties in the performance of passive systems, an active system with the capability to provide backup functions is added to the scope of RTNSS. The portions of FAPCS (Subsection 9.1.3.2) that provide low pressure injection and suppression pool cooling are added in the scope for RTNSS. These FAPCS modes of operation are chosen because they provide a diverse method of core cooling and containment heat removal using active components.

Using the design parameters for the FAPCS heat exchanger found in Table 9.1-8, analysis shows that additional capacity can be credited in which elevated suppression pool temperature results in a higher differential temperatures in the heat exchanger such that the heat transfer rate increases to as much as 34 MW, which is sufficient to prevent containment failure during a beyond design basis accident.

The support systems needed for FAPCS are: Reactor Component Cooling Water System (RCCWS), standby diesel generators, standby diesel generator auxiliary systems (including standby diesel generator fuel oil storage and transfer system), PIP buses, Electrical Building HVAC

(to cool the standby diesel generators and the PIP buses), RCCWS and Fuel Building HVAC (to cool the FAPCS pumps), Nuclear Island Chilled Water (to cool HVAC), and Plant Service Water System (PSWS) (to cool the RCCWS). These support systems are in scope for RTNSS Criterion C and their design basis capacity is sufficient to accommodate the beyond design basis performance of FAPCS described above. The FAPCS trains are physically and electrically separated such that no single active component failure can fail the function. This provides the CDF and LRF reduction needed to address the PRA uncertainty concerns associated with the performance of passive system components.

19A.4.3 PRA Initiating Events Assessment

The At-Power and Shutdown PRA models have been reviewed to determine whether nonsafety-related SSCs could have a significant effect on the estimated frequency of initiating events. An SSC failure that is a dominant contributor to an initiating event is significant if the initiating event contributes 10% or more to at-power or shutdown internal events CDF. The following screening criteria are imposed on the at-power and shutdown initiating events:

1. Are nonsafety-related SSCs considered in the calculation of the initiating event frequency?
2. Does the unavailability of the nonsafety-related SSCs significantly affect the calculation of the initiating event frequency?
3. Does the initiating event significantly affect CDF or LRF for the baseline PRA?

If the answer to all three of these questions is “Yes,” then the non-safety SSC is a RTNSS candidate. The results are discussed below.

19A.4.3.1 At-Power Generic Transients

Initiating events that are considered Generic Transients are listed in Subsection 19.2.3.1. Because several initiating events in this group are caused by the failures of nonsafety-related SSCs, screening questions 1, 2, and 3 are answered “Yes.” However, this category of transient initiating events includes various failures of components or operator errors. No specific nonsafety-related systems have a significant effect on risk, and there are no RTNSS candidates from this category.

19A.4.3.2 At-Power Inadvertent Opening of a Relief Valve

SRVs are safety-related. Therefore, they are not RTNSS candidates.

19A.4.3.3 At-Power Transient with Loss of Feedwater

The initiating events in this group begin with a prompt and total loss of feedwater and require the success of other mitigating systems for reactor vessel level control. The SSCs related to feedwater and condensate are nonsafety-related, and thus Questions 1 and 2 are answered “Yes.” Because of design improvements, the loss of feedwater initiating event is not a significant contributor to CDF, so Question 3 is answered “No.” Several features in the advanced design of the new generation feedwater level control system add significant reliability and, thus, a lower failure probability for loss

of feedwater initiating events. The feedwater level control system is implemented on a triplicated, fault-tolerant digital controller. Therefore, a control failure is much less likely to occur in the ESBWR than in the design of current generation of reactors. Also, due to the capacity of the pumps and the digital control system capability, loss of a single feedwater pump does not cause a turbine trip or scram.

The dominant contributors to a total loss of feedwater are a loss of control power to the feedwater controllers and loss of AC power to the pumps. Only a total and immediate loss of all feedwater flow is included in the Loss of Feedwater initiating event category. A controller failure that results in reduced feedwater flow is much less significant than a complete loss of feedwater.

Therefore, due to the conservative treatment of the condensate and feedwater systems in the PRA, their risk significance does not warrant additional regulatory oversight.

19A.4.3.4 At-Power Loss of Preferred Power

Loss of Preferred Power (LOPP) occurs as a result of severe weather, grid disturbances (including switchyard faults), plant-centered failures, or switchyard faults. LOPP is assumed to cause a plant trip and a loss of feedwater, with longer-term effects on other mitigating systems requiring AC power.

The associated systems and components that comprise the plant-centered failures, such as the onsite AC power distribution system are nonsafety-related, and thus, Questions 1, and 2 are answered “Yes.” However, those plant-centered components, such as substations, breakers, motor control centers, and protective relays, are much less risk-significant and the contribution of plant-centered LOPP is below the threshold for significance, so Question 3 is answered “No.”

Other than plant-centered faults, the dominant risk contributions are from the loss of incoming AC power from the utility grid and weather related faults. These types of faults are caused by components that are not controlled by the site organization. Questions 1 and 2 are answered “No” for these components because they are not controllable by the plant. Therefore, the SSCs within the ESBWR design scope for preventing a LOPP initiating event are not risk significant and do not warrant additional regulatory oversight. The standby diesel generators and PIP buses have RTNSS controls due to other criteria.

19A.4.3.5 At-Power LOCA

Loss of coolant accidents are initiated by piping leaks, valve leaks, or breaks. LOCAs are postulated to initiate in systems, such as RWCU/SDC and Main Steam. However, general design considerations require that all piping and components within the reactor coolant pressure boundary be safety-related. The RWCU/SDC and Main Steam piping have redundant safety-related isolation valves that automatically close on a LOCA signal. Questions 1, 2, and 3 are answered “No.”

In addition, Safety Relief Valves are safety-related. Therefore, there are no RTNSS candidates from this category.

19A.4.3.6 Shutdown Loss of Preferred Power

The causes and effects of loss of preferred power initiating event during shutdown are similar to at-power conditions, which were discussed previously. Loss of preferred power, during shutdown, initiates a loss of shutdown cooling and affects the availability of active mitigation systems. The higher contributions to loss of preferred power during shutdown are plant-centered and switchyard faults. Questions 1, and 2 are answered “Yes.” Switchyard components and plant-centered components, such as substations, breakers, motor control centers, and protective relays, are not risk-significant and below the threshold for RTNSS consideration, so Question 3 is answered “No.” For losses of incoming AC power due to grid or weather-related faults, Questions 1, 2 and 3 are answered “No” because they are caused by equipment or conditions that are not controlled by the site organization. Therefore, the nonsafety-related SSCs that contribute to shutdown LOPP do not warrant additional regulatory oversight.

19A.4.3.7 Loss of Shutdown Cooling

The decay heat removal function during shutdown modes of operation is provided by the Reactor Water Cleanup/Shutdown Cooling (RWCU/SDCS) system operating in shutdown cooling mode. Shutdown risk is dominated by loss of coolant events. Therefore, RWCU/SDC components have a relatively low importance and it is unlikely that their performance would degrade to the point where there is a measurable effect on Core Damage Frequency.

During Mode 5, in addition to RWCU/SDC, decay heat removal can be provided by safety-related ICS. During Mode 6, FAPCS may be used as an alternative. FAPCS suppression pool cooling and low pressure injection functions can remove decay heat, and they are in the RTNSS category with regulatory oversight in the form of availability controls.

With the reactor well unflooded, it is assumed that both RWCU/SDC trains are in service and that one train is sufficient to remove decay heat while maintaining stable reactor coolant temperature. Therefore, if one RWCU/SDC pump were to trip in this configuration, it would not initiate a loss of shutdown cooling event. Questions 1 and 2 are answered “Yes” because common mode failures of RWCU components are considered in the initiating event frequency. Question 3 is answered “No” because RWCU component failures leading to a loss of shutdown cooling do not meet the threshold for significance.

There are no RTNSS candidates for regulatory oversight.

19A.4.3.8 Shutdown LOCA

The frequency of Shutdown LOCA events is lower than at full power, due to the reduced vessel pressure and temperature. Also, the fact that control rods are fully inserted, the reduced pressure and temperature of the reactor coolant, and the lower decay heat level allow for longer times available for recovery actions.

Breaks outside containment can be originated only in ICS, RWCU/SDC or FAPCS piping, or instrument lines, because these are the only systems that remove reactor coolant from the containment during shutdown. The rest of the RPV vessel piping is isolated. The RWCU/SDC and FAPCS containment penetrations have redundant and automatic power-operated safety-related containment isolation valves that close on signals from the leak detection and isolation system and the reactor protection system. The ICS lines have redundant power operated safety-related isolation valves inside containment to terminate a loss of inventory in the event of an ICS line break outside of containment. Questions 1, 2, and 3 are answered “No.”

An equipment hatch for removal of equipment during maintenance and an air lock for entry of personnel are provided in the lower drywell. These access openings are sealed under normal plant operation but may be opened when the plant is shut down. Closure of both hatches is required for the shutdown Loss-of-Coolant Accident (LOCA) below top of active fuel (TAF) initiators during Modes 5 and 6. Therefore, the lower drywell hatches are in the scope of RTNSS.

19A.4.4 Summary of RTNSS Candidates from Criterion C

The focused PRA sensitivity study requires certain portions of DPS being designated as RTNSS. The portions that provide capability for a manual backup of safety-related automatic actuation of safety functions provides the level of protection necessary to meet both the CDF and LRF goals. These RTNSS DPS functions are: GDCS injection mode and equalize mode actuation, ADS actuation, isolation of RWCU/SDC isolation valves, and opening of the IC/PCCS pool cross-connect valves. They are risk significant and receive high regulatory oversight, as described in Subsection 19A.8.1.

The assessment of uncertainties concludes that the defense-in-depth role of FAPCS in providing a backup source of low pressure injection and suppression pool cooling is within the scope for RTNSS. Supporting systems for FAPCS include: RCCWS, standby diesel generators, PIP buses, Electrical Building HVAC, Fuel Building HVAC, Nuclear Island Chilled Water, and PSWS. In addition, the assessment of shutdown initiating events identifies that the lower drywell hatches should have regulatory oversight.

19A.5 Criterion D: Containment Performance Assessment

The containment performance goal in SECY-93-087, Issue I.J is addressed in Subsection 19.3.3 and Appendices 19B and 19C.

The containment bypass issue from SECY-93-087, Issue II.G, during severe accidents is concerned with potential sources of steam bypassing the suppression pool and failure of heat exchanger tubes in passive containment cooling systems. These concerns are addressed in the Design Control Document. Subsection 19.3.2.4 addresses the steam bypass of the suppression pool. Subsection 6.2.2.3 addresses the design of the Passive Containment Cooling Heat Exchanger

tubes. These Criterion D safety concerns are addressed in the ESBWR design, and no RTNSS candidates are identified.

The BiMAC device provides an engineered method to assure heat transfer between a core debris bed and cooling water in the lower drywell during severe accident scenarios. Waiting to flood the lower drywell until after the introduction of core material minimizes the potential for energetic fuel-coolant interaction. Covering core debris with water provides scrubbing of fission products released from the debris and cools the corium, thus limiting off-site dose and potential core-concrete interaction. The BiMAC device provides additional assurance of debris bed cooling by providing engineered pathways for water flow through the debris bed. BiMAC failure could occur if no water is supplied. The BiMAC device is not safety-related. It is added to the ESBWR to reduce the uncertainties involved with severe accident phenomenology. As such, the BiMAC device, the nonsafety-related GDCS deluge squib valves, and the associated actuation logic are in the scope for RTNSS.

Igniters (glow plugs) in the lower drums of the PCCS condensers recombine the hydrogen and oxygen at low concentrations, thereby keeping the resultant internal pressure of the PCCS condensers within acceptable limits to ensure there is no plastic deformation during a detonation under severe accident conditions. During the initial stages of a severe accident, there is essentially no water in the vicinity of the core, so radiolysis is greatly reduced. However, large quantities of hydrogen are released into the drywell due to metal-water reactions. The high abundance of hydrogen relative to oxygen effectively reduces the potential for detonation in the PCCS. Later in the postulated event, after the core melts through the vessel and interacts with the concrete, the deluge valves open and the core once again has the potential to resume radiolysis. Thereafter, relative concentrations of hydrogen and oxygen trend closer to a stoichiometric ratio at pressures much higher than during a DBA. The igniters are activated by the existing GDCS deluges (BiMAC) control system implemented in a nonsafety-related technology programmable logic controller.

19A.6 Criterion E: Assessment of Significant Adverse Interactions

Systems interactions are usually well recognized and, therefore, are accounted for by design engineers and within the PRA model. However, there is the potential for unrecognized subtle dependencies among the various SSCs that could be significant. The term used to describe such dependencies is adverse systems interaction (ASI). It is broadly applied in terms of functional interactions, spatial interactions and human acts of commission. Such interactions are RTNSS candidates under Criterion E.

A preliminary ASI assessment was performed, and as the design has progressed, additional assessments have been completed. The preliminary assessment and results are presented in Subsection 19A.6.1. Results of the additional assessments are provided in Subsection 19A.6.2.

19A.6.1 Systematic Approach

As part of the PRA input to design programs and processes, potential ASI discovered during the construction of the PRA are assessed for applicability to the RTNSS process under Criterion E. For the purpose of this assessment, an ASI exists if the action or condition of an active, interfacing system causes a loss of safety function of a passive safety-related system. A systematic process is used to analyze specific features and actions that are designed to prevent postulated adverse interactions, while taking into consideration the extensive operating experience that has been used in the current design criteria to prevent adverse systems interactions.

Many protection provisions are already included in the design of the Emergency Core Cooling System (ECCS) passive safety-related systems. Protection is afforded against missiles, pipe whip and flooding. Also accounted for in the design are thermal stresses, loadings from a LOCA, and seismic effects. The ECCS passive systems are protected against the effects of piping failures up to and including the design basis event LOCA.

The passive safety-related systems of the ESBWR are presented below. Active systems that interact with the passive systems are identified, followed by an evaluation of potential adverse interactions. Only those nonsafety-related systems with a potential adverse effect are analyzed further as RTNSS candidates.

19A.6.1.1 Gravity Driven Cooling System

19A.6.1.1.1 Design Features

GDCS provides flow through safety-related squib actuated injection and equalize valves to the annulus region of the reactor through dedicated nozzles. These valves are actuated by any two of three divisions of power or a nonsafety DPS signal. It provides gravity-driven flow from three separate water pools located within the drywell at an elevation above the active core region. It also provides water flow from the suppression pool to meet long-term post-LOCA core cooling requirements. The system provides these flows by gravity forces alone once the reactor pressure is reduced to near containment pressure.

All GDCS piping connected with the RPV is classified as safety-related, Seismic Category I. The electrical design of the GDCS is classified as safety-related GDCS is protected against the effects of pipe whip, which might result from piping failures up to and including the design basis event LOCA. This protection is provided by separation, pipe whip restraints, energy-absorbing materials or by providing structural barriers.

19A.6.1.1.2 System Interfaces

GDCS interfaces with the following systems: Containment, DC Power, Fuel and Auxiliary Pools Cooling System (FAPCS), Suppression Pool, and Passive Containment Cooling System (PCCS).

19A.6.1.1.3 Analysis of Potential Adverse System Interactions

Squib valve and deluge logic and valve initiation circuitry are powered by redundant, nonsafety-related power. To minimize the probability of common mode failure, the deluge valve pyrotechnic booster material is different from the booster material in the other GDCS injection and equalizing line squib valves. The pyrotechnic charge for the deluge valve is qualified for the severe accident environment in which it must operate.

The following GDCS indications are reported in the control room:

- Status of the locked-open maintenance valves
- Status of the squib-actuated valves
- GDCS pools and suppression pool level indication
- Position of each GDCS check valve
- Suppression pool high and low level alarm
- GDCS pools high and low level alarms
- Squib valve continuity alarms

FAPCS is used to cool the GDCS pools during normal operations. Inadvertent actuation of pool cooling does not adversely affect the function of GDCS. A manifold of four motor operated valves is attached to each end of the FAPCS cooling and cleanup trains. These manifolds are used to connect the FAPCS train with one of the two pairs of suction and discharge piping loops to establish the desired flow path during FAPCS operation. One loop is used for the Spent Fuel Pool and auxiliary pools, and the other loop for the GDCS pools and suppression pool and for injecting water to drywell spray sparger and reactor vessel via RWCU/SDC and feedwater pipes. The use of manifolds with proper valve alignment and separate suction-discharge piping loops allows operation of one train independently of the other train to permit on-line maintenance or dual mode operation using separate trains if necessary. It also prevents inadvertent draining of the pool, or mixing of contaminated water in the Spent Fuel Pool with clean water in other pools. The power operated safety-related containment isolation valves on the FAPCS pool cooling suction and return lines to and from the GDCS pools automatically close, if open, upon receipt of a containment isolation signal from the Leak Detection and Isolation System (LD&IS).

Inadvertent actuation of the Lower Drywell Deluge squib valves that supply the BiMAC system would adversely affect the GDCS injection function by emptying the GDCS pools into the lower drywell. The probability of an inadvertent actuation is extremely low because the Deluge squib valves and actuation logic are interlocked by safety-related temperature switches that prevent actuation until the lower drywell temperatures are indicative of a core melt-through of the reactor vessel.

The conclusion of this analysis is that existing design features of GDCS and its supporting systems are adequate to ensure that potential adverse systems interactions are not significant.

19A.6.1.2 Automatic Depressurization System (ADS)

19A.6.1.2.1 Design Features

The depressurization function is accomplished through the use of safety relief valves (SRVs) and depressurization valves (DPVs). Supporting systems for ADS include the instrumentation, logic, control and motive power sources. The instrumentation and logic power is obtained from corresponding safety-related divisional uninterruptible and 120 VAC power sources. Either source can support ADS operation. The actual SRV solenoid and DPV squib initiator power is supplied by the corresponding safety-related divisional batteries. The motive power for the electrically-operated pneumatic pilot solenoid valves on the SRVs is provided by the SRV accumulators that are charged during normal operations by the nonsafety-related High Pressure Nitrogen Supply System (HPNSS). Failure of the HPNSS does not result in a loss of SRV function.

19A.6.1.2.2 System Interfaces

ADS interfaces with the following systems: Main Steam, Containment, Suppression Pool, and DC Power.

19A.6.1.2.3 Analysis of Potential Adverse System Interactions

DC Power supplies the SRV solenoids and the DPV squibs, which actuate a shearing plunger in the valve. The squibs are initiated by any of four battery-powered independent firing circuits. The firing of one initiator-booster is adequate to activate the plunger. The valve design and initiator-booster design is such that there is substantial thermal margin between operating temperature and the self-ignition point of the initiator-booster.

The design features of ADS and its supporting systems are adequate to ensure that potential adverse systems interactions are not significant.

19A.6.1.3 Isolation Condenser System (ICS)

19A.6.1.3.1 Design Features

The ICS provides additional liquid inventory to the RPV upon opening of the condensate return valves to initiate the system. ICS also provides the reactor with initial depressurization before ADS is required, in event of loss of feed water, such that the ADS can take place from a lower water level.

Each IC is located in a subcompartment of the Isolation Condenser/Passive Containment Cooling System (IC/PCCS) pool, and all pool subcompartments communicate at their lower ends to enable full utilization of the collective water inventory, independent of the operational status of any given IC train. A valve is provided at the bottom of each IC/PCCS pool subcompartment that can be closed so the subcompartment can be emptied of water to allow IC maintenance. Pool water can heat up to about 101°C (214°F); steam that is formed, being non-radioactive and having a slight positive pressure relative to station ambient, vents from the steam space above each IC segment where it is

released to the atmosphere through large-diameter discharge vents. A moisture separator is installed at the entrance to the discharge vent lines to preclude excessive moisture carryover. IC/PCCS pool makeup clean water supply for replenishing level during normal plant operation is provided from FAPCS. A separate FAPCS makeup line provides emergency makeup water into the IC/PCCS pool from the fire protection system and from piping connections located in the reactor yard.

A purge line is provided to assure that, during normal plant operation (ICS standby conditions), excess hydrogen from radiolytic decomposition or air entering into the reactor coolant from the feedwater does not accumulate in the isolation condenser steam supply line, thus assuring that the isolation condenser tubes are not blanketed with non-condensables when the system is first started.

Upper header and lower header vent lines with valves are provided to mitigate the buildup of hydrogen during LOCA and non-LOCA events. Both valves can be operated manually. The lower header vent valve is fail-open and is automatically opened with a time delay after ICS is initiated.

On the condensate return piping just upstream of the reactor entry point is a loop seal and two valves in parallel: (1) a condensate return valve (fail as-is), and, (2) a condensate return bypass valve (fail open). These two valves are closed during normal station power operations. Because the steam supply line valves are normally open, condensate forms in the in-line isolation condenser reservoir and develops a level up to the steam distributor, above the upper headers. To start an isolation condenser into operation, the condensate return valve or condensate return bypass valve is opened, whereupon the standing condensate drains into the reactor and the steam-water interface in the isolation condenser tube bundle moves downward below the lower headers to a point in the main condensate return line. The fail-open condensate return bypass valve along with the fail-open vent valves open if the DC power is lost.

The ICS is automatically isolated to mitigate buildup of noncondensable gases during LOCA events. The signal that isolates ICS is a confirmed opening of any two DPVs.

19A.6.1.3.2 System Interfaces

System interfaces include: Main Steam, Containment, Suppression Pool, FAPCS, DC Power, and Process Radiation Monitoring.

19A.6.1.3.3 Analysis of Potential Adverse System Interactions

The ICS and PCCS pools have two local panel-mounted, safety-related level transmitters. Both transmitter signals are indicated on the safety-related displays and sent through the gateways for nonsafety-related display and alarms. Both signals are validated and used to control the valve in

the makeup water supply line to the IC/PCCS pool. The FAPCS IC/PCCS pools cooling and cleanup subsystem pump is automatically tripped on low water level in IC/PCCS pools. Water level in the skimmer surge tanks is maintained by automatic open/closure of the makeup water supply isolation valve. Water level in the IC/PCCS pools is maintained by automatic open/closure of the makeup water supply isolation valve.

Four radiation monitors are provided in the IC/PCCS pool steam atmospheric exhaust passages for each isolation condenser train. They are shielded from all radiation sources other than the steam flow in the exhaust passages for a specific isolation condenser train. The radiation monitors are used to detect isolation condenser train leakage outside the containment. Detection of a low-level leak results in alarms to the operator. At high radiation levels, isolation of the leaking isolation condenser occurs automatically by closure of steam supply and condensate return line isolation valves.

Four sets of differential pressure instrumentation are located on the isolation condenser steam line and another four sets on the condensate return line inside the drywell. Detection of excessive flow beyond operational flow rates in the steam supply line or in the condensate return line (2/4 signals) results in alarms to the operator, plus automatic isolation of both steam supply and condensate return lines.

The design features of ICS and its supporting systems are adequate to ensure that potential adverse systems interactions are not significant.

19A.6.1.4 Standby Liquid Control (SLC) System

19A.6.1.4.1 Design Features

The SLC system provides a diverse backup capability for reactor shutdown, independent of normal reactor shutdown with control rods. It also provides makeup water to the RPV to mitigate the consequences of a LOCA.

19A.6.1.4.2 System Interfaces

Control Building, Containment, DC Power

19A.6.1.4.3 Analysis of Potential Adverse System Interactions

Electrical heating of the accumulator tank and the injection line is not necessary because the saturation temperature of the solution is less than 15.5°C (60°F) and the equipment room temperature is maintained above that value at all times when SLC injection is required to be operable.

The design features of SLC and its supporting systems are adequate to ensure that potential adverse systems interactions are not significant.

19A.6.1.5 Passive Containment Cooling System (PCCS)

19A.6.1.5.1 Design Features

PCCS removes the core decay heat rejected to the containment after a LOCA. It provides containment cooling for a minimum of 72 hours post-LOCA, with containment pressure never exceeding its design pressure limit, and with the IC/PCCS pool inventory not being replenished. After 72 hours, the PCCS Vent Fans are operated to remove non-condensable gases from the PCCS tubes to increase heat transfer efficiency so that containment pressure is reduced.

19A.6.1.5.2 System Interfaces

PCCS interfaces with the following systems: Containment, FAPCS, ICS, Suppression Pool, and RWCU/SDC piping.

19A.6.1.5.3 Analysis of Potential Adverse System Interactions

Due to their similar passive designs and physical arrangements, PCCS and ICS have similar considerations for potential adverse interactions. In addition, PCCS is dependent on successful operation of the drywell to wetwell vacuum breakers, which are safety-related.

19A.6.2 Further Assessment of Potential Adverse System Interactions

As the ESBWR design evolves, more details are available to support the recognition of potential adverse systems interactions (ASI). The consideration of ASI is an ongoing facet of the design as well as the PRA. Accordingly, additional ASI assessments beyond the scope provided in Subsection 19A.6.1 have been conducted.

The importance of identifying potential unwanted interactions is recognized and an effort is made to assess systems for adverse functional, spatial or human interface interactions that may be present in the ESBWR design. While not meant to be exclusive, a potential adverse system interaction may exist in instances where:

1. Redundant portions of passive systems or their auxiliary support functions that are considered independent in the design and accident analysis could be degraded.
2. A passive system is degraded by a non-safety system.
3. Operator interface could degrade the operation of passive systems.

The ESBWR active and passive systems were assessed independently of whether or not one system is designed to be dependent on another. Many potential interactions were found to be addressed through design requirements or operational programs. Those interactions are captured as key insights in the PRA.

19A.6.2.1 Assessment of Potential Adverse Functional Interactions

For assessment of functional interactions, active and passive ESBWR PRA systems have been examined to identify relationships among the passive safety systems, as well as between the safety and non-safety systems, that may not have been considered in the design. The restricted number

of the ESBWR safety systems and components limits the potential for adverse interactions to affect safety systems. No risk-significant functional interactions have been discovered that are not already adequately identified in the design or through operational programs.

19A.6.2.2 Assessment of Potential Adverse Spatial Interactions

Spatial interactions are broadly considered in the design for flood protection, missile protection, protection against the dynamic effects of high energy line breaks, seismic design and fire protection. These interactions are also considered in the PRA. During the assessment of potential adverse system interactions, an issue was discovered that relates to Main Control Room (MCR) habitability under certain post-LOCA containment cooling with fuel failure. A potentially adverse interaction could arise due to the need to filter the MCR habitability area. The filtering is necessary to avoid the additional dose that could be generated during certain conditions for which MCR habitability must be considered.

The potentially adverse interaction involves the need to process contaminated air expected following fuel damage. The processing of contaminated water occurs within the Reactor Building. Reactor Building HVAC accident exhaust filters ensure that effluent from the Reactor Building is controlled so that dose levels in the MCR remain within acceptable limits. Contaminated air from the Reactor Building must be processed following fuel damage. Subsection 5.4.8 describes post-LOCA cooling with fuel failure during which time the accident exhaust filters would be required to operate in order to prevent exceeding the MCR dose limits.

If the accident exhaust filters do not perform with adequate efficiency, unacceptably high dose levels could occur in the MCR. Therefore, it is prudent to place increased regulatory treatment on these filters as an added measure to ensure acceptable performance.

The assessment did not identify any other potential adverse spatial interactions not already addressed in the design or by an operating program.

19A.6.2.3 Assessment of Potential Adverse Operator Interface

Human interface acts of commission were not specifically modeled in the ESBWR PRA. However, for operator actions, there is uncertainty about how the ESBWR operating guidelines might differ from the guidelines for existing plants and, therefore, how operator actions that are undesired in the ESBWR PRA accident sequences might be induced.

A potential adverse interaction between operators and equipment was found to exist for certain initiating events where the lower drywell hatch is open during shutdown. The assessment of shutdown initiating events reveals that the lower drywell hatches should have regulatory oversight.

Specifically, a LOCA below the core with the lower hatch open could result in the inability to maintain core coverage. It will be necessary, therefore, for the operators to close the lower hatch within a certain time frame.

Because of the importance of maintaining the single ability to close the lower hatch during shutdown in order to be able to keep the core covered during breaks below core level, the hatch closure function should be subject to regulatory oversight.

The assessment did not identify any other adverse operator interfaces not already addressed by design or operational program requirements.

19A.6.2.4 Conclusion

Based on the assessment of potential adverse systems interaction for the ESBWR, together with design and procedure controls, there is reasonable assurance that the more risk significant interactions are recognized and appropriate action has been taken to address them through design, procedures or regulatory oversight.

With two exceptions, potential adverse system interactions are addressed by design or operating program requirements. For those two instances, the interactions are important enough to be designated RTNSS under Criterion E, and be subjected to increased regulatory oversight.

The Reactor Building HVAC accident exhaust filters and the lower drywell hatches discussed under Subsections 19A.6.2.2 and 19A.6.2.3, respectively, require increased regulatory oversight. The specific oversight mechanisms are indicated in Table 19A-2.

19A.7 Selection of Important Nonsafety-Related Systems

As described above, the selection of RTNSS systems considers nonsafety-related SSCs that are necessary to meet NRC regulations, safety goal guidelines, and containment performance goal objectives. RTNSS systems needed to meet the NRC regulations specified in Criteria A, B and E are based on deterministic analyses. RTNSS systems needed to meet Criteria C and D are based on probabilistic insights.

Regulatory oversight is recommended for all RTNSS systems, commensurate with their risk significance. Important RTNSS systems have a relative high risk significance, and a more robust regulatory treatment, as discussed in Section 19A.8. RTNSS systems are evaluated in the focused PRA sensitivity studies to ensure that the combination of safety-related and nonsafety-related systems meets the safety goal guidelines. If the focused PRA analysis determines that a RTNSS system is necessary to meet the NRC safety goal guidelines, then it is considered as High Regulatory Oversight, otherwise, it is considered as Low Regulatory Oversight. The risk significance of each RTNSS system is discussed in Subsection 19A.8.4. Results of the regulatory treatment assessment are summarized in Table 19A-2.

19A.8 Proposed Regulatory Oversight

19A.8.1 Regulatory Oversight – Availability Treatment

Regulatory oversight is applied to each system designated as RTNSS to ensure that it has sufficient reliability and availability to perform its RTNSS function, as defined by the focused PRA, or

deterministic criteria. Oversight is applied in the form of availability controls, including Maintenance Rule performance monitoring for all RTNSS functions, and either Availability Controls Manual or Technical Specifications. The extent of oversight is commensurate with the safety significance of the RTNSS function, and is categorized as either High Regulatory Oversight (HRO), Low Regulatory Oversight (LRO), or Support.

HRO – If the focused PRA analysis determines that a RTNSS system is significant to public health and safety (that is, necessary to meet the NRC safety goals) then it is classified as HRO. Technical Specification Limiting Condition for Operation is established for the system/component, in accordance with 10 CFR 50.36.

LRO – If a RTNSS system is not significant, as described above, then the proposed level of regulatory oversight is Low Regulatory Oversight (LRO), which is addressed in regulatory availability specifications, which are described in the Availability Controls Manual in this appendix.

Support – These systems are LRO and they provide support (generally component and room cooling) for RTNSS systems that provide active mitigation functions. Treatment of support systems relative to the systems they support is described in the Availability Controls Manual in this appendix.

19A.8.2 Reliability Assurance

All RTNSS systems shall be in the scope of the Design Reliability Assurance Program, as directed by Section 17.4, which will be incorporated into the Maintenance Rule program.

Quality assurance controls for RTNSS SSCs are addressed in Subsection 17.1.22, which states that nonsafety-related structures, systems and components (SSCs) that perform safety significant functions have quality assurance requirements applied commensurate with the importance of the items function. The identification of nonsafety-related structures, systems and components and their quality classification is shown in Table 3.2-1.

19A.8.3 Augmented Design Standards

Systems that meet RTNSS Criterion B (that is, for actions required beyond 72 hours and seismic events) require augmented design standards to assure reliable performance in the event of hazards, such as seismic events, high winds, flooding, and environmental conditions experienced during an accident.

RTNSS B components are required to function following a seismic event and they are designed to Seismic Category II, at a minimum. (Some RTNSS B structures are Seismic Category I due to safety-related equipment within). Because these systems are designated to perform their function post 72 hours, the equipment does not need to be able to perform their functions during the seismic event, but must be available following the event. The structures housing RTNSS B components are identified in Table 19A-3. In addition, any non-RTNSS system that can adversely interact with RTNSS B systems are designed to the same seismic requirements as the affected RTNSS system.

RTNSS Criterion B equipment are qualified to IEEE-344-1987 to demonstrate seismic performance and structural integrity.

In addition to seismic standards, Seismic Category II structures that house RTNSS Criterion B equipment are designed to withstand missiles generated from Category 5 hurricanes at (313.8 km/hr) 195 mph, 3-sec gust. As with seismic, the systems do not need to perform their functions during the high wind event, but must be available following the event. Table 19A-4 discusses the capability of structures housing RTNSS B components with respect to flooding, winds and wind-generated missiles.

The plant design for protection of SSCs from the effects of flooding considers the relevant requirements of General Design Criterion 2, “Design Bases for Protection Against Natural Phenomena,” and 10 CFR Part 100, Appendix A, “Seismic and Geologic Siting Criteria for Nuclear Power Plants,” Section IV.C as related to protecting safety-related SSCs from the effects of floods, tsunamis and seiches. The design meets the guidelines of Regulatory Guide 1.59 with regard to the methods utilized for establishing the probable maximum flood (PMF), probable maximum precipitation (PMP), seiche and other pertinent hydrologic considerations, and the guidelines of Regulatory Guide 1.102 regarding the means utilized for protection of safety-related SSCs from the effects of the PMF and PMP. To ensure that RTNSS systems are protected from flood-related effects associated with fluid piping and component failures, they are located above the maximum internal flooding level analyzed by Section 3.4.

To provide assurance that RTNSS components are capable of performing in any anticipated environmental conditions, they are designed with the following requirements:

1. RTNSS components inside containment are designed, procured, and maintained in accordance with the environmental requirements of the environmental qualification (EQ) program, as described in, Sections 3.9, 3.10, and 3.11.
2. RTNSS components outside the containment are required to be designed and procured with the requirement that they remain functional in any anticipated environmental conditions.

Systems that meet RTNSS Criteria A, C, D, or E do not require augmented design standards described above, but must incorporate the defense-in-depth principles of redundancy and physical separation to ensure adequate reliability and availability.

RTNSS C systems do not require augmented seismic design criteria. However, some RTNSS C systems are housed in Seismic Category I or II structures, and some are housed in non-seismic structures that are designed using the International Building Code – 2003 by International Code Council, Inc. (IBC-2003) to maintain structural integrity under SSE conditions. Non-seismic structures that house RTNSS Criterion C systems are seismically designed using dynamic analysis method with the SSE ground input motion equal to two-thirds of the Certified Seismic Design Spectra taken from Figures 2.0-1 and 2.0-2 adjusted as required to their bases. An Occupancy Importance Factor of 1.5, Response Modification Factor of 2 and Seismic Design Category

D/Seismic Use Group III apply to these structures. RTNSS C systems and components are designed to the seismic requirements of IBC-2003 consistent with the above SSE ground motion.

Seismic Category NS structures that house RTNSS Criterion C equipment are designed to withstand wind and missiles generated from Category 5 hurricanes at 195 mph (313.8 km/hr), 3-sec gust. Seismic Category II structures that house RTNSS Criterion C equipment are designed to withstand missiles generated from Category 5 hurricanes at (313.8 km/hr) 195 mph, 3-sec gust. Table 19A-4 discusses the capability of structures housing RTNSS C components with respect to flooding, winds and wind-generated missiles. RTNSS Criterion C equipment are qualified to IEEE-344-1987 to only demonstrate structural integrity. RTNSS C components are not required to remain functional following a seismic event. The seismic margins analysis results indicate that RTNSS C components are not required to function in order to avoid core damage following a seismic event. In addition, any non-RTNSS system that can adversely interact with RTNSS C systems are designed to the same seismic requirements as the affected RTNSS system.

The hurricane missile spectrum for Seismic Category NS and Seismic Category II structures that house RTNSS equipment is consistent with the tornado missile spectrum identified in Table 2.0-1. The design criteria associated with hurricane missile protection follows Section 3.5 for missiles generated by natural phenomenon. The tornado wind speed is substituted with hurricane wind speed to design the concrete or steel barriers for missile impact.

19A.8.4 Regulatory Treatment

The proposed regulatory treatment of RTNSS systems is presented below, and is summarized in Tables 19A-2, 19A-3 and 19A-4.

19A.8.4.1 Nonsafety-Related ATWS Actuation Logic

ATWS actuation logic provides backup reactor shutdown methods that are diverse from the safety-related reactor protection system. Alternate Rod Insertion, Feedwater Runback, and ADS Inhibit use DPS to perform their actuation functions. These functions are RTNSS Criterion A relative to the ATWS Rule, 10 CFR 50.62. They do not have a high risk significance due to the redundancy and diversity of the reactor protection system. The proposed level of regulatory oversight for these functions is in the Availability Controls Manual.

19A.8.4.2 FPS Pool Cooling Makeup

The diesel-driven and motor-driven FPS pumps, and associated tanks, piping and valves, are RTNSS Criterion B. The pumps and the FPS piping and valves are classified as nonsafety-related but are designed so that the necessary portions of the system remain available following a seismic event to keep equipment required for safe shutdown free from fire damage during a safe shutdown earthquake. In conjunction with the pumps, FPS makeup includes the water supply, the suction pipe from the water supply to the pump, one of the supply pipes from the FPE to the Reactor Building

and Fuel Building, and the connections to the FAPCS. Loss of this function does not challenge the CDF or LRF goals. Therefore, the proposed level of regulatory oversight for this function is in the Availability Controls Manual.

19A.8.4.3 Diverse Protection System

DPS provides diverse actuation functions that enhance the plant's ability to mitigate dominant accident sequences involving the common cause failure of actuation logic or controls. The following functions of DPS are significant with respect to the focused PRA sensitivity study to meet the NRC safety goal guidelines: ADS actuation, GDCS actuation, RWCU/SDC valve isolation, and IC/PCCS Pool Connection valves actuation. The risk significance is high for the special case of the focused PRA, such that the proposed level of regulatory oversight for the portions of DPS that provide these functions are contained in Technical Specifications.

DPS provides backup shutdown methods for ATWS mitigation, as described in Subsection 19A.8.4.1.

In addition, DPS provides the following backup functions that are modeled in the PRA:

- Scram
- MSIV Closure
- SRV Actuation
- FMCRD Actuation
- ICS Actuation (Condensate Return Valve and Vent Valve Opening Signals)
- SLC Actuation for LOCA
- ADS Inhibit Function

These functions do not have a high risk significance, so their proposed level of regulatory oversight is in the Availability Controls Manual.

19A.8.4.4 Post-Accident Monitoring

Post-accident monitoring is performed by Q-DCIS. Operability of the post-accident monitoring instrumentation is addressed in Technical Specification LCO 3.3.3.2, "Post-Accident Monitoring (PAM) Instrumentation." Support for the safety-related post-accident monitoring instrumentation is necessary for component cooling and lighting. The CRHAVS air handling units and auxiliary heating and cooling units ensure that, after 72 hours, room temperatures for equipment used in post-accident monitoring are within the range for qualified operation. Emergency lighting assists the operators in post-accident monitoring activities. These functions provide long-term support and are RTNSS Criterion B. Because they are not required for the first 72 hours, they do not affect core cooling or containment heat removal in the PRA, and thus have low risk significance. The proposed level of regulatory oversight for emergency lighting is in the Maintenance Rule and the proposed level of oversight for heating/cooling is in the Availability Controls Manual.

19A.8.4.5 Basemat Internal Melt Arrest and Coolability System and GDCS Deluge Lines

The BiMAC device and GDCS deluge valves play an important role in mitigating core melt scenarios. Therefore, they are candidates for RTNSS consideration. The BiMAC device and GDCS valves function during severe accidents, and thus have no effect on the Level 1 PRA. The inclusion of the BiMAC device in the ESBWR design provides an engineered method to assure heat transfer between the debris bed and cooling water. By flooding the lower drywell after the introduction of core material, the potential for energetic fuel-coolant interaction is minimized. Covering core debris with water provides scrubbing of fission products released from the debris and cools the corium, limiting potential core-concrete interaction (CCI). The BiMAC device provides additional assurance of debris bed cooling by providing engineered pathways for water flow through the debris bed. BiMAC failure can occur if no water is supplied. Other failure mechanisms include manufacturing defects, unforeseen phenomenology problems or a broken GDCS line that would divert flow. In these instances, the situation becomes similar to flooding the debris bed without the engineered flow through the corium. Thus, BiMAC failure to function can be conservatively modeled as failure to supply water from the GDCS deluge lines.

Loss of the BiMAC function does not pose a challenge to the LRF goals when other safety-related and RTNSS systems are taken into account. The proposed level of regulatory oversight for the BiMAC function is in the Availability Controls Manual.

19A.8.4.6 Nonsafety-Related Distributed Control and Information System

The Nonsafety-Related Distributed Control and Information System (N-DCIS) performs control functions for several RTNSS functions. N-DCIS provides uninterruptible AC power with battery backup for at least two hours. For loss of offsite power events or loss of battery backup, N-DCIS is operated from the PIP buses powered from the standby diesel generators. The following RTNSS functions are supported by N-DCIS:

- DPS
- RCCWS
- FAPCS
- PSWS
- Standby Diesel Generators
- Nuclear Island Chilled Water System
- 6.9 kV PIP buses

The proposed regulatory oversight for N-DCIS, in support of RTNSS functions, is addressed in the Maintenance Rule.

19A.8.4.7 Fuel and Auxiliary Pools Cooling System

FAPCS can supply core cooling and containment heat removal in certain non-seismic PRA sequences as a backup to passive safety functions. FAPCS and its supporting functions (e.g., AC power and component cooling) are therefore RTNSS systems. The loss of any train of FAPCS does not challenge the goals for CDF or LRF, so the proposed level of regulatory oversight for these functions is in the Availability Controls Manual.

19A.8.4.8 AC Power System

The Standby Diesel Generators and PIP buses provide standby AC power to support FAPCS in non-seismic PRA sequences (Criterion C). The Diesel Generators and PIP buses do not challenge the NRC safety goal guidelines, and as such, the proposed level of regulatory oversight for this function is in the Availability Controls Manual.

The Ancillary Diesel Generators and associated 480V buses power the motor-driven FPS pump (core cooling), the PCCS Vent Fans (containment integrity), the main control room emergency filter units (control room habitability) and Q-DCIS (post-accident monitoring). In addition, ancillary AC power provides backup power to the control room air handling units. Like standby AC power, the NRC safety goal guidelines are met without ancillary AC power and therefore, the proposed level of regulatory oversight is addressed in the Availability Controls Manual.

19A.8.4.9 Component Cooling – HVAC, Cooling Water, Chilled Water, and Plant Service Water

To support post-accident monitoring beyond 72 hours, it is necessary to provide component cooling to the Q-DCIS components. Long-term post-accident monitoring (RTNSS B) component cooling for Q-DCIS cabinets in the Reactor Building is provided by local cooling from the Reactor Building HVAC System, and the Ancillary Diesel Building HVAC supports the Ancillary Diesel Generators.

To support FAPCS (RTNSS C), component cooling is needed for FAPCS and the following support equipment: Standby Diesel Generators, PIP Buses, N-DCIS local cabinets, RCCWS, and Nuclear Island Chilled Water System. FAPCS cooling is performed by RCCWS and the room cooler portion of the Fuel Building HVAC System. The Standby Diesel Generators are cooled by RCCWS and the Electrical Building HVAC System. The PIP Buses, and associated N-DCIS support are also cooled by the Electrical Building HVAC System. RCCWS, Nuclear Island Chilled Water System, and associated N-DCIS support cooling is performed by the room cooler portions of the Turbine Building HVAC System.

The risk significance for these supporting functions is commensurate with the functions that they support. The proposed level of regulatory oversight for these functions is covered under the evaluations of the supported systems. The Availability Controls Manual addresses degraded or lost support systems in the context of the supported functions. No explicit availability controls are supplied for these support systems, because they are frequently or continuously operating during normal plant operations, so additional availability control surveillance requirements are not

beneficial. In addition, performance monitoring of RTNSS components is required by the Maintenance Rule.

19A.8.4.10 Long-Term Containment Integrity

Long-term containment pressure control is accomplished by a combination of passive auto-catalytic recombiners (PARs) in the containment airspaces and PCCS Vent Fans, which are operated to remove the non-condensable gases from the PCCS tubes to increase heat transfer efficiency.

PARs are independently mounted components which are capable of recombining a stochiometric mix of hydrogen and oxygen into water vapor. This recombination is facilitated through the use of a selective metal catalyst, and requires no external power or controls. A Passive Containment Cooling vent fan takes suction off of each PCCS vent line and exhausts to the GDCS pool. The fan aids in the long-term removal of non-condensable gas from the PCCS for continued condenser efficiency. The fans are operated by operator action and are powered by a reliable power source which has a diesel generator backed up by an ancillary diesel if necessary without the need to enter the primary containment.

Igniters (glow plugs) in the lower drums of the PCCS condensers recombine the hydrogen and oxygen at lower concentrations, thereby keeping the resultant internal pressure of the PCCS condensers within acceptable limits to ensure there is no plastic deformation during a detonation under severe accident conditions.

The PARs and PCCS vent fans maintain containment pressure below the design pressure by counteracting a slight increase in noncondensable gases over time. The PCCS igniters prevent combustible gas deflagration from adversely challenging the integrity of the PCCS heat exchangers. These components are not risk-significant and the proposed regulatory oversight is in the Availability Controls Manual.

19A.8.4.11 Reactor Building HVAC Accident Exhaust Filters

The reactor building contaminated area ventilation system filters (Reactor Building HVAC Accident Exhaust Filters only) must maintain the required filtering efficiency to ensure that theoretical control room doses are not exceeded for certain beyond design basis LOCAs. Failure to provide adequate filtration is considered to be an adverse system interaction. They have regulatory oversight in the Availability Controls Manual to provide assurance that they are capable of performing their function.

19A.8.4.12 Lower Drywell Hatches

An equipment hatch for removal of equipment during maintenance and an air lock for entry of personnel are provided in the lower drywell. These access openings are sealed under normal plant operation but may be opened when the plant is shut down. Closure of both hatches is required for the shutdown Loss-of-Coolant-Accident (LOCA) below top of active fuel (TAF) initiators during MODES 5 and 6. Due to the low frequency of occurrence, this function is not risk-significant and the proposed regulatory oversight is in the Availability Controls Manual.

19A.8.4.13 Standby Liquid Control System Actuation/Feedwater Runback Logic

The regulatory treatment of the ATWS actuation logic and Feedwater Runback Logic functions is provided in Subsection 19A.8.4.1, and the treatment of the SLC actuation for LOCA is provided in Subsection 19A.8.4.3. These functions are included in the Availability Controls Manual.

19A.8.4.14 Control Room Habitability – Long-Term Cooling

The regulatory treatment of the control room habitability function is provided in Subsection 19A.8.4.9, along with the treatment of the ancillary AC power that supplies backup power to the control room air handling units. The function is included in the Availability Controls Manual.

19A.8.5 COL Information

None.

19A.8.6 References

None.

Table 19A-1 (Deleted)

Table 19A-2 RTNSS Functions (Sheet 1 of 2)

RTNSS Function	Description	Availability Controls
DPS – ARI Actuation	A - ATWS Rule	ACLCO 3.3.1
DPS – FWRB Actuation	A - ATWS Rule	ACLCO 3.3.3
DPS – ADS Inhibit	A - ATWS Rule	ACLCO 3.3.4
FPS Diesel Driven Pump	B - Long Term Core Cooling: RPV At-Power and Spent Fuel Pool; Long Term Containment Integrity	ACLCO 3.7.1
FPS Motor Driven Pump	B - Long Term Core Cooling: RPV At-Power and Spent Fuel Pool; Long Term Containment Integrity	ACLCO 3.7.1
FPS to FAPCS Connection Piping	B - Long Term Core Cooling: RPV At-Power and Spent Fuel Pool; Long Term Containment Integrity	ACLCO 3.7.1
PARs	B - Long Term Containment Integrity	ACLCO 3.6.2
PCCS Vent Fans	B - Long Term Containment Integrity	ACLCO 3.6.3
Emergency Lighting	B - Post-Accident Monitoring	Maintenance Rule
DPS – GDCS Injection Mode and Equalize Mode Actuation	C - Focused PRA (CDF, LRF) High Regulatory Oversight	TS LCO 3.3.8.1
DPS – ADS Actuation	C - Focused PRA (CDF, LRF) High Regulatory Oversight	TS LCO 3.3.8.1
DPS – Open IC/PCCS Pool Cross-Connect Valves	C - Focused PRA (CDF, LRF) High Regulatory Oversight	TS LCO 3.3.8.1
DPS – Isolation RWCU/SDC Valves	C - Focused PRA (CDF, LRF) High Regulatory Oversight	TS LCO 3.3.8.1
DPS – Scram	C - Focused PRA (CDF, LRF)	ACLCO 3.3.4
DPS – MSIV Closure	C - Focused PRA (CDF, LRF)	ACLCO 3.3.4
DPS – SRV Actuation	C - Focused PRA (CDF, LRF)	ACLCO 3.3.4
DPS- FMCRD Actuation	C - Focused PRA (CDF, LRF)	ACLCO 3.3.4
DPS – ICS Actuation (Condensate Return Valve and Vent Valve)	C - Focused PRA (CDF, LRF)	ACLCO 3.3.4
DPS – SLC Actuation LOCA	C - Focused PRA (CDF, LRF)	ACLCO 3.3.4
FAPCS (LPCI, SPC Modes)	C - Focused PRA (Uncertainty)	ACLCO 3.7.2 ACLCO 3.7.3
BiMAC Device	D - Containment Performance	AC 4.1
GDCS Deluge Valves	D – Containment Performance	ACLCO 3.5.1
PCCS Igniters	D- Containment Performance	ACLCO 3.6.4
Reactor Building HVAC Accident Exhaust Filters	E – Adverse System Interactions	ACLCO 3.7.4
Lower Drywell Hatches	E – Adverse System Interactions	ACLCO 3.6.1
FPS Water Tank	B - Supports core cooling for refill of pools	ACLCO 3.7.1

Table 19A-2 RTNSS Functions (Sheet 2 of 2)

RTNSS Function	Description	Availability Controls
FPS Diesel Fuel Oil Tank	B - Supports Diesel Driven FPS pump	ACLCO 3.7.1
Ancillary Diesel Generators	B - Supports FPS Motor Driven Pump, PCCS Vent Fans, CRHAVS AHUs, Emergency Lighting, Q-DCIS	ACLCO 3.8.3
Ancillary AC Power Buses	B - AC power distribution from Ancillary Diesel Generators to plant loads.	Maintenance Rule
Ancillary DG Fuel Oil Tank	B - Supports Ancillary Diesel Generators	Maintenance Rule
Ancillary DG Fuel Oil Transfer Pump	B - Supports Ancillary Diesel Generators	Maintenance Rule
Ancillary Diesel Building HVAC	B – Supports Ancillary Diesel Generators	Maintenance Rule
N-DCIS	C - The portions that support DPS, FAPCS and supporting equipment	Maintenance Rule
Standby Diesel Generators	C - Supports FAPCS operation	ACLCO 3.8.1, ACLCO 3.8.2
6.9 kV PIP Buses	C - AC power distribution from Standby Diesel Generators to plant loads associated with FAPCS	Maintenance Rule
Standby DG Auxiliaries	C - Supports Standby DG	Maintenance Rule
RCCWS	C - Supports Standby Diesel Generators and Nuclear Island Chilled Water Subsystem (NICWS)	Maintenance Rule
Nuclear Island Chilled Water	C – Building HVAC	Maintenance Rule
PSWS	C - Supports RCCWS	Maintenance Rule
Electrical Building HVAC Area Cooling	C - Supports PIP Buses, N-DCIS for FAPCS	Maintenance Rule
Fuel Building HVAC Local Cooling	C - Supports FAPCS, N-DCIS for FAPCS	Maintenance Rule
Reactor Building HVAC Local Cooling	C - Supports N-DCIS for FAPCS	Maintenance Rule
Turbine Building HVAC Local Cooling	C – Supports FAPCS	Maintenance Rule
CRHAVS Air Handling Units	B - Long-term control room habitability	ACLCO 3.7.5
CRHAVS Air Handling Unit auxiliary heaters and coolers	B - Cooling for post-accident monitoring heat loads	ACLCO 3.7.5

Note:

1. All RTNSS functions have Maintenance Rule availability controls.

Table 19A-3 Structures Housing RTNSS Functions

System	RTNSS Criterion	Location	Building Category
FPS Diesel Driven Pump	B	Fire Pump Enclosure	Seismic Cat. I
FPS Motor Driven Pump	B	Fire Pump Enclosure	Seismic Cat. I
FPS to FAPCS Connection	B	Reactor Building	Seismic Cat. I
PARs	B	Containment	Seismic Cat. I
PCCS Vent Fans	B	Containment	Seismic Cat. I
CRHAVS Air Handling Units	B	Control Building	Seismic Cat. I
Emergency Lighting	B	Control Building	Seismic Cat. I
FPS Water Tank	B	Fire Pump Enclosure	Seismic Cat. I
FPS Diesel Fuel Oil Tank	B	Fire Pump Enclosure	Seismic Cat. I
Ancillary Diesel Generators	B	Ancillary DG Building	Seismic Cat. II
Ancillary AC Power Buses	B	Ancillary DG Building	Seismic Cat. II
Ancillary DG Fuel Oil Tank	B	Ancillary DG Building	Seismic Cat. II
Ancillary DG Fuel Oil Transfer Pump	B	Ancillary DG Building	Seismic Cat. II
Ancillary Diesel Building HVAC	B	Ancillary DG Building	Seismic Cat. II
CRHAVS Air Handling Unit auxiliary heaters and coolers	B	Control Building	Seismic Cat. I

Notes:

1. RTNSS components that support the RTNSS functions for the systems shown in Table 19A-3 are designed/installed with similar protection from missiles and flooding described in Table 19A-4.
2. Seismic Category I and II structures that house RTNSS equipment are not required to be designed to withstand hurricane Category 5 wind velocity at 87.2 m/s (195 mph), 3- second gust but are required to be designed to withstand 100-year wind velocity at 67.1 m/s (150 mph) identified in Table 2.0-1.
3. The hurricane missile spectrum for Seismic Category II structures that house RTNSS equipment is consistent with the tornado missile spectrum identified in Table 2.0-1. The design criteria associated with hurricane missile protection follows Section 3.5 for missiles generated by natural phenomenon. The tornado wind speed is substituted with hurricane wind speed to design the concrete or steel barriers for missile impact.

Table 19A-4 Capability of RTNSS Related Structures[(1)(2)](Sheet 1 of 2)

System Location	A. (Internal Flooding)	B. (External Flooding)	C. (Internal Missiles)	D. (Extreme Wind and Missiles)
Reactor Bldg. (RB) Control Bldg. (CB) Fuel Bldg. (FB) Fire Pump Enclosure Bldg. (FPE)	The design/installation of RTNSS equipment includes protection from the effects of internal flooding.	Seismic Category I structures are designed to withstand the flood level and groundwater level specified in Table 2.0-1 and described in Subsection 3.4.1.2. All exterior access openings are above flood level and exterior penetrations below design flood and groundwater levels are appropriately sealed as described in Subsection 3.4.1.1. On-site storage tanks are designed and constructed to minimize the risk of catastrophic failure and are located to allow drainage without damage to site facilities in the event of a tank rupture per Subsection 3.4.1.2.	There are no credible sources of internal missiles per Section 3.5.	Seismic Category I structures designed for tornado and extreme wind phenomena are described in Section 3.3 and Subsection 3.5.1.4.
Ancillary DG Building		The Ancillary DG Building is designed to withstand external flooding with the same acceptance criteria as a Seismic Category I Structure.		The Ancillary DG Building is designed for tornado wind loads. RTNSS systems in the Ancillary Diesel Building are protected from Category 5 hurricane missiles.

Table 19A-4 Capability of RTNSS Related Structures(1)(2)(Sheet 2 of 2)

System Location	A. (Internal Flooding)	B. (External Flooding)	C. (Internal Missiles)	D. (Extreme Wind and Missiles)
Electrical Bldg. (EB) Service Water Bldg. (SF) Turbine Bldg. (TB)	The design/installation of RTNSS equipment includes protection from the effects of internal flooding.	All exterior access openings are above flood level and exterior penetrations below design flood and groundwater levels are appropriately sealed; basemat and walls are designed for hydrostatic loading, therefore protected from external flooding.	N/A	The EB and SF are RTNSS Structures designed for Category 5 hurricane winds. RTNSS systems in the EB and SF are protected from Category 5 hurricane wind and missiles. The TB structure is designed for tornado wind loads. The design/installation of the RTNSS systems in the TB includes protection to comply with the requirement of Subsection 19A.8.3 to withstand missiles generated from Category 5 hurricanes.
PSW System located Outdoors Onsite	N/A	The design/installation of the RTNSS system includes protection from the effects of flooding.	N/A	The design/installation of the RTNSS system complies with the requirement of Subsection 19A.8.3 to withstand winds and missiles generated from Category 5 hurricanes.

Notes:

1. Seismic Category NS structures and PSW System located outdoors onsite that house RTNSS equipment are designed to withstand hurricane Category 5 wind velocity at 87.2 m/s (195 mph), 3-second gust. Seismic Category I and II structures that house RTNSS equipment are not required to be designed to withstand hurricane Category 5 wind velocity at 87.2 m/s (195 mph), 3-second gust but are required to be designed to withstand 100-year wind velocity at 67.1 m/s (150 mph) identified in Table 2.0-1.
2. The hurricane missile spectrum for Seismic Category NS, PSW System located outdoors onsite and Seismic Category II structures that house RTNSS equipment is consistent with the tornado missile spectrum identified in Table 2.0-1. The design criteria associated with hurricane missile protection follows Section 3.5 for missiles generated by natural phenomenon. The tornado wind speed is substituted with hurricane wind speed to design the concrete or steel barriers for missile impact.

Appendix 19B Deterministic Analysis For Containment Pressure Capability

19B.1 Introduction

This Appendix presents the deterministic analysis performed and results obtained for the containment ultimate capability under internal pressure in accordance with requirements in 10 CFR 50.44(c)(5) and SECY-93-087.

10 CFR 50.44(c)(5) states, “An applicant must perform an analysis that demonstrates containment structural integrity. This demonstration must use an analytical technique that is accepted by the NRC and include sufficient supporting justification to show that the technique describes the containment response to the structural loads involved. The analysis must address an accident that releases hydrogen generated from 100 percent fuel clad-coolant reaction accompanied by hydrogen burning. Systems necessary to ensure containment integrity must also be demonstrated to perform their function under these conditions”. RG 1.7 Revision 3 provides an acceptable method for demonstration of containment structural integrity in meeting the ASME Section III acceptance criteria as follows:

- That steel containments meet the requirements of the ASME Boiler and Pressure Vessel Code (Edition and Addenda as incorporated by reference in 10 CFR 50.55a(b)(1)), Section III, Division 1, Subarticle NE-3220, Service Level C Limits, considering pressure and dead load alone (evaluation of instability is not required).
- That concrete containments meet the requirements of the ASME Boiler and Pressure Vessel Code, Section III, Division 2, Subarticle CC-3720, Factored Load Category, considering pressure and dead load alone.

SECY-93-087, item J states “The containment should maintain its role as a reliable, leak-tight barrier by ensuring that containment stresses do not exceed ASME Service Level C limits for a minimum period of 24 hours following the onset of core damage, and that following this 24-hour period the containment should continue to provide a barrier against the uncontrolled release of fission products.”

Both sets of requirements are satisfied by performing a deterministic analysis, termed “Level C Evaluation”, to ensure that the Level C or Factored Load pressure capability of the containment structure is no less than 0.997 MPaG (145 psig) generated from 100 percent fuel clad-coolant reaction nor 0.62 MPaG (90 psig) resulting from more likely severe accident challenges, taking into account temperature effect on the material strength. The representative severe accident temperature considered is 260°C (500°F). The pressure units MPaG used in this appendix are gauge pressures unless noted otherwise.

The current Level C analysis provided herein is based on the updated temperature conditions used for the pressure capacity fragility described in more detail in Appendix 19C. The global analysis for the Level C capacity check for the Reinforced Concrete Containment Vessel (RCCV) and Liners is

updated for the new temperature conditions in the airspace under the drywell head, 260°C (500°F), and in the water in the reactor well and the equipment storage pool, 100°C (212°F), associated with the 260°C (500°F) steady state accident condition.

19B.2 RCCV and Liners

19B.2.1 Analysis Methods

A deterministic analysis is performed to demonstrate Level C pressure capability of the RCCV walls and liner. This analysis is based on detailed, 3D finite element modeling using the ANACAP-U concrete material model, Reference 19B-3, coupled to the ABAQUS/Standard finite element program, Reference 19B-2. The modeling and analysis methods are the same as employed for the probabilistic evaluation of pressure fragility, described in more detail in Appendix 19C. For Level C capacity, the material properties are based on specified design values, which represent lower bound values, and include degradation with temperature. The analysis considers nonlinear material response. The analysis includes dead load (weight and water pool pressures), but ignores the thermal strains leading to thermal induced stresses, in accordance with Regulatory Guide 1.7. The temperature distribution within the structure for evaluation of temperature dependent material properties is taken to be the steady state thermal condition where the drywell boundary is at 260°C (500°F). This represents an upper bound for drywell temperature for the most likely severe accidents. The wetwell temperature is defined based on a 0.0207 MPa (3 psi) pressure differential between the drywell and wetwell and assuming saturated conditions in the wetwell. The outside environment and interior rooms outside the containment correspond to winter conditions. The temperature distributions within the structure are established through a steady state thermal analysis. The stress analysis model is first initialized to be stress free at a uniform ambient temperature of 15.5°C (60°F), and the hydrostatic pressures for the various water pools and superstructure loads are applied on the model. Next, the design pressure of 0.31 MPaG (45 psig) along with the accident temperature distributions are incrementally applied to the model using static equilibrium iterations for nonlinear effects. Note that the coefficient of thermal expansion for all materials is set to zero to ignore thermal stresses. Finally, the internal pressure is incrementally increased, again using static equilibrium iterations, until the desired pressure is reached. The calculated stresses and strains are then evaluated to demonstrate structural integrity.

To meet the requirements of SECY-93-087 leakage requirements, the containment stresses (concrete, rebar, and liner) must meet the ASME allowable limits for factored loads for an internal pressure resulting from the most likely severe accident challenges. For the ESBWR, this pressure is 0.62 MPaG (90 psig) or 2.0 times the design pressure. To meet the requirements of 10 CFR 50.44, the containment must maintain its structural integrity for an internal pressure corresponding to an accident resulting in 100% fuel clad-coolant reaction. For the ESBWR, this is an internal pressure of 0.997 MPaG (145 psig) or 3.2 times design pressure. Table 19B-1 summarizes the ASME Level C or Factored Load Limits that are used to demonstrate structural integrity under these severe accident conditions.

19B.2.2 Model Description

The modeling for the stress analysis consists of a half-symmetric representation of the RCCV and the surrounding reactor building, including the basemat, the pedestal wall, the suppression pool floor slab, the upper drywell walls, the top slab, the upper pools structure and refueling floor, and the floors and walls of the reactor building, as illustrated in Figure 19B-1. This figure also shows the thermal contours for the temperature distribution associated with the 260°C (500°F) steady state thermal condition. The model is supported on an elastic layer of continuum elements representing the soil foundation. Solid (20-node continuum) elements with reduced Gaussian quadrature integration are used to model the reinforced concrete sections. The reinforcement bars are modeled as embedded, truss-like steel elements at the appropriate locations within the concrete elements. Membrane elements (plate elements without bending stiffness) are generally used to model the steel liners. These elements are attached to the nodes of the concrete elements for compatibility with the concrete deformations. This assumes that the liner anchorage system keeps the liners in contact with the concrete for this global modeling of the RCCV performance. Some plate bending elements are used for the thickened sections at connections. Representations for the large equipment hatches, personnel airlock penetrations, and the drywell head components are included using plate bending elements. Plate bending elements are also used to model the steel components of the internal structures, including the vent wall, diaphragm floor, reactor vessel shield wall, and the reactor pressure vessel support brackets.

The material properties used for the Level C analysis correspond to minimum design values. The structural properties are dependent on temperature and are summarized in the following tables. Table 19B-2 provides a summary of the elastic properties for steels, and Table 19B-3 provides a summary of the plastic properties of the steel materials. Table 19B-4 provides a summary of the concrete properties. All thermal properties are assumed to be constant with temperature and are summarized in Table 19B-5.

19B.2.3 Analysis Results

Figure 19B-2 plots contours of the minimum principal stress in the concrete at 0.992 MPaG (144 psig) or a load factor of 3.2 times design pressure to illustrate the concrete compressive stress distribution. This plot identifies the locations of elevated concrete stresses in four areas; a) on the RCCV wall below the suppression pool floor connection, b) on the bottom of the top slab around the drywell head opening, c) on the top surface of the top slab at the RCCV walls, and d) at the outside connection of the pedestal wall with the basemat. The peak compressive stresses identified in the plot are on the top surface of the top slab under the PCCS pool walls. Figure 19B-3 plots contours of the maximum principal strain in the concrete at 0.992 MPaG (144 psig) or a load factor of 3.2 times design pressure to illustrate the areas of concrete cracking and potential elevated rebar stresses. This plot indicates that the critical area for this loading is at the connection of the RCCV wall to the top slab and to a lesser extent at the connection of the RCCV wall to the suppression pool slab.

Table 19B-6 provides a summary of the maximum rebar and concrete stresses and the associated ratio to the ASME Level C (factored load) allowable limits at an internal pressure of 0.62 MPaG (90 psig) corresponding to the most likely severe accident conditions. All concrete and rebar stresses are found to be well below the ASME allowable limits for this pressure in accordance with the requirements of SECY-93-087.

Figure 19B-4 plots contours of maximum principal strains in the liner at 0.992 MPaG (144 psig) or 3.2 P_d, where P_d is the design pressure. This plot has the maximum strain contour value set to 0.3% corresponding to the ASME factored load allowable for membrane tension to identify the critical areas. The critical areas are at the RCCV wall connection with the suppression pool floor slab and at the connection with the top slab. Examination of individual element strains indicates that the two most critical areas are at the connection of the RCCV wall to the top slab under the location where the upper pool girders are connected across the top slab. Figure 19B-5 plots the maximum principal strain versus pressure at these two locations near these stiffness discontinuities, identified as points A and D in the figure. This peak strain includes membrane and bending and meets the 1% allowable limit. Figure 19B-6 plots the membrane strain in the liner at other representative points away from these discontinuities. This plot shows that the liner membrane strain remains below the allowable of 0.3% for an internal pressure of 0.997 MPaG (145 psig) pressure corresponding to 100% fuel clad-coolant reaction, even for the locations at the top slab connection but away from the discontinuity. All liner strains easily meet the ASME strain limits for 0.62 MPaG (90 psig) pressure or a load factor of 2.0 P_d. Thus, it is demonstrated through the nonlinear analysis that the liner remains a leak tight barrier for 0.997 MPaG (145 psig) pressure corresponding to 100% fuel clad-coolant reaction and meets the requirements of 10 CFR 50.44.

While not a requirement of 10 CFR 50.44, the peak rebar and concrete stresses along with the ratios to ASME factored load allowable limits are summarized in Table 19B-7 for a pressure of 0.992 MPaG (144 psig) or a load factor of 3.2 P_d. All concrete compressive stresses remain below the ASME allowable limit at this pressure level. The same local area identified in the liner strains shows some slight yielding in the rebar at this pressure level. These are the inner vertical bars in the RCCV wall and the bottom horizontal bars in the top slab at this connection, but only for a local area under the connection of the upper pool girders with the top slab. The table also identifies the maximum plastic strain levels found in the rebars for these locations. The largest plastic strain is 0.40%, which is almost within the ASME limit for liner membrane strain. Again, the peak response of these local rebars is just past the 0.2% yield and still well on the shoulder of the stress-strain curve. This level of plastic strain is well below the failure level for reinforcement steel, and the nonlinear analysis confirms the integrity of the RCCV walls and liner at this pressure level.

19B.2.4 Summary

The deterministic finite element analysis demonstrates that the RCCV and liner maintain structural integrity and provide a leak tight barrier per the requirements of SECY-93-087 for internal pressure corresponding to the most likely severe accident challenges and per the requirements of 10 CFR 50.44(c)(5) for pressures corresponding to 100% fuel clad-coolant reaction. The analysis uses lower bound material properties, including degradation with temperature. The modeling is consistent with the pressure fragility analyses in Appendix 19C, accounting for nonlinear material response, such as concrete cracking in tension with reduced shear stiffness, concrete yielding and strain softening in compression, and steel yielding and strain hardening in compression or tension. The concrete and rebar stresses and the liner strains remain within the ASME factored load allowable limits for 0.62 MPaG (90 psig) per the requirements of SECY-93-087. The concrete stresses also remain within the ASME allowable limit for factored load level even at 0.997 MPaG (145 psig) pressure. The liner strains are within the factored load allowable at 0.997 MPaG (145 psig). Some slight yielding of rebar develops at the 0.997 MPaG (145 psig) pressure level in local areas. It is thus demonstrated that the structural integrity of the RCCV and liner system is maintained for the more likely severe accident challenges and for the scenario for pressures generated from 100% fuel clad-coolant reaction.

An estimate of the actual Level C pressure capacity is determined using Figures 19B-5 and 19B-6 to find the internal pressure where the calculated liner strains reach the ASME allowable limits. Both the 1% strain for membrane plus bending at the discontinuity and the 0.3% hoop membrane strain away from discontinuities are reached near the same load factor. Thus, the Level C pressure capacity of the RCCV and Liner system is established at a load factor of 3.26 times the design pressure or 1.011 MPaG (146.5 psig) based on the deterministic design-based analysis.

19B.3 Drywell Head

Level C pressure capability of the drywell head is evaluated for pressure retaining parts (sleeve/torispherical head), bolted flange and anchor structures (flange plates/gusset plates).

The basic equation for Level C pressure capability is:

$$P_c = (S_c - \sigma_d)/\sigma_{up} \quad (19B\text{-}1)$$

where:

P_c	=	Level C pressure
S_c	=	Level C allowable stress at temperature 260°C (500°F)
σ_d	=	Stress due to dead load
σ_{up}	=	Stress due to unit pressure, 1 MPaG (145 psig)

Pressure retaining parts (sleeve and torispherical head) are evaluated based on the primary membrane stress Pm applying ASME Section III NE-3324, in which the maximum allowable stress S is taken to be Sy (material yield strength at temperature) as Level C stress limit in accordance with NE-3220. The local membrane stress PL and local membrane plus primary bending stress PL + Pb are non-controlling. Dead load (self-weight and hydrostatic pressure of the reactor well) is conservatively neglected.

The bolted flange is evaluated in accordance with ASME Section III, Division 1, Appendix XI. The average of longitudinal hub stress and radial flange stress, which is the most severe stress among the ones stipulated in article XI-3250, and the flange bolt stress stipulated in article XI-3220 of Appendix XI and Subsection NE-3230 are evaluated. Dead load is conservatively neglected.

Anchor structures (flange plates and gusset plates) are evaluated based on stress intensity applying ASME Section III NE-3221. Concrete compressive stress is evaluated in accordance with ASME Section III Division 2 CC-3421.1 for factored load limit. Dead load including reactor well hydrostatic pressure is considered for the evaluation of Level C capability of anchor structures.

The Level C pressure capabilities of each part of the drywell head are summarized in Table 19B-9. The governing pressure is 1.033 MPaG (150 psig), which is controlled by the lower flange plate of the anchorage.

19B.3.1 Buckling Analysis

An evaluation for the buckling capacity of the drywell head was analyzed using the ABAQUS finite element program (Reference 19B-2). An elastic-plastic analysis was analyzed including the effects of gross and local buckling, geometric imperfections, material nonlinearities, and large deformations as allowed in ASME Section III NE-3222 (Reference 19B-1) for establishing buckling stress values of torispherical heads. This analysis is used to determine the pressure capacity and

the failure mode, whether due to buckling under compressive hoop stress in the knuckle or due to tensile plastic failure in the dome region above the knuckle.

The first step in the analysis is to confirm and demonstrate that the torispherical head is modeled with sufficient resolution and that the analytical procedure is capable of capturing the buckling failure mode from compressive hoop stress in the knuckle region. To this end, a benchmark analysis was performed using the drywell head model, but modifying the thickness of the shell to simulate a torispherical shell configuration that exhibited this buckling failure mode when tested. The finite element model for the torispherical head including the top flange for this benchmark buckling study is shown in Figure 19B-7. The thickness of the shell elements in the analysis model was reduced so that the outside diameter to thickness, D/t, ratio matches that of a tested configuration reported in Reference 19B-4. The model is then clamped along the flanges, and an internal pressure load is incrementally applied until failure occurs in the analysis. The analysis model clearly predicts buckling failure at the same internal pressure where buckling occurred in an experimental test of a similar configuration. The analysis model considers a 10.4 m (34.12 ft) diameter torispherical head, based on the ESBWR design, but with the shell thickness reduced so that the diameter to thickness ratios match that of a tested configuration having a 4.92 m (16.14 ft) diameter. The parameters for the analysis model and the tested shell configuration are summarized in Table 19B-8, along with the comparison of the calculated and measured pressure causing buckling.

Figure 19B-8 plots the crown deflection to shell thickness ratio versus the load and shows the sudden snap back indicative of bifurcation type buckling failure. It is noted that torispherical heads can sustain significantly more internal pressure than that causing the first buckle in the knuckle region, as reported in Reference 19B-6. However, when the buckles develop, there is a temporary instability due to sudden volume change and sudden large changes in the material response, and these effects generally cause the numerical instability in the analysis. Figure 19B-9 plots the plastic strain contours for the buckled shape predicted by the analysis model. This benchmark analysis is in good agreement with experimental test data in predicting pressure causing buckling in the knuckle. Thus, it is concluded that the modeling has sufficient resolution and the analytical procedure employed has the required capability to capture buckling failure modes in the analyses for pressure capacity of the torispherical drywell head.

An analysis for the pressure capacity of the ESBWR drywell head configuration is thus performed using the design thickness of 40 mm (1.57 in) for the torispherical shell. This gives a value of 262 for the D/t parameter of the actual drywell head. Figure 19B-10 shows the finite element model used for the buckling analysis of the ESBWR drywell head. This model retains the same finite element mesh that was qualified in the buckling study above, but adds the tapered barrel section and flange thickness corresponding to the latest design configuration for the ESBWR drywell head. The analysis uses the lower bound or design values for the steel properties evaluated at 260°C (500°F), namely yield strength = 212.4 MPa (30.8 ksi), tensile strength = 483 MPa (70 ksi), and

minimum required elongation of 17%. The model is clamped along the bottom of the flange, and the internal pressure is incrementally increased to find the true pressure capacity. This analysis is performed at 260°C (500°F) and includes the external hydrostatic pressure of the water on the top of the head. Figure 19B-11 provides a plot of the crown deflection as a ratio of the shell thickness for the increasingly applied internal pressure load. The load factor is the multiplier on the design pressure of 0.31 MPaG (45 psig). Also indicated on this figure is the procedure described in Reference 19B-5 for identifying the axisymmetric yielding pressure, P_{c2}, developed from studies on a wide range of test configurations. Basically, the procedure is to find the value for D/t at first yield (point a), then take double this value for the same load (point b), draw a line through this point from the origin to intersect the displacement curve (point c), and read the corresponding pressure load (point d). This axisymmetric yield pressure is the internal pressure at which plastic yielding in the crown of the shell initiates leading to plastic failure of the shell. However, as noted in Reference 19B-5, P_{c2} is typically well below the actual failure pressure. As shown in the figure, the ABAQUS elastic plastic analysis calculates a similar but slightly higher value for this initiation of tensile yielding and also indicates that the shell still has significant reserve strength after the initiation of yielding in the crown. This analysis confirms that buckling in the knuckle region due to hoop compressive stress does not develop for the as-designed thickness of the drywell head.

To determine the pressure capacity of the drywell head due to tensile rupture in the dome, the pressure is incrementally increased until the strains reach the ductility limit of the material. In the dome, the material is under 1:1 biaxial tensile loading, and the ductility is limited to 50% of the elongation data determined from uniaxial specimens. The specified minimum elongation for A 516 Grade 70 material is 17% at ambient temperatures. This elongation reduces slightly (16.4%) up to temperatures of 260°C (500°F), then increases to about 24% at 538°C (1000°F). For this evaluation, the ductility or failure limit for the material is taken to be a plastic strain of 8%. Because the mesh is adequate (able to capture buckling) and there are no discontinuities in the region where failure will occur, no strain concentration factor for mesh fidelity is required. Figure 19B-12 plots contours of the equivalent plastic strain at mid-thickness for increasing internal pressure to illustrate the plastic deformations leading to tensile rupture in the dome. Initial yielding develops in the knuckle due to hoop compression and meridional tension. Once buckling in the knuckle is avoided, yielding and plastic deformations then concentrate in the dome due to biaxial tension “ballooning” in the dome and apex. At a load factor near 15, the ductility limit of 8% strain is reached and rupture of the dome will occur.

In previous analyses considering the torispherical head buckling study, the pressure capacity analysis was repeated considering initial imperfections in the geometry of the shell. The magnitudes of the geometric imperfections considered are based on the maximum allowed imperfections provided in ASME Section III NE-4222.2 of Reference 19B-1, namely that the shell surface shall not deviate outside the specified shape by more than 1-¼% of the head diameter or inside the specified shape by more than 5/8% of the diameter. While it is most likely that these

minimum and maximum deviations will only occur in one or two locations around the shell surface, as found in Reference 19B-6, a cosine type shape with six peaks in the half model was constructed. This evaluates whether such imperfections could trigger buckling in the knuckle region and change the mode of failure. The assumption is that the closer the imperfections are to the buckling shape, the more likely the chance that the imperfections could trigger the buckling. This analysis also confirmed that buckling did not develop for the actual drywell head configuration even in the presence of these assumed imperfections.

Figure 19B-13 plots the mid-thickness plastic strain in the crown with increasing pressure for the analysis at 260°C (500°F). Allowing for some conservatism, the pressure capacity for the drywell head is established at 12 P_d or an internal pressure of 3.72 MPaG (540 psig).

In summary, this analysis confirms that the drywell head will not buckle prior to tensile failure in the dome.

19B.4 Hatches and Airlocks

Level C pressure capabilities of hatches and personnel airlocks were evaluated for pressure retaining parts (sleeve/head for hatches, sleeve only for airlock), bolted flanges of hatches, sidewalls of airlocks and anchor structures (flange plates/gusset plates).

The basic equation for determining Level C pressure capability is the same as the drywell head described in Section 19B.3; however, stresses of hatches and air locks caused by dead load are small are negligibly small.

Pressure retaining parts are evaluated in a manner similar to the drywell head.

Bolted flanges of hatches are evaluated based on the stress analysis result applying ASME Section III, Division 1, Appendix XI and Subsection NE-3221.

Sidewalls of airlocks and anchor structures are evaluated based on stress intensity applying ASME Section III NE-3221.

The Level C pressure capabilities of each part of the hatches and airlocks are summarized in Table 19B-10. The governing pressure is 1.047 MPaG (152 psig), which is controlled by the inside gusset plate of the equipment hatch anchorage.

19B.5 Penetrations

The most critical of the RCCV penetrations are the main steam pipe penetrations. They have the largest flued head and anchor sleeves. Considering the loads transmitted by the main steam pipes, the maximum Level C pressure capability at temperature of 260°C (500°F) is 3.38 MPaG (490 psig).

19B.6 PCCS Heat Exchangers

The PCCS heat exchangers are part of containment boundary. The Level C pressure capacity of the most critical component in the PCCS heat exchangers is 38.7 Mpa (5613 psia).

19B.7 Summary

The Level C or Factored Load Category pressure capacities of various components of the containment structure are summarized in Table 19B-11. The limiting pressure is 1.011 MPaG (146.6 psig) associated with the strain limits in the liner. It is higher than 0.997 MPaG (145 psig) generated from 100 percent fuel clad-coolant reaction and 0.62 MPaG (90 psig) resulting from more likely severe accident challenges.

19B.8 References

19B-1 ASME 2004: Boiler and Pressure Vessel Code, Section III – Rules for Construction of Nuclear Power Plant Components, Division 1 – Subsection NE – Class MC Components.

19B-2 ABAQUS/Standard, Version 5.8, Hibbitt, Karlssen, and Sorensen, Inc., Pawtucket, RI, 1998.

19B-3 ANACAP-U, Version 2.5, Theory Manual, ANA-QA-145, ANATECH Corp., San Diego, CA, 1998.

19B-4 Galletly, G. D., “A Simple Design Equation for Preventing Buckling in Fabricated Torispherical Shells Under Internal Pressure,” Journal of Pressure Vessel Technology, Vol 108, pp 521-525, November 1986.

19B-5 Galletly, G. D. and Blachut, J., “Torispherical Shells Under Internal Pressure – Failure Due to Asymmetric Plastic Buckling or Axisymmetric Yielding,” Proceedings of the Institution of Mechanical Engineers, Vol 199, No C3, pp 225-238, 1985.

19B-6 Miller, C. D., Grove, R. B., and Bennett, J. G., “Pressure Testing of Large Scale Torispherical Heads Subject to Knuckle Buckling,” NUREG/CP-0065, August 1985.

19B-7 (Deleted)

Table 19B-1 Summary of ASME Factored Load Limits Used for Containment Integrity

Load	Concrete Stress	Rebar Stress	Liner Strain
Tension	N/A	0.9 σ_y	0.3% membrane 1.0% membrane + bending
Compression	0.60 f_c' membrane 0.75 f_c' membrane + bending	0.9 σ_y	0.5% membrane 1.4% membrane + bending

Table 19B-2 Summary of Steel Elastic Properties for Level C Analysis

	≤ 65.6°C (150°F)	121.1°C (250°F)	260°C (500°F)
Carbon Steel			
Modulus (GPa)	203.4	196.9	188.3
Poisson's Ratio	0.289	0.291	0.295
Stainless Steel			
Modulus (GPa)	200.0	192.0	180.0
Poisson's Ratio	0.295	0.301	0.311

SI to English Unit Conversion (SI units are the controlling units and English units are for reference only):

1 Pa = 1.45038×10^{-4} psi

Table 19B-3 Summary of Steel Plastic Properties for Level C Analysis

	≤65.6°C (150°F)	121.1°C (250°F)	260°C (500°F)
SA516 Grade 70			
Yield Stress (MPa)	262.1	235.9	212.4
Tensile Strength (MPa)	482.8	482.8	482.8
Elongation (%)	17.0	17.0	17.0
A572 Grade 50			
Yield Stress (MPa)	344.8	327.6	284.5
Tensile Strength (MPa)	448.3	425.9	369.8
Elongation (%)	18.0	18.0	18.0
A36			
Yield Stress (MPa)	248.3	235.9	204.8
Tensile Strength (MPa)	413.8	393.1	341.4
Elongation (%)	20.0	25.0	30.0
A709 HPS 70W			
Yield Stress (MPa)	482.8	458.6	398.3
Tensile Strength (MPa)	586.2	556.9	483.6
Elongation (%)	19.0	20.0	21.0
A615 Grade 60 Rebar			
Yield Stress (MPa)	413.8	377.7	327.5
Tensile Strength (MPa)	551.7	503.6	436.7
Elongation (%)	10.0	11.0	12.0
SA240 SS 304L			
0.2% Yield Stress (MPa)	172.4	139.3	112.4
Tensile Strength (MPa)	482.8	438.3	398.6
Elongation (%)	40.0	44.0	38.0
SA437 Grade B4B Bolting			
Yield Stress (MPa)	724.1(1)	693.4(2)	616.6(1)
Tensile Strength (MPa)	1000.0(1)	957.6(2)	851.5(1)
Elongation (%)	13.0(1)	12.7(2)	14.1(1)

Notes:

1. Table 19C-3.
2. Linearly interpolated between 65.6°C (150°F) and 260°C (500°F) values.

SI to English Unit Conversion (SI units are the controlling units and English units are for reference only):

1 Pa = 1.45038×10^{-4} psi

Table 19B-4 Summary of Concrete Properties for Level C Analysis

	≤65.6°C (150°F)	121.1°C (250°F)	260°C (500°F)
RCCV Concrete (5 ksi)			
Comp Strength (MPa)	34.48	28.58	25.91
Strain at Peak Comp (%)	0.19	0.22	0.27
Modulus (GPa)	27.80	18.58	14.83
Tensile Strength (MPa)	3.66	3.03	2.75
Fracture Strain (xE-6)	131.6	163.2	185.3
Poisson's Ratio	0.2	0.2	0.2
Basemat Concrete (4 ksi)			
Comp Strength (MPa)	27.59	22.86	20.73
Strain at Peak Comp (%)	0.19	0.22	0.27
Modulus (GPa)	24.86	16.62	13.26
Tensile Strength (MPa)	3.27	2.71	2.46
Fracture Strain (xE-6)	131.6	163.2	185.3
Poisson's Ratio	0.2	0.2	0.2

SI to English Unit Conversion (SI units are the controlling units and English units are for reference only):

1 Pa = 1.45038×10^{-4} psi

Table 19B-5 Summary of Thermal Material Properties

Material	Weight Density		Specific Heat		Thermal Conductivity	
	(lbf/ft^3)	(MN/m^3)	(Btu/lbm-^{o}F)	(J/kg-K)	(Btu/hr-ft-^{o}F)	(W/m-K)
Concrete	150	0.0235	0.210	879	0.92	1.6
Carbon Steel Liner	490	0.0770	0.110	460	30.9	53.5
Stainless Steel Liner	490	0.0770	0.118	494	9.42	16.3
Structural Steel	490	0.0770	0.110	460	30.9	53.5

SI units are the controlling units and English units are for reference only.

Table 19B-6 Summary of Maximum Stresses in Rebar and Concrete at 0.620 MPaG (90 psig) Pressure (Sheet 1 of 2)

Location	Maximum Rebar Tension		Maximum Rebar Compression		Maximum Concrete Compression	
	Stress, MPa (ksi)	Ratio to Allowable(1)	Stress, MPa (ksi)	Ratio to Allowable(1)	Stress, MPa (ksi)	Ratio to Allowable(2)
Top Slab					-8.27 (-1.20)	0.32
X-Bar Top	63.63 (9.229)	0.17	-20.39 (-2.957)	0.05	On top surface under pool girder at RCCV wall	
X-Bar Bot	154.69 (22.436)	0.52	-55.61 (-8.065)	0.19		
Y-Bar Top	84.28 (12.22)	0.23	-27.3 (-3.96)	0.07		
Y-Bar Bot	181.3 (26.30)	0.62	-54.57 (-7.915)	0.19		
RCCV Wall					-10.12 (-1.47)	0.39
Vert In	193.11 (28.008)	0.66	-20.79 (-3.015)	0.07	At connection with top slab	
Vert Out	53.36 (7.740)	0.14	-16.46 (-2.387)	0.04		
Hoop In	24.22 (3.513)	0.08	-10.26 (-1.488)	0.03		
Hoop Out	23.07 (3.346)	0.06	-7.01 (-1.02)	0.02		
SP Slab					-9.36 (-1.36)	0.36
Hoop Top	5.86 (0.850)	0.02	-5.85 (-0.850)	0.02	On bottom surface at RCCV wall	
Hoop Bot	13.35 (1.936)	0.04	-0.24 (-0.035)	0.00		
Rad Top	117.56 (17.050)	0.40	-24.99 (-3.624)	0.08		
Rad Bot	84.14 12.20	0.23	-30.67 (-4.448)	0.08		

Table 19B-6 Summary of Maximum Stresses in Rebar and Concrete at 0.620 MPaG (90 psig) Pressure (Sheet 2 of 2)

Location	Maximum Rebar Tension		Maximum Rebar Compression		Maximum Concrete Compression	
	Stress, MPa (ksi)	Ratio to Allowable(1)	Stress, MPa (ksi)	Ratio to Allowable(1)	Stress, MPa (ksi)	Ratio to Allowable(2)
Pedestal Wall					-14.25 (-2.07)	0.55
Vert In	8.15 (1.18)	0.03	-49.49 (-7.178)	0.17	Outside surface at connection with basemat	
Vert Out	0.02 (0.003)	0.00	-48.52 (-7.037)	0.13		
Hoop In	31.65 (4.590)	0.11	-11.66 (-1.691)	0.04		
Hoop Out	27.12 (3.933)	0.07	-10.03 (-1.455)	0.03		
Basemat					-6.12 (-0.89)	0.30
Top Layers	13.81 (2.003)	0.05	-18.56 (-2.692)	0.06	Top surface at pedestal wall, [27.6 MPa, (4 ksi) concrete]	
X-Bar Bot	149.37 (21.664)	0.40	-23.23 (-3.369)	0.06		
Y-Bar Bot	132.28 (19.185)	0.36	-23.98 (-3.478)	0.06		

Notes:

1. allowable is 90% of yield; for inner bars, yield = 327.5 MPa (47.50 ksi); for outer bars, yield = 413.8 MPa (60.02 ksi)
2. allowable is 75% of fc'; for inner surface, fc' = 25.91 MPa (3.75 ksi); for outer surface, fc' = 34.48 MPa (5.0 ksi)

Table 19B-7 Summary of Maximum Stresses in Rebar and Concrete at 0.992 MPaG (144 psig) Pressure (Sheet 1 of 2)

Location	Maximum Rebar Tension		Maximum Rebar Compression		Maximum Concrete Compression	
	Stress, MPa (ksi)	Ratio to Allowable(1)	Stress, MPa (ksi)	Ratio to Allowable(1)	Stress, MPa (ksi)	Ratio to Allowable(2)
Top Slab					-21.34 (-3.10)	0.83
X-Bar Top	175.97 (25.522)	0.47	-40.52 (-5.877)	0.11	0.042% peak plastic strain in horizontal bars at connection with top slab at pool girders	
X-Bar Bot	344.88 (50.020)	1.17	-159.25 (-23.10)	0.54		
Y-Bar Top	254.38 (36.895)	0.68	-40.09 (-5.815)	0.11		
Y-Bar Bot	339.85 (49.291)	1.15	-167.77 (-24.33)	0.57		
RCCV Wall					-27.53 (-3.99)	1.06
Vert In	354.41 (51.402)	1.20	-31.45 (-4.561)	0.11	0.40% peak plastic strain in vertical bars at top slab under pool girder locations	
Vert Out	231.67 (33.601)	0.62	-37.15 (-5.388)	0.10		
Hoop In	142.78 (20.708)	0.48	-32.52 (-4.717)	0.11		
Hoop Out	184.63 (26.778)	0.50	-7.27 (-1.05)	0.02		
SP Slab					-18.04 (-2.62)	0.70
Hoop Top	3.17 (0.46)	0.01	-19.78 (-2.869)	0.07		
Hoop Bot	81.25 (11.78)	0.22	-5.45 (-0.79)	0.01		
Rad Top	201.65 (29.247)	0.68	-49.23 (-7.140)	0.17		
Rad Bot	162.98 (23.638)	0.44	-55.6 (-8.06)	0.15		

Table 19B-7 Summary of Maximum Stresses in Rebar and Concrete at 0.992 MPaG (144 psig) Pressure (Sheet 2 of 2)

Location	Maximum Rebar Tension		Maximum Rebar Compression		Maximum Concrete Compression	
	Stress, MPa (ksi)	Ratio to Allowable(1)	Stress, MPa (ksi)	Ratio to Allowable(1)	Stress, MPa (ksi)	Ratio to Allowable(2)
Pedestal Wall					-26.59 (-3.86)	1.03
Vert In	78.17 (11.34)	0.27	-75.1 (-10.9)	0.25		
Vert Out	2.69 (0.39)	0.01	-84.32 (-12.23)	0.23		
Hoop In	110.41 (16.014)	0.37	-21.99 (-3.19)	0.07		
Hoop Out	88.52 (12.84)	0.24	-23.11 (-3.352)	0.06		
Basemat					-12.28 (-1.78)	0.59
Top Layers	181.55 (26.331)	0.62	-43.57 (-6.319)	0.15		
X-Bar Bot	320.38 (46.467)	0.86	-31.16 (-4.52)	0.08		
Y-Bar Bot	336.25 (48.769)	0.90	-42.24 (-6.126)	0.11		

Notes:

1. allowable is 90% of yield; for inner bars, yield = 327.5 MPa (47.50 ksi); for outer bars, yield = 413.8 MPa (60.02 ksi)
2. allowable is 75% of fc'; for inner surface, fc' = 25.91 MPa (3.75 ksi); for outer surface, fc' = 34.48 MPa (5 ksi)

Table 19B-8 Summary of Torispherical Shell Parameters for Benchmark Analysis

Parameter	Tested Shell	Analysis Model
D/t	770	770
r/D	0.17	0.174
R/D	0.90	0.903
D (m)	4.92	10.4
Yield Stress (MPa) (ksi)	344 (49.9)	344 (49.9)
Buckling Pressure (MPa) (ksi)	0.731 (0.106)	0.738 (0.107)

SI to English Unit Conversion (SI units are the controlling units and English units are for reference only):

25.4 mm = 1 in

Table 19B-9 Level C Pressure Capability of Drywell Head at 260°C (500°F)

Part		Calculated Pressure Capability, MPaG (psig)
Sleeve		2.036 (295.3)
Torispherical head		1.369 (198.5)
Bolted Flange	Hub/Flange	1.150 (166.8)
	Flange Bolt	1.150 (166.8)
Anchor Structure	Inside Flange Plate	1.033 (149.8)
	Inside Gusset Plate	1.194 (173.2)
	Concrete	1.224 (177.5)

Table 19B-10 Level C Pressure Capability of Hatches and Airlocks at 260°C (500°F)

Component	Part		Calculated Pressure Capability, MPaG (psig)
Equipment Hatch	Sleeve		2.817 (408.6)
	Head		3.544 (514.0)
	Bolted Flange	Flange	1.153 (167.2)
		Bracket	1.153 (167.2)
		Flange Bolt	1.153 (167.2)
	Anchor Structure	Inside Flange Plate	1.768 (256.4)
		Inside Gusset Plate	1.047 (151.9)
		Concrete	3.383 (490.7)
Personnel Airlock	Sleeve		2.817 (408.6)
	Sidewall		1.078 (156.3)
	Anchor Structure	Inside Flange Plate	1.768 (256.4)
		Inside Gusset Plate	1.570 (227.7)
		Concrete	3.383 (490.7)
Wetwell Hatch	Sleeve		3.375 (489.5)
	Head		4.251 (616.6)
	Bolted Flange	Flange	1.272 (184.5)
		Bracket	1.272 (184.5)
		Flange Bolt	1.272 (184.5)
	Anchor Structure	Inside Flange Plate	2.140 (310.4)
		Inside Gusset Plate	1.499 (217.4)
		Concrete	3.924 (569.1)

Table 19B-11 Summary of Level C/Factored Load Category Pressure Capacity at 260°C (500°F)

Component	Pressure, MPaG (psig)
RCCV and Liners	1.011 (146.6)
Drywell Head	1.033 (149.8)
Hatches and Airlocks	1.047 (151.9)
Penetrations	3.38 (490)
PCCS Heat Exchangers	38.7 (5613)

Figure 19B-1 Finite Element Model Showing Steady State Thermal Condition

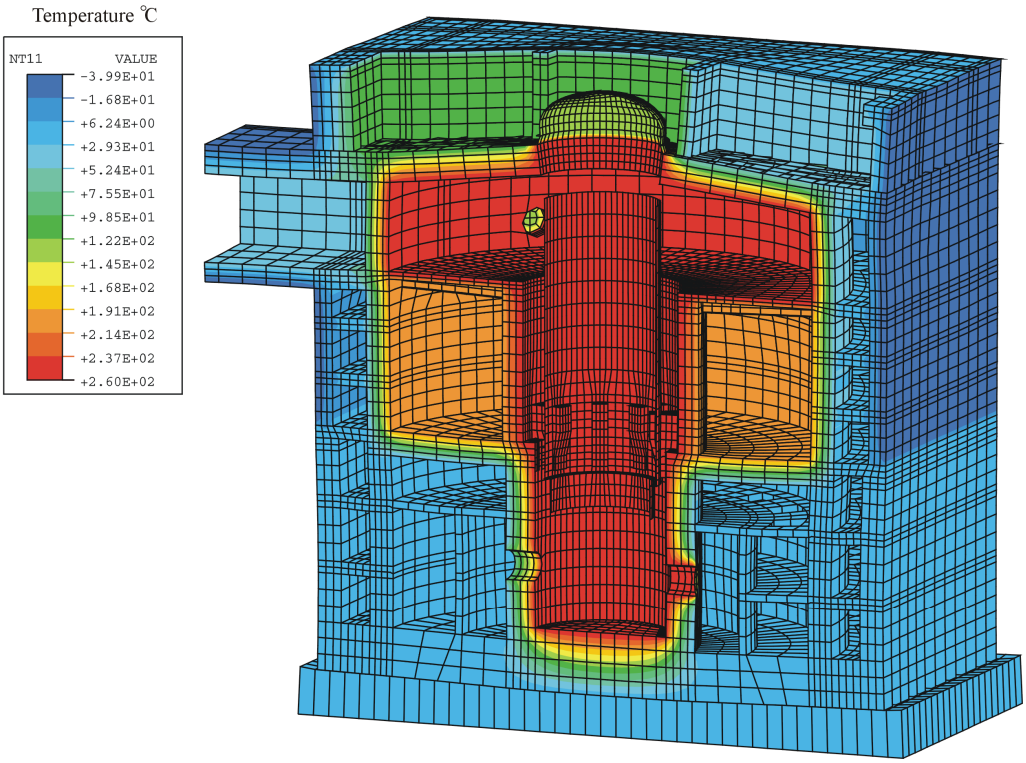


Figure 19B-2 Concrete Compressive Stress, Level C Analysis, 0.992 MPaG (144 psig) Pressure

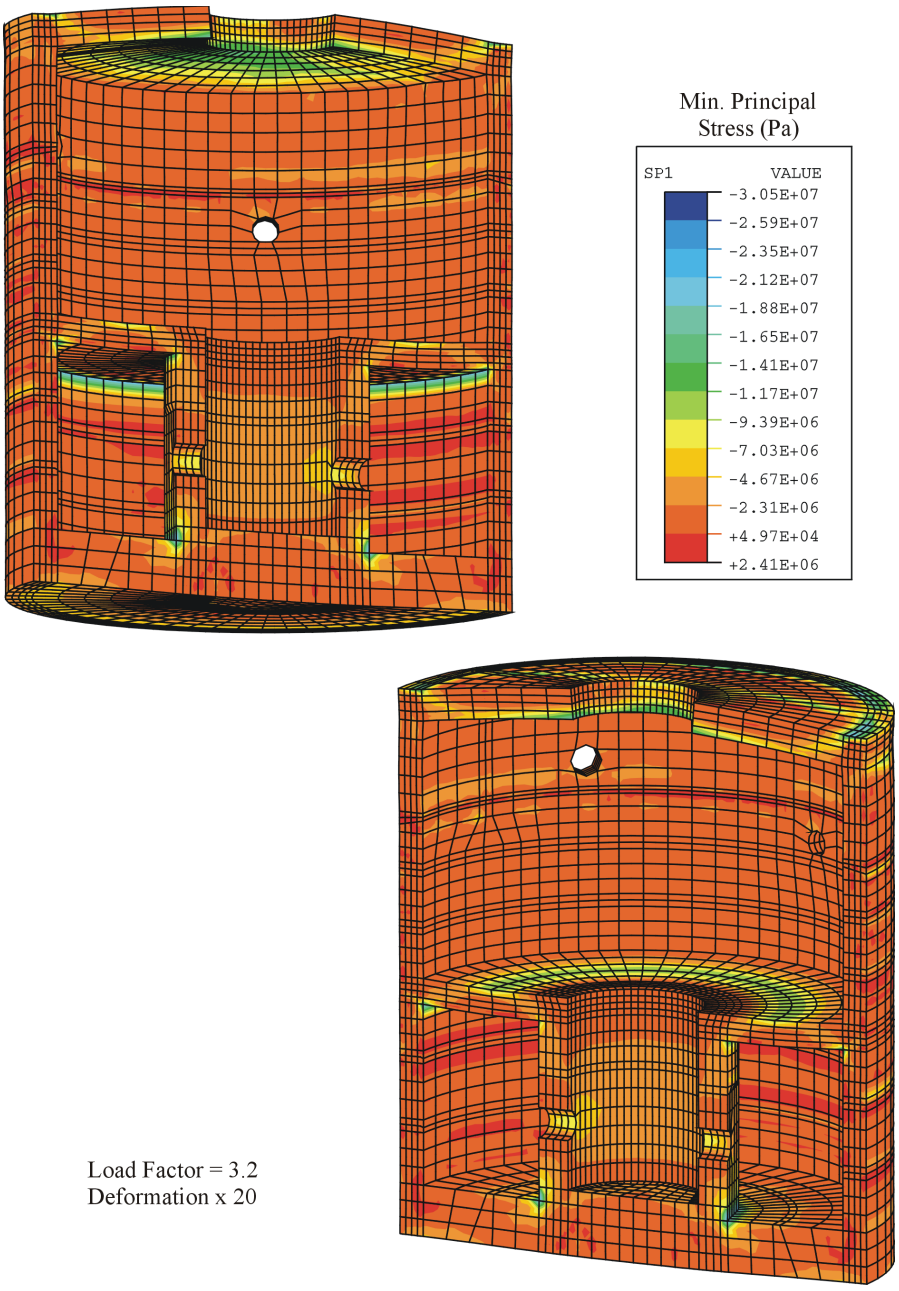


Figure 19B-3 Concrete Cracking Strain, Level C Analysis, 0.992 MPaG (144 psig) Pressure

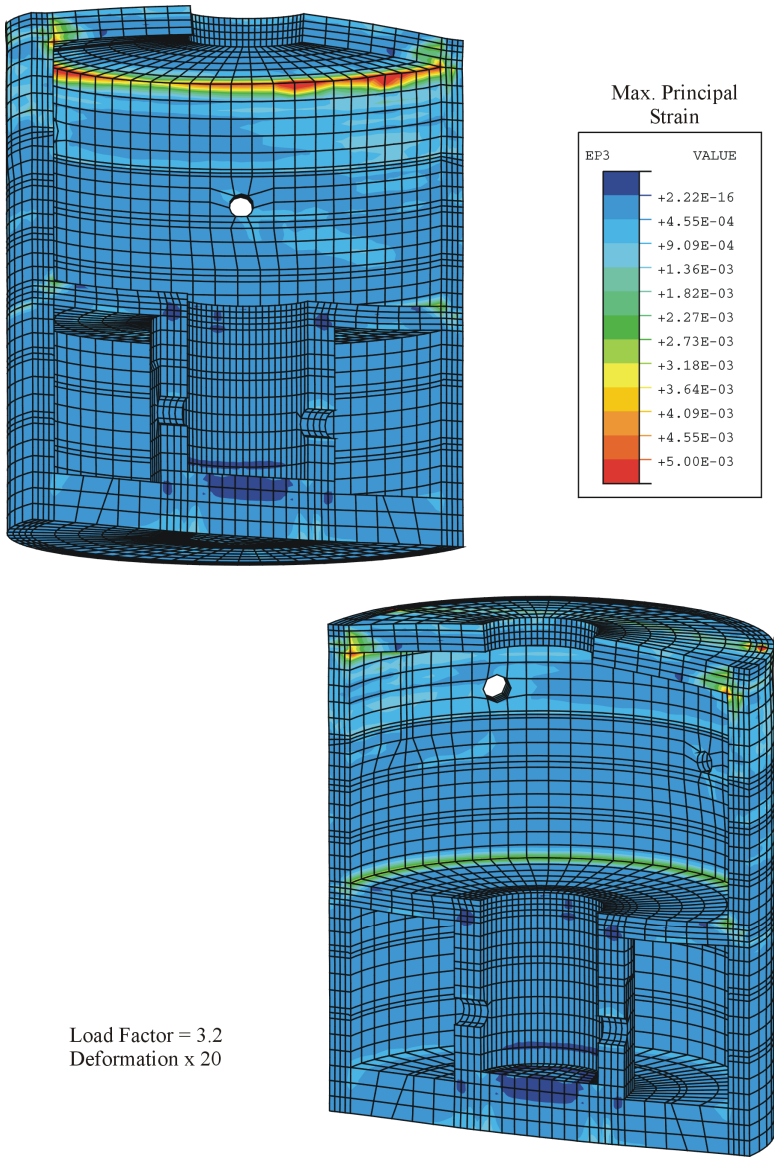


Figure 19B-4 Liner Maximum Principal Strain, Level C Analysis, 0.992 MPaG (144 psig) Pressure

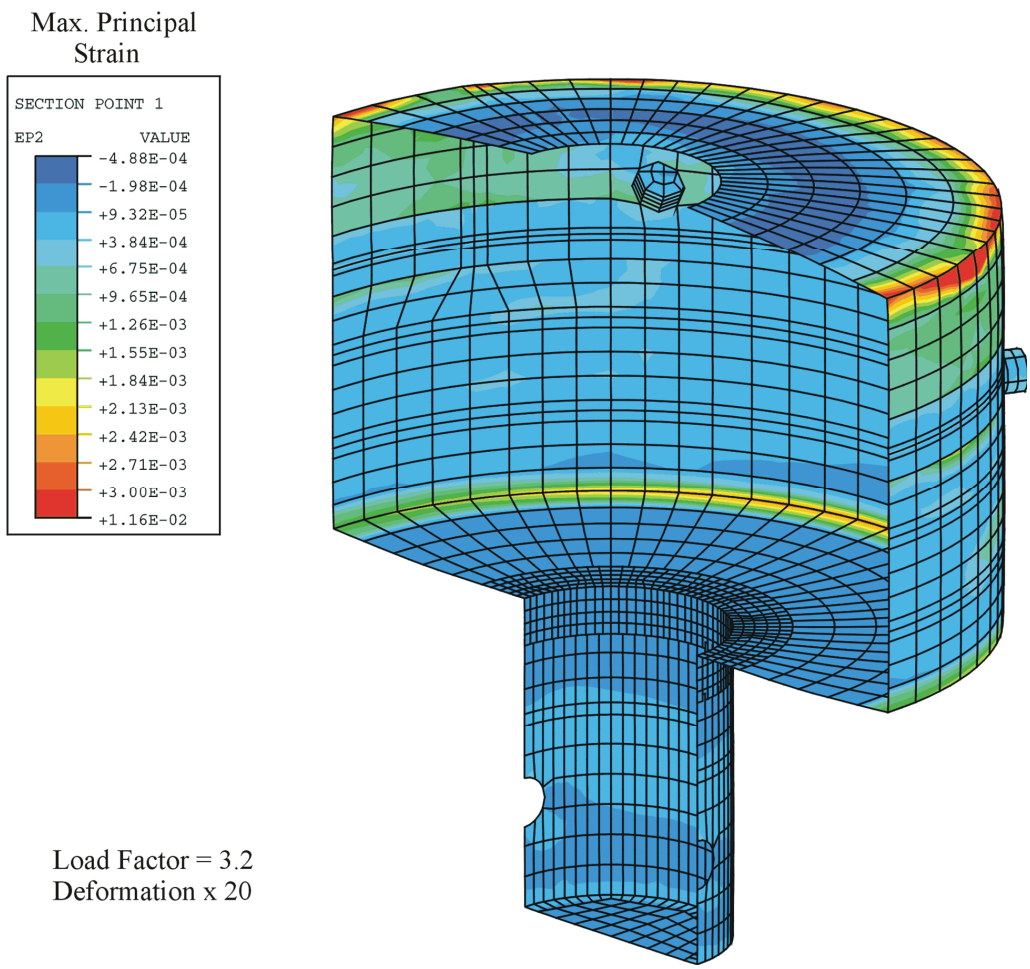


Figure 19B-5 Maximum Principal Strains in Liner Near Discontinuities, Level C Analysis

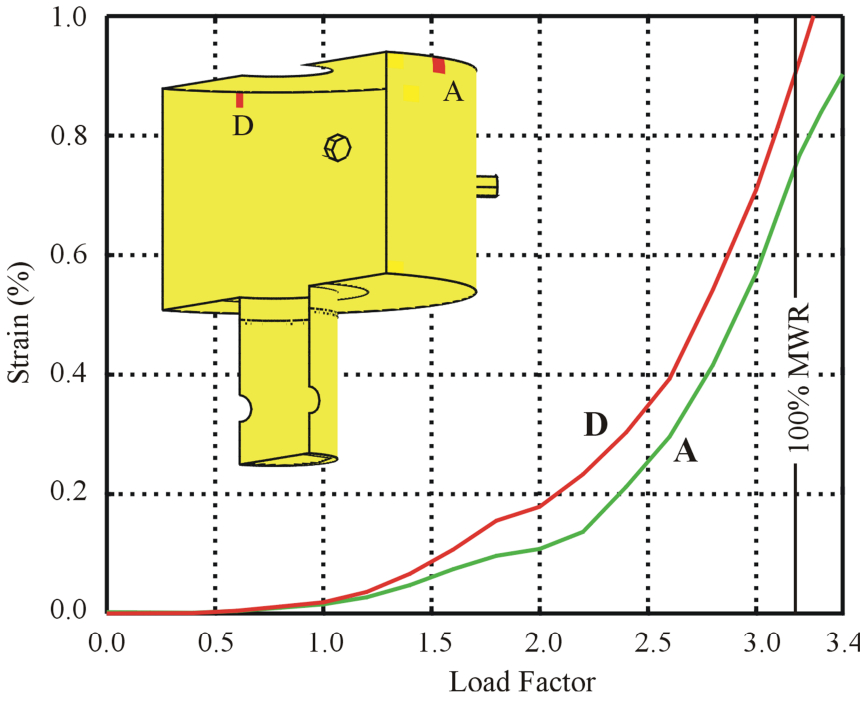


Figure 19B-6 Liner Membrane Strain at Representative Locations, Level C Analysis

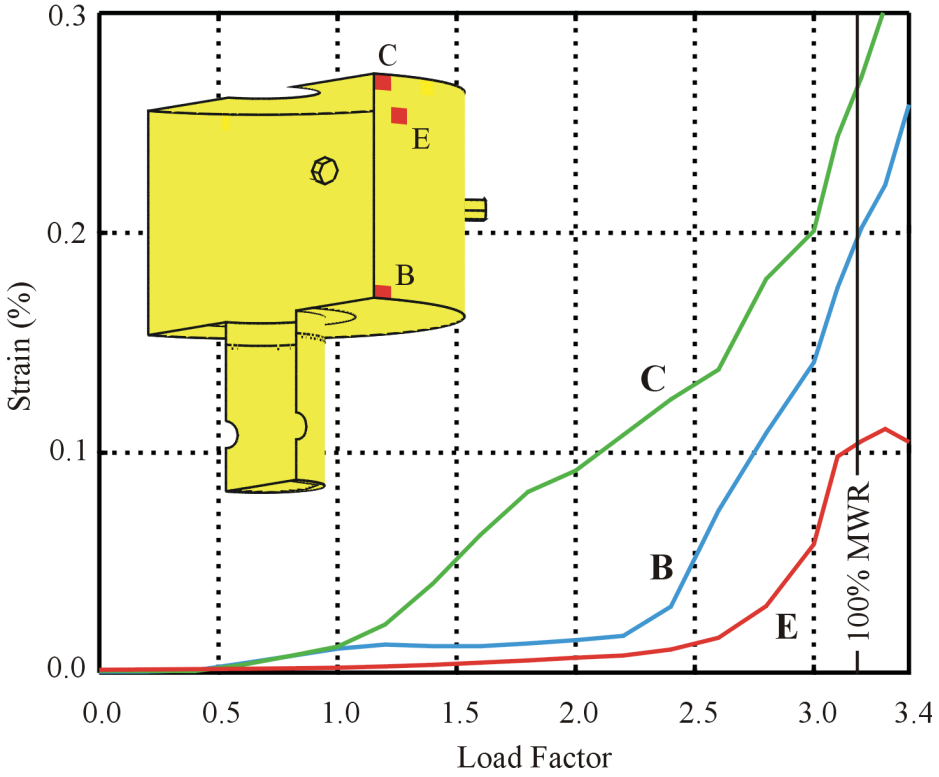


Figure 19B-7 Finite Element Model for Drywell Head Capacity Study

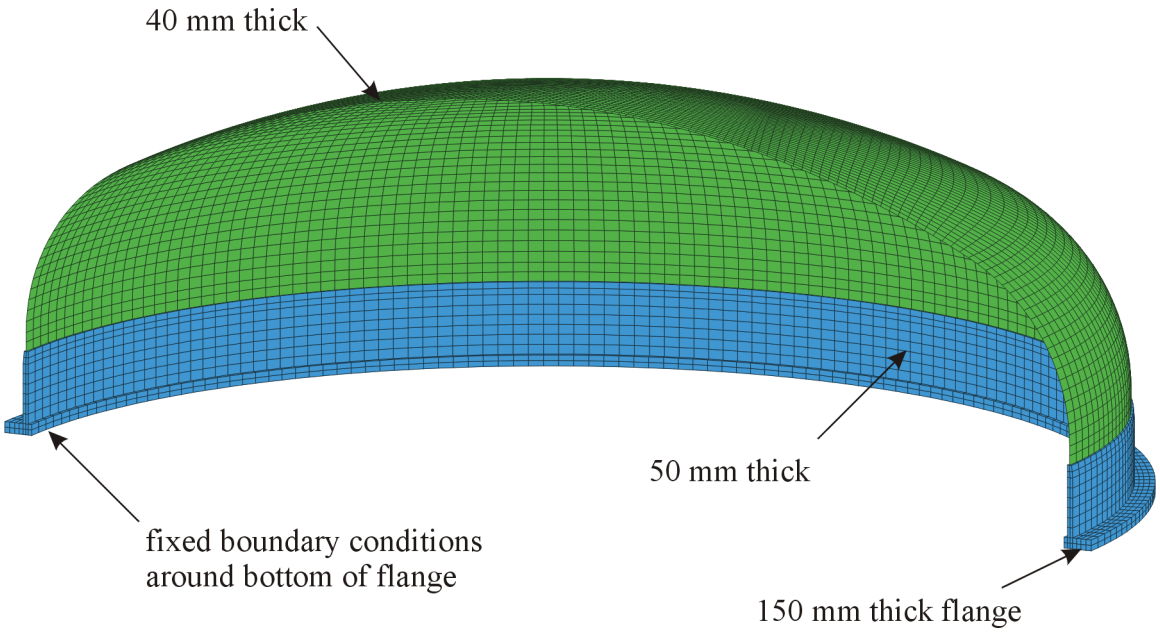


Figure 19B-8 Displacement at Crown in Buckling Test Analysis

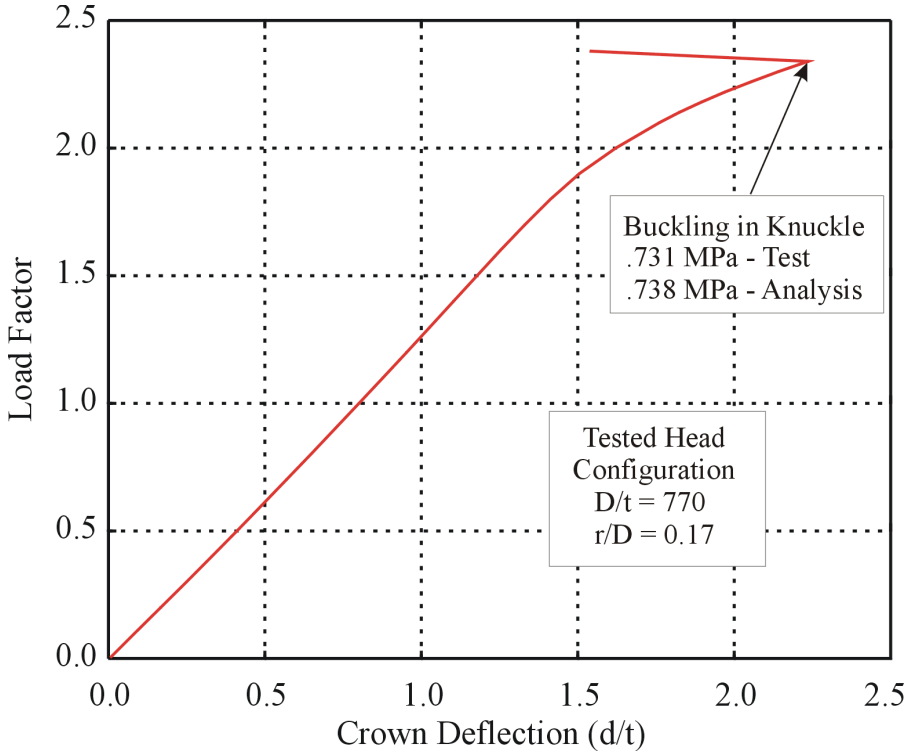


Figure 19B-9 Post Buckled Shape of Test Analysis Model

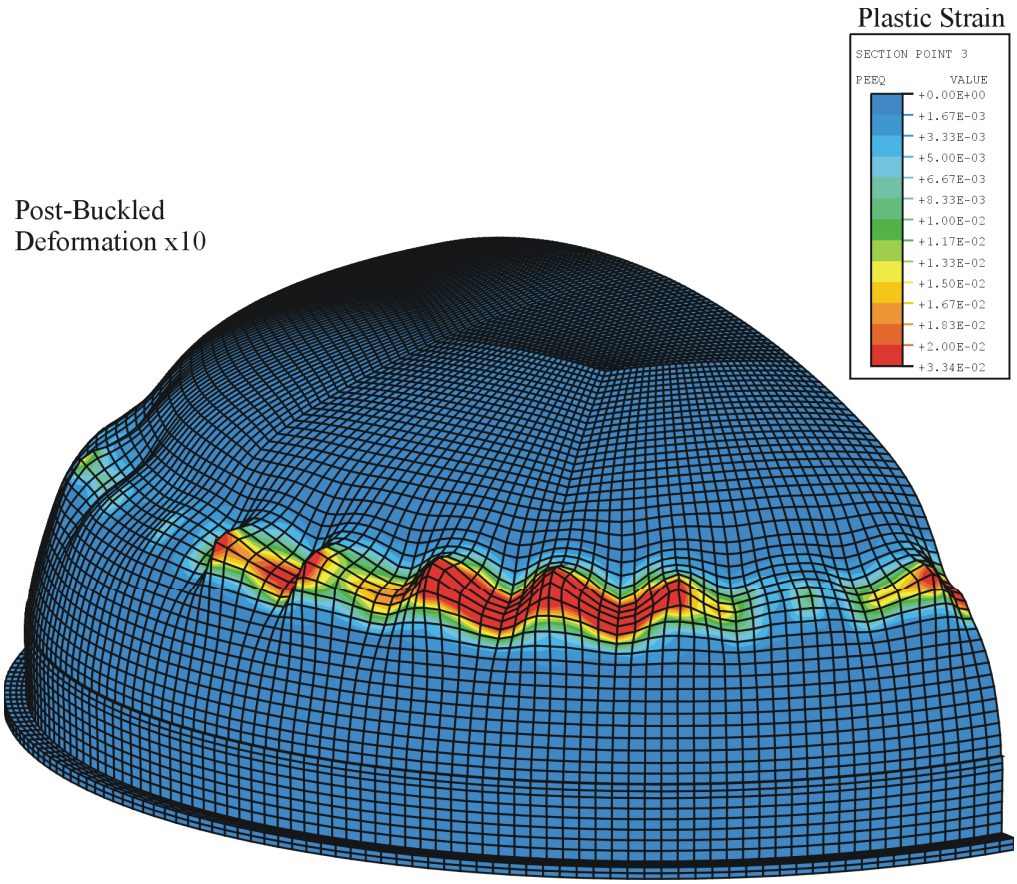


Figure 19B-10 Finite Element Model for Buckling Analysis of ESBWR Drywell Head

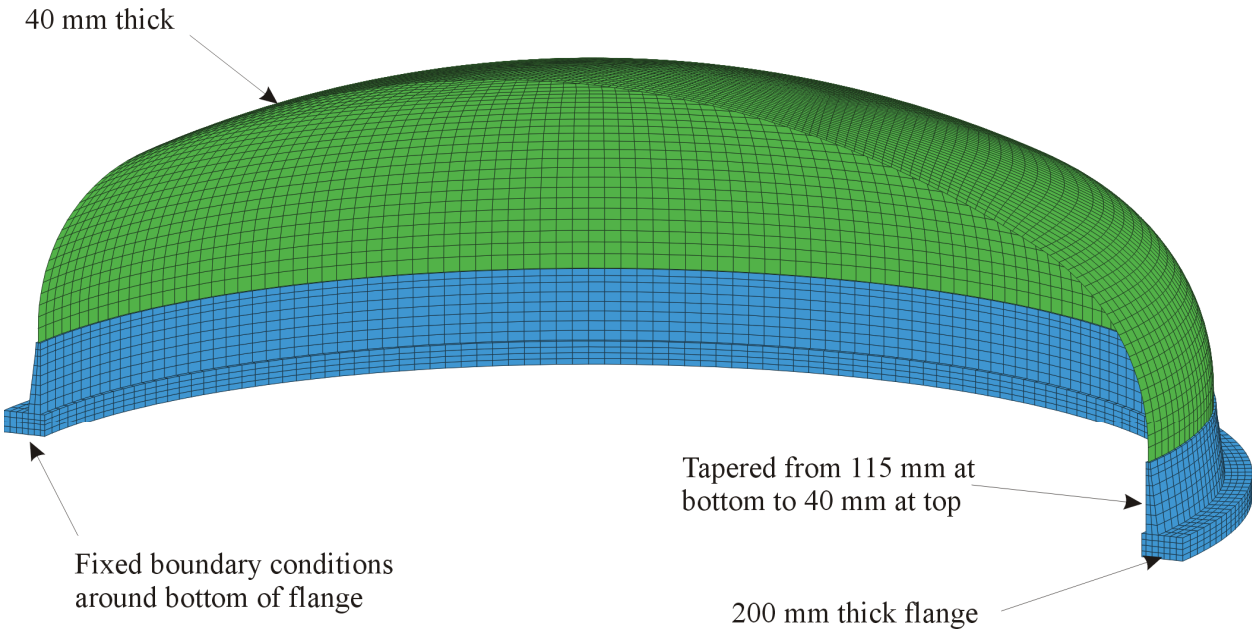


Figure 19B-11 Performance of ESBWR Drywell Head Under Internal Pressure at 260°C (500°F)

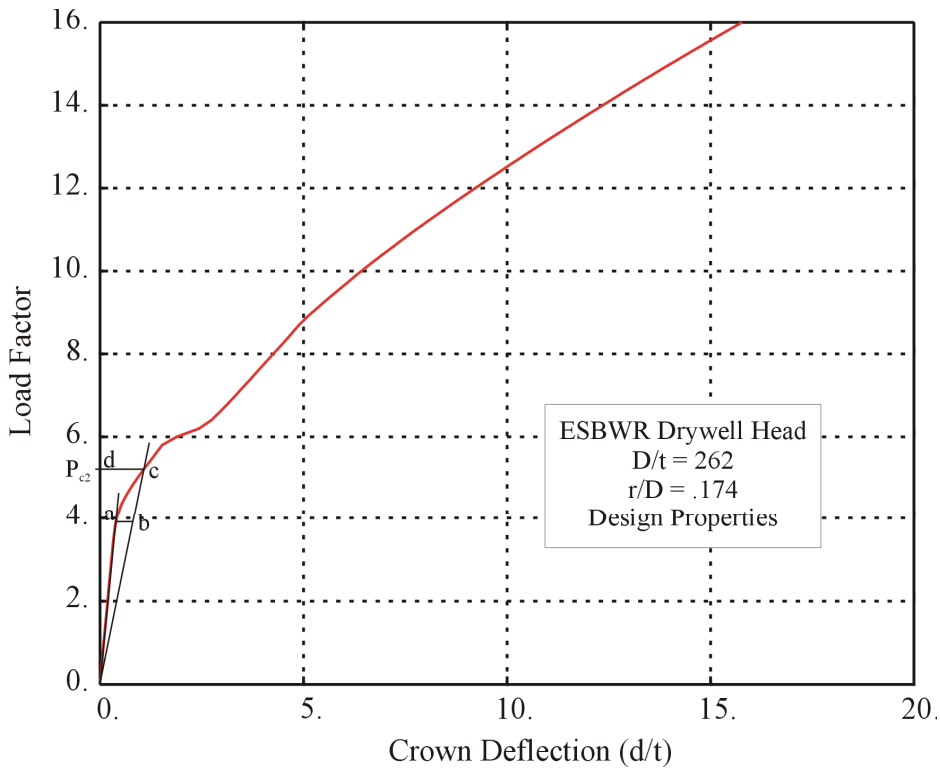


Figure 19B-12 Plastic Strains, Nominal Geometry, 260°C (500°F)

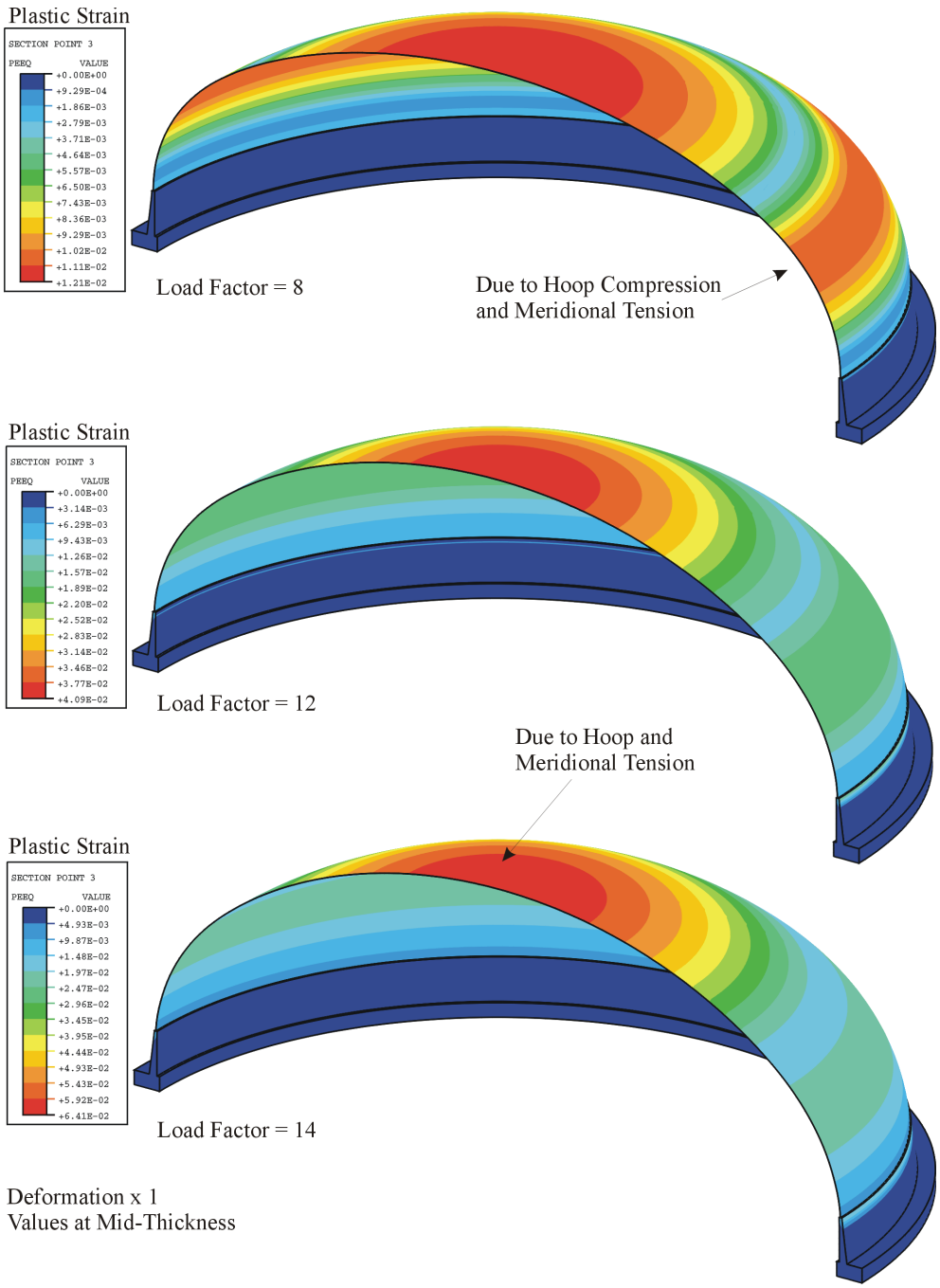
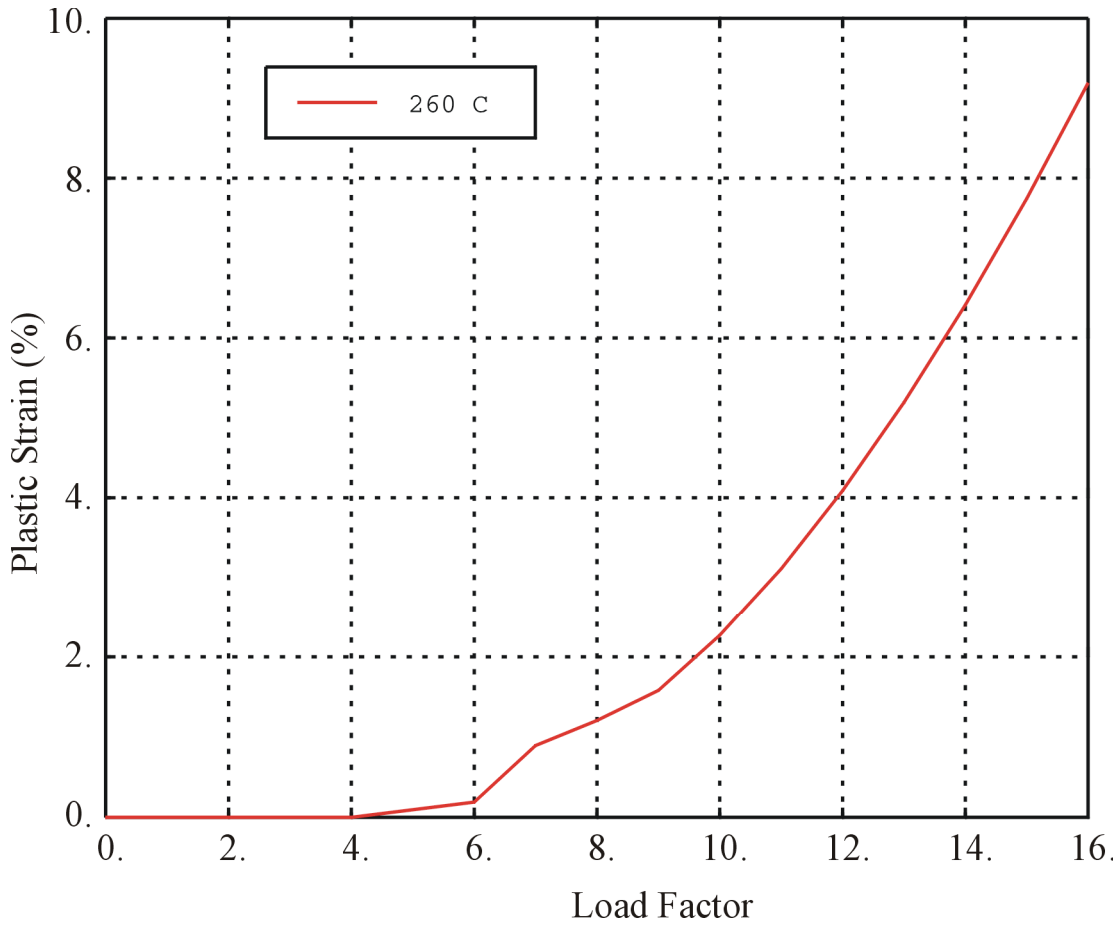


Figure 19B-13 Mid-Thickness Plastic Strain at Crown Under Increasing Pressure at 260 °C (500°F)



Appendix 19C Probabilistic Analysis for Containment Pressure Fragility

19C.1 Introduction

This appendix presents the probabilistic analyses and results for the fragility of the ESBWR primary containment system for over-pressurization. Fragility is defined as the cumulative probability of failure for increasing internal pressure. Here, failure of the containment is taken to mean a breach in the containment boundary, which can occur as a result of structural failure in the RCCV walls, liner tearing at discontinuities (such as anchorages, corner connections, or thickened plates at penetrations), rupture in the steel components of the penetrations or drywell head, or separation of the bolted flanges for the penetrations or drywell head. Analyses for the pressure capacity of these components requires different levels of modeling. A global, 3D finite element model is used to determine the pressure capacity of the RCCV structure assuming no leakage or failure in the steel penetration components. However, local detailed 3D models are used to determine the pressure limits associated with the steel components (drywell head and equipment hatch) using results from the global model as boundary conditions for the local models. The pressure units of MPaG used in this appendix are gauge pressures unless noted otherwise. Absolute pressure is designated as MPa.

For the current analyses, the thermal conditions corresponding to the 260°C (500°F) steady state accident conditions have been modified. For this accident condition, the temperature in the airspace under the drywell head is changed to be 260°C (500°F) corresponding to the atmosphere in the remainder of the drywell air space. Previously, the temperature on the inner surface of the drywell head was considered to be 43.3°C (110°F) with a transition to 260°C (500°F) across the barrel section of the drywell head in the top slab. In addition, the temperature of the water in the reactor well and in the equipment storage pool is changed from 43°C (110°F) to 100°C (212°F) due to heat flowing across the drywell head under these conditions. This new temperature condition affects the median pressure capacity determined for the RCCV global analysis because the global deformations and structural performance is dependent on the temperature in the upper water pools. The median pressure capacity for the drywell head determined from the local analysis is also affected because of the global deformations of the top slab and the higher temperatures on the drywell head, and also because of the updated bolt material and bolt preloads in Figure 3G.1-51.

However, the uncertainty in the calculations is not affected by this change in temperature conditions. The uncertainty is primarily associated with modeling methods, material properties, and failure criteria or structural limits used to establish the pressure capacity. The relative change in pressure capacity due to these uncertainties from the new median value will be very close to the relative change from the old median value that has previously been determined. Thus, it is not necessary to repeat the matrix of analyses with parameter variations to calculate the variance or standard deviation in the pressure capacity. New median pressure capacities are calculated for the

RCCV global model and for the drywell head local model, and the new fragility is based on the previously calculated lognormal standard deviations.

Likewise, the new temperature conditions determined for the 260°C (500°F) steady state accident conditions do not affect the pressure capacity that has been previously calculated for the ambient condition or for the 538°C (1000°F) transient accident condition. The ambient case does not consider any elevated temperatures, and the 538°C (1000°F) transient condition is based on a short term DCH temperature spike. Here, the temperatures under the drywell head and in the upper pools do not have time to react, and the previous assumptions for these temperatures are still valid. Thus, it is not necessary to repeat any of the analyses for pressure capacity at ambient conditions or at the 538°C (1000°F) transient conditions. The changes in conditions for the 260°C (500°F) steady state accident conditions also do not affect the temperature distributions already considered for the equipment hatch, and thus, new calculations to update the pressure capacities for the equipment hatch are not required.

19C.1.1 Analysis Methods

These analyses use the ANACAP-U concrete constitutive model (Reference 19C-1) coupled with the ABAQUS/Standard finite element computer program (Reference 19C-2). These analyses are based on detailed 3D finite element modeling, advanced material constitutive relations, and an assessment of uncertainties within a probabilistic framework. The uncertainties in the analysis results are associated with the finite element modeling, the material properties of the in-situ structure at the time of the accident, failure criteria or limit states used in establishing the pressure capacity, and the loading conditions that lead to pressurization of the containment. The uncertainties in the finite element modeling, such as mesh fidelity and constitutive relations, are discussed in Section 19C.1.5. The uncertainties in material properties and failure criteria are evaluated by first identifying those parameters that are likely to have a significant effect on the analysis results and then evaluating the effect of variations in these parameters using the 95% confidence value of the specific parameter while keeping all other parameters at the median values. The 95% confidence value is defined as V_m-1.645·β_v, where V_m is the median value of the property and β_v is the standard deviation for the distribution of the variation in that property. This represents a value such that there is 95% confidence that the actual value of that property will be larger than this value. In some cases, such as material property variations, additional analytical calculations are needed to evaluate the uncertainty. In other cases, such as variation in failure criteria, re-evaluation of an existing analysis result can be performed.

The failure pressure is characterized using a lognormal probability density function defined as

$$p_f(p) = \frac{1}{p\beta\sqrt{2\pi}} \exp\left[-\frac{1}{2}\left(\frac{\ln(p)-\mu}{\beta}\right)^2\right] \quad \text{(19C-1)}$$

where p is the failure pressure, μ is the mean value of the natural log of the failure pressure, and β is the standard deviation of the natural log of the failure pressure. Thus, the lognormal standard deviations for the various key parameters having uncertainty are determined using the equation

$$\beta_s^i = \frac{Ln(P_s^i/P_m)}{-1.645} \quad \text{(19C-2)}$$

where P_s^i is the pressure capacity when evaluated using the 95% confidence value for the ith parameter or material property, and P_m is the median pressure capacity determined by using the median values of all the key parameters. The composite lognormal standard deviation is then defined as the square root of the sum of the squares of the individual standard deviations, including the standard deviation for modeling uncertainty. The fragility, defined as the cumulative probability of failure for increasing internal pressure, is then calculated from the integral of the probability density function.

19C.1.2 **Thermal Conditions**

Accident conditions leading to over-pressurization will also include elevated temperatures. Because of thermal induced stresses and material property degradation at elevated temperatures, the fragility for over-pressurization is also a function of temperature. Thus, the fragility analyses are conducted for three different thermal conditions, 1) steady state normal operating temperatures (referred to as ambient conditions), 2) steady state conditions with the drywell liner at 260°C (500°F) representing long-term accident conditions, and 3) transient thermal conditions for a temperature spike representative of direct containment heating (DCH) conditions using a snapshot of the temperature distributions when the liner is at 538°C (1000°F). The temperature distributions for the above conditions are established through steady state or transient thermal analysis. The stress analysis model is first initialized to be stress free at a uniform ambient temperature of 15.5°C (60°F), and the hydrostatic pressures for the various water pools and superstructure loads are applied on the model. Next, the design pressure of 0.31 MPaG (45 psig) along with the accident temperature distributions under investigation are incrementally applied to the model using static equilibrium iterations for nonlinear effects. Finally, the internal pressure is incrementally increased,

again using static equilibrium iterations, to determine the pressure at which failure or leakage occurs according to the failure criteria of limit states defined. Note that the 538°C (1000°F) transient thermal condition starts from the steady state normal operating condition.

19C.1.3 Material Properties

The analyses for establishing the pressure fragility of the primary containment system are best estimate calculations and are based on median or expected material properties and failure criteria. The thermal properties for the thermal analyses are assumed to be constant with temperature, and variations in these properties are not considered in the uncertainty evaluation. This is handled by considering the three different thermal conditions in evaluating the overall pressure fragility. The thermal properties are summarized in Table 19C-1. For structural properties, analyses using the 95% confidence value of these important parameters are used to assess the effect of uncertainty in the analyses. The median and 95% confidence values must be developed for the elastic and plastic material properties and failure criteria, all as a function of temperature. While a set of three discrete thermal conditions are identified for the range of temperatures of interest, the temperatures within the structural components have a continually varying distribution. Thus, the property and criteria values must cover the entire range of temperatures from ambient to 538°C (1000°F). These data have been collected and synthesized from a variety of sources, (References 19C-3 through 19C-12). Typically, data for the median value and for estimating the distribution of a property at room temperature is available, and some data for the variation of the median value with temperature have been found. The 95% confidence values at elevated temperatures are then determined using the distribution at room temperature but with increasing uncertainty for increasing temperature. Table 19C-2 provides a summary of the elastic properties for steel, and Table 19C-3 provides a summary of the plastic properties of steel. Table 19C-4 provides a summary of the concrete properties.

19C.1.4 Failure Criteria

In evaluating the pressure capacity for the containment system, failure criteria must be defined to establish limit states on the structural response where the internal pressure is no longer contained by the structure. There is uncertainty in defining these failure criteria, so median and 95% confidence values are defined to evaluate the effect of the uncertainty on the analysis results. For the reinforced concrete containment vessel (RCCV) components, failure either occurs when tensile loads cause rebars to yield and then rupture, or when the shear forces across a section exceed the shear capacity. The rupture strain for Grade 60 reinforcing bars is based on the elongation limits from test data, factored to account for strain concentration factors that are not captured by the finite element modeling, which is based on smeared cracking. From previous experience with similar modeling (References 19C-13 and 19C-14), the calculated strain at which rebar rupture can occur is generally taken to be about one half of the uniaxial elongation data. As the limit state for section shear failure, a criterion for concrete shear strain across a section is defined. This failure criterion

has been established for the modeling methodology employed based on previous work and benchmarking with experimental tests on structural specimens (References 19C-14, 19C-15, and 19C-16). Once a shear band forms and the concrete shear strains reach a critical level across the complete section, a brittle type shear failure of the section can occur.

Failure criteria are also defined to consider leakage due to tearing of the liner. Tests of over-pressurization of RCCV scale models show that liner tearing will develop at discontinuities where strain concentration factors exist. From previous work, for example Reference 19C-17, these failure criteria for a tearing strain are based on the ductility of the material and the magnitude of strain concentration factors not captured by the fidelity of the modeling. First, the ductility of the liner material is defined using elongation data performed on uniaxial test specimens. The ductility depends on the state of stress, which is generally biaxial loading. For the liner, the loading due to internal pressure is biaxial with the hoop tension which is generally twice that of the tension in the axial direction. This biaxial loading produces a ductility limit of 60% of the uniaxial elongation data. In addition, to account for reduced ductility in the heat affected zones of welds in the liner, a further reduction of 15% on the uniaxial test data are used. This ductility limit must then be further reduced for comparison to calculated liner strains to account for the strain concentration factors not captured in the analyses. This factor depends on the fidelity of the modeling, and thus different tearing strain limits are defined for the global model and for the local model. In the global model, the liner strains are taken at the local areas showing distress, that is, local strains rather than far field strains, and a median strain concentration factor of 6 is used on the ductility limit to establish liner tearing. In the local modeling with more mesh refinement, a median factor of 4 can be used for this strain concentration factor in establishing the failure criteria for liner tearing. For the thicker steel components of the penetration, the loading can be triaxial, and the elongation data are factored by 50% to determine the material ductility. A strain concentration factor of 4 is again used to account for the mesh fidelity of these steel components in the local modeling.

Finally, criteria for leakage through a bolted flange connection are defined based on a flange separation distance. This criterion is based on experimental test data reported in Reference 19C-18 for pressure-unseating equipment hatches. The pressure differential between first unseating and measured leakage along with the bolt stiffness and cover area is used to calculate a flange separation distance that leads to leakage past the gasket seal. Several tests were performed in the referenced study with variations in parameters, such as bolt prestress, number of bolts, and temperature. The median and 95% confidence values for flange separation leading to leakage are developed based on these variations in test results. These failure criteria were also considered constant with temperature because the test data did not show any significant sensitivity with temperature. Note that the initiation of section yielding in the bolts is also monitored as a criterion for leakage at the bolted connection. In the drywell head, the flange separation distance criterion does not apply to the bolted flange configuration. In the drywell head configuration, the flanges do not uniformly separate as in the equipment hatch configuration. The drywell head flanges separate

in a bending or prying fashion, separating first along the inside edge and developing bearing pressure along the outside or toe of the flange. Thus, only the initiation of bolt yield is used as the criterion for leakage at the drywell head. A summary of these failure criteria used in this pressure fragility evaluation is provided in Table 19C-5.

19C.1.5 Modeling Uncertainty

There is also uncertainty associated with the modeling used in the analyses for determining the failure pressures for any given set of material properties, geometry, or other problem parameters. This uncertainty concerns the mesh fidelity, the type of element formulations used, the robustness of the constitutive models, the equilibrium iteration algorithms and convergence tolerances, geometric imperfections, fabrication and construction exactness, rebar placement locations, and the like. This modeling uncertainty must be quantified as part of the fragility calculation. Historically, this uncertainty is based on the experience and judgment of the analyst because the analytical effort needed to consider variations in these modeling parameters is prohibitive. For this effort, the modeling uncertainty is based on previous work where similar modeling has been used to predict structural performance that can be compared to test data. Several pretest analytical predictions have been performed for structural specimen tests using the same software and modeling philosophy, namely mesh fidelity, element formulations, convergence algorithms, and so forth. Many of these predictions and tests concern the pressure capacity of reinforced concrete containments, for example, the 1:6 scale RCCV model tested to over-pressurization failure at Sandia National Laboratories, Reference 19C-20. Thus, the modeling uncertainty can be determined by comparing the predicted analysis results with the test results. A list is constructed of about 20 such comparisons, and the ratio of the test result to the predicted result is determined for each. These data points are sorted into ascending order and plotted for cumulative probability versus the ratio of test result to analysis prediction. The cumulative probability is calculated for each point as n/(N+1) where n is the nth point in the series and N is the total number of data points. A cumulative probability function, based on a lognormal probability distribution function, can then be fitted to these data through a least squares fit for the two parameters defining the lognormal Probability Density Function (PDF). The resulting curve fit is illustrated in Figure 19C-1.

Because the test data and analyses are all at ambient temperatures, the calculated β for modeling uncertainty is increased by 10% for the analyses associated with the 260°C (500°F) thermal conditions and by 20% for the analyses of the 538°C (1000°F) thermal conditions. Also, because the local modeling for the drywell head and equipment hatch take boundary conditions from the global model and perform additional analyses, the respective modeling uncertainties are increased by an additional variance of β = 0.06 which is typical for analyses of steel components. The values of lognormal standard deviations for modeling uncertainties are summarized in Table 19C-6.

19C.2 RCCV and Liners

19C.2.1 Model Description

A global 3D model is used to assess the ultimate capacity of the reinforced concrete components of the primary containment system due to over-pressurization under severe accident conditions. The modeling consists of a half-symmetric representation of the RCCV and the surrounding reactor building, including the basemat, the pedestal wall, the suppression pool floor slab, the upper drywell walls, the top slab, the upper pools structure and refueling floor, and the floors and walls of the reactor building, as illustrated in Figure 19C-2. This figure also illustrates the temperature distribution for the 260°C (500°F) steady state condition. It is noted that the temperature of the water in the reactor well and the equipment storage pool is now 100°C (212°F). The inner surface of the drywell head is 260°C (500°F) and the outer surface is 100°C (212°F). The global temperature plot is based on points near the outer surface for the plate elements representing the drywell head. The model is supported on an elastic layer of continuum elements representing the soil foundation. Solid (20-node continuum) elements with reduced Gaussian quadrature integration are used to model the reinforced concrete sections. The reinforcement bars are modeled as embedded, truss-like steel elements at the appropriate locations within the concrete elements. Membrane elements (plate elements without bending stiffness) are generally used to model the steel liners. These elements are attached to the nodes of the concrete elements for compatibility with the concrete deformations. This assumes that the liner anchorage system keeps the liners in contact with the concrete for this global modeling of the RCCV performance. Some plate bending elements are used for the thickened sections at connections. Representations for the large equipment hatches, personnel airlock penetrations, and the drywell head components are included using plate bending elements. Plate bending elements are also used to model the steel components of the internal structures, including the vent wall, diaphragm floor, reactor vessel shield wall, and the reactor pressure vessel support brackets, so that the stiffness and thermal induced stresses on the RCCV from these components are included in the modeling.

19C.2.2 Median Capacity Analysis

Figure 19C-3 plots the maximum principal strains, representative of cracking strains, in the RCCV at a drywell pressure of four times design pressure. This figure also shows the deformed shapes magnified by ten and illustrates the structural response of the RCCV containment system. The contour limits in these plots are set to indicate distressed areas where cracking is concentrated. The critical locations for the RCCV pressure capacity is at the connection of the RCCV upper drywell wall to the flat top slab, which is supported by the upper pool girders extending across the top slab. Cracking and distress is also evident in these upper pool main girders. Examination of the structural response relative to the failure criteria indicates that the pool girders will fail due to section shear capacity at a containment pressure of 1.741 MPaG (252 psig) or a load factor of 5.61 times the design pressure. The critical location for liner tearing is at the connection of the RCCV wall to

the top slab and, in particular, directly under the location of the upper pool girder on the top of the slab at the steam tunnel connection, as illustrated in Figure 19C-4. The calculated strain at this location is plotted versus internal pressure and evaluated against the failure criteria. Liner tearing is predicted to initiate at this top slab connection at a median pressure of 1.643 MPaG (238 psig) or a load factor of 5.30 times the design pressure.

19C.2.3 Evaluation for Uncertainty

For the RCCV wall capacity, the important material property parameters are the concrete strength, which also affects the concrete modulus and tensile strength, and the yield strength of the reinforcement. The ultimate strength of the reinforcement also has uncertainty, but this is handled through the failure strain for the reinforcement. There is also uncertainty in the yield stress and ultimate strength of the liner material. However, for the global modeling, the evaluation for liner tearing is also handled through the failure strain limit for the liner. The liner yield stress is not considered an important parameter because the liner is “glued” to the concrete and thus deforms along with the concrete in a strain-controlled manner. Variations on the analysis for the 260°C (500°F) thermal condition are performed to establish the failure pressures under the 95% confidence values for these key parameters. Table 19C-7 summarizes the results of these studies for evaluation of the uncertainty. The table provides the failure pressures found and the calculated lognormal standard deviations for variation of the key parameters identified. The composite lognormal standard deviation including the modeling uncertainty is also shown in the table. As discussed previously, it is noted that the variance or uncertainty for the pressure capacity is not affected due to the new temperature conditions associated with the 260°C (500°F) steady state accident condition. The lognormal standard deviations for each area of uncertainty that have been previously computed, relative to the previous median pressure capacities, are used to assess the fragility with the current median pressure capacities.

19C.2.4 Variation with Temperature

To determine the variation of failure pressure with temperature for RCCV components, the global analyses using the median values of all parameters are performed for the other thermal conditions, namely normal operating (ambient) and the 538°C (1000°F) liner temperature under transient conditions. It is found that the RCCV response and mode of failure is the same as found in the 260°C (500°F) steady state thermal condition. The pressure capacity for the RCCV walls is again limited by shear failure of the upper pool girders spanning across the top slab. The calculated median pressure capacities for failure of the RCCV wall and liner tearing in the RCCV wall at the connection with the top slab for these thermal conditions are summarized in Table 19C-8.

19C.2.5 Summary

Table 19C-8 provides a summary of the pressure fragility for the capacity of the RCCV wall and for liner tearing at the connection of the RCCV wall to the top slab. This table provides the mean and standard deviations for the lognormal PDF function, along with the median value of pressure capacity and the 95% confidence value for the pressure capacity all for the variations in thermal conditions for an accident. The 95% confidence value is the pressure value such that there is a 95% confidence that the actual failure pressure will be higher. Figure 19C-5 illustrates the pressure fragility for the RCCV wall with temperature, and Figure 19C-6 plots the fragility with temperature for the RCCV liner tearing failure mode.

The pressure capacity of the RCCV structure is limited by tearing of the drywell liner on the RCCV wall at the connection to the top slab. The capacity of the actual RCCV wall is limited by shear failure of the main upper pool girders supporting the top slab. This failure in the supporting upper pool girder will lead to a subsequent rapid failure of the RCCV wall at the top slab connection. While the RCCV wall capacity has a higher median pressure capacity than liner tearing, it also has more uncertainty. This failure mode for the pressure capacity of the RCCV boundary does not change with temperature. The RCCV wall capacity shows a decrease of about 20% from ambient conditions to elevated temperature conditions. This is due to the elevated water temperatures that develop in the upper pools under the steady state accident condition. Likewise, the difference between the capacity at 260°C (500°F) steady state conditions and the 538°C (1000°F) transient conditions is mainly because the upper pool girder controls this failure mode, and the performance of these upper pool girders is dependent on the temperature of the water in the pools. The resistance to liner tearing at the RCCV wall to top slab connections increases somewhat with temperature because of the effects of compressive stresses induced into the liner at elevated temperatures, which counteracts the tensile stress leading to tearing due to pressure. The liner material also has higher ductility at the upper range of the temperatures.

19C.3 Drywell Head

19C.3.1 Model Description

A detailed local model for the drywell head was constructed to evaluate the pressure fragilities for leakage from tearing in the steel components or from flange distortion and loss of seal. The drywell head model includes a section of the reinforced concrete top slab around the drywell head. Displacement boundary conditions, extracted from the global model, are imposed on the cut sections of the top slab in the local model. The boundary displacements enforce the deformation patterns from the global response of the containment system on the local model while capturing more refinement in the structural response of the drywell head components. A contact surface between the flanges is used to allow flange separation to develop. The closure bolts are modeled with beam elements of the appropriate length, cross-sectional area, and initial prestress. Figure 19C-7 illustrates the local modeling for the drywell head. This model for the drywell head was tested to ensure that it can capture the buckling failure mode due to hoop compression in the knuckle region. The testing and analysis showing that the drywell head does not fail in this mode are discussed in Appendix 19B.

19C.3.2 Median Capacity Analysis

As in the global modeling, the evaluations for the median pressure capacity and the uncertainties in the analysis are performed for the 260°C (500°F) steady state thermal conditions. Figure 19C-8 illustrates the temperature distributions in the drywell head region along with the deformation patterns plotted at a load factor of 7 P_d with a magnification of 10. The top slab bulges upward due to the pressure in the drywell below. This forces the collar for the bottom flange to undergo bending deformations. Figure 19C-9 plots the accumulated plastic strain at a pressure of 2.17 MPaG (315 psig) or a load factor of 7 P_d for the steel components of the drywell head. The areas showing plastic deformation at this load are in the liners at the connections with the thickened shear plate and in the collar section at the connection with the top slab where the thickness taper ends. Evaluation of these locations against the steel tearing strain shows that tearing does not develop before bolt yielding and leakage past the flange seals.

Figure 19C-10 illustrates the bending or prying deformation response in the bolted flanges and provides the bolt stresses versus pressure for the more critical bolt locations. For increasing internal pressure, the inside surface of the flanges begin to separate with increasing bearing stress around the toe of the flanges. Because this prying action produces substantial bearing stress and contact around the toe of the flanges, the pressure capacity is based on initiation of midsection yielding in the bolts. While the bolts can incur some additional plastic deformation before rupture, the median failure pressure is conservatively taken as that pressure causing first midsection yielding in the bolts. For the 260°C (500°F) steady state thermal condition, the median failure pressure for leakage at the bolted flange of the drywell head is 1.426 MPaG (207 psig) or 4.60 P_d.

19C.3.3 Evaluation for Uncertainty

A variation in the analyses using 95% confidence values for the yield stress of the steel material was performed to evaluate the variance due to uncertainty in this material property. Reevaluation of the median-based analysis using the 95% confidence values of the strain limit for steel tearing and for bolt yield stress were performed to assess variance due to uncertainty in these parameters. Separate analyses were also performed using a 95% confidence value for the bolt prestress and another for the temperature distribution in the top head to assess the variance from uncertainty in these problem parameters. Table 19C-9 summarizes the results of these studies for evaluation of the uncertainty. The table provides the failure pressures found and the calculated lognormal standard deviations for variation of the parameters identified. The composite lognormal standard deviation including the modeling uncertainty is also shown in the table. For the drywell head penetration, the pressure capacity is controlled by leakage at the bolted flange from bolt yielding. In this case, the bolt prestress has little affect on the pressure capacity because of the stiffness of the flange and the prying action in the connection. Variation in the bolt yield has a direct affect on the pressure capacity. A reduced yield stress for the steel components has the effect of increasing the capacity from bolt yield because earlier yielding in the collar reduces the prying action on the bolts. However, bolt yielding still develops before tearing in the steel components so that the mode of failure does not change.

It is again noted that the variance or uncertainty for the pressure capacity of the drywell head remains the same as previously calculated from the matrix of parameter variations already considered.

19C.3.4 Variation with Temperature

The variation with temperature for the failure pressure causing leakage in the drywell head was evaluated using median-based analyses for the ambient (normal operating) and 538°C (1000°F) transient thermal conditions. Thermal analyses, consistent with the global model analyses, are performed for the local drywell head model to establish the temperature distributions within the refined modeling. The loads due to increasing drywell pressure are then applied along with the boundary conditions from the global model at the corresponding load increments for the global analysis. Bolt yielding leading to leakage at the flange connection also limits the pressure capacity of the drywell head for these other temperature conditions. Both ambient and 538°C (1000°F) transient conditions provide somewhat higher capacities for pressure because the prying action at the flange is reduced for these cases due to global thermal deformation demands.

19C.3.5 Summary

Table 19C-10 provides a summary of the pressure fragility for the drywell head for the various thermal conditions. This table provides the mean and standard deviations for the lognormal PDF, along with the median value of pressure capacity and the 95% confidence value for the pressure capacity. The 95% confidence value is the pressure value such that there is a 95% confidence that the actual failure pressure will be higher. Figure 19C-11 illustrates the pressure fragility for the drywell head with temperature.

19C.4 Equipment Hatches

19C.4.1 Model Description

A detailed local model of a representative equipment hatch in the drywell was constructed to evaluate the pressure fragility for leakage from either tearing in the steel components or flange distortion and loss of seal. A hatch configuration in the upper drywell was chosen as the basis of the modeling. All equipment hatches have the same diameter, fabrication, section sizes, and closure configurations. The equipment hatch in the lower drywell differs only in that it penetrates the thicker pedestal wall. The thinner RCCV wall in the upper drywell will be more flexible and thus more critical for deformations leading to possible flange distortions or tearing in the steel components of the equipment hatch. The shear resistance along the barrel of the penetration is more critical for the thinner wall. The bolted flange connections perform similarly for the upper or lower drywell equipment hatches. The personnel airlock penetrations have a closure lid on the inside of the containment so that increasing pressure acts to keep this inner seal closed and the closure lid in compression. In addition, this configuration inhibits high temperatures during an accident from acting directly on the interior of the penetration. Thus, the equipment hatch in the upper drywell is used as the basis for this fragility analysis.

The local modeling for the equipment hatch is illustrated in Figure 19C-12. This figure also illustrates the temperature distribution for the 260°C (500°F) steady state thermal condition. The equipment hatch model includes a section of the RCCV wall around the penetration. Displacement boundary conditions, extracted from the global RCCV model, are imposed on the cut sections of the RCCV wall in the local model. This enforces the deformation patterns from the global response of the containment system on the local model while capturing more refinement in the structural response of the equipment hatch components. A contact surface between the flanges is modeled to allow flange separation to develop. The closure bolts are modeled with beam elements of the appropriate length, cross-sectional area, and initial pre-stress. A thermal analysis, consistent with that performed for the global model, was performed for the local model to establish the temperature distributions in the refined mesh of the local model. The thermal and pressure loads were incrementally applied in coordination with the displacement boundary conditions for the same loading states in the global model to evaluate the failure modes and failure pressure levels in the equipment hatch.

19C.4.2 Median Capacity Analysis

Under the temperature and increasing internal pressure, the RCCV wall experienced significant cracking in the outer half of the wall around the equipment hatch penetration but maintained good shear resistance. Figure 19C-13 plots contours for the accumulated equivalent plastic strains in the steel components of the equipment hatch at a pressure of 2.17 MPaG (315 psig) or a load factor of 7 times the P_d for the 260°C (500°F) thermal conditions. This figure indicates some distress around the thickened support plate connection, but with more extensive yielding in the barrel section near

the connection with the outer ring stiffener. The peak plastic strain shown for this load factor is below the failure strain criterion needed for tearing. Evaluation of these results against the median failure criterion indicates that flange separation and leakage develop before tearing of the steel components. It is found that the median failure pressure sufficient to cause leakage for this representative equipment hatch configuration is 1.882 MPaG (273.0 psig) or 6.07 P_d. An examination of the bolt responses shows that section yield in the bolts does not develop until after this pressure so that leakage is controlled by the flange separation. Similarly, tearing of the liner at the connection with the thickened support plate on the equipment hatch did not occur before leakage at the bolted flange. To further evaluate and confirm this finding, a more detailed analysis of the liner and anchorage system and the rectangular stiffener plate around the equipment hatch penetration was performed. This local effects slice model includes the embedded T-anchors and the thickened stiffener plate along with a slice of concrete where boundary conditions were supplied by the local model. Figure 19C-14 plots the plastic strains in the liner and thickened plate at a load factor of 7 times the design pressure for the 260°C (500°F) steady state thermal conditions. This local slice model shows peak plastic strains of 0.56% along the top of the thickened plate, and plastic strains of about 0.2% along the connections of the T-anchors. Again, these strain levels are well within the failure criteria for tearing, and these results confirm that liner tearing would not occur before leakage at the bolted connection.

19C.4.3 Evaluation for Uncertainty

Variations in the analyses using 95% confidence values for the yield stress of the steel material and for the yield stress of the bolt material were performed to evaluate the uncertainties in material properties. These were two separate analyses using the 95% confidence value of each and the median values of all other parameters. A separate analysis was also performed using a 95% confidence value for the bolt prestress to assess the uncertainty in this parameter. Reevaluation of the median-based analysis now using the 95% confidence value of the flange separation distance was performed to assess the uncertainty in this parameter. Table 19C-11 summarizes the results of these studies for evaluation of the uncertainty. The table provides the failure pressures identified and the calculated lognormal standard deviations for variation of the parameters identified. The composite lognormal standard deviation including the modeling uncertainty is also shown in the table. For the equipment hatch, the pressure capacity is limited by leakage at the bolted flange, which is controlled by flange separation. The pressure capacity is most affected by variations in the bolt prestress and distance of flange separation causing leakage. The bolt prestress affects the pressure required for initial flange unseating, after which the stiffness of the bolts govern the flange separation leading to leakage past the seal. Variation in the bolt yield has little effect on the pressure capacity because it does not change the mode of failure, and sufficient flange separation develops for leakage before bolt yielding.

19C.4.4 Variation with Temperature

The variation with temperature for the failure pressure causing leakage in the equipment hatch penetration was evaluated using median-based analyses for the ambient (normal operating) and 538°C (1000°F) transient thermal conditions. Again, thermal analyses, consistent with the global model analyses, were performed for the local equipment hatch model to establish the temperature distributions within the refined modeling. The loads from increasing drywell pressure were then applied along with the boundary conditions from the global model at the corresponding load increments for the global analysis. The evaluation for ambient thermal conditions shows that the pressure capacity was still limited by leakage due to flange separation, which has a higher capacity than at elevated temperatures. For the 538°C (1000°F) transient thermal conditions, leakage due to flange separation occurs at a much reduced pressure capacity. This reduced capacity is due to the configuration where the high temperatures act directly on the interior of the penetration and closure lid. This causes a thermally-induced bending load that acts to separate the toe of the flanges coupled with softening of the material at elevated temperatures that reduces the stiffness of the bolted flange connection.

19C.4.5 Summary

Table 19C-12 provides a summary of the pressure fragility for a representative equipment hatch for the variations in thermal conditions during an accident. This table provides the mean and standard deviations for the lognormal PDF, along with the median value of pressure capacity and the 95% confidence value for the pressure capacity. The 95% confidence value is the pressure value such that there is a 95% confidence that the actual failure pressure will be higher. Figure 19C-15 illustrates the pressure fragility for the equipment hatch with temperature. A significant drop off in the pressure capacity of the equipment hatch penetrations is found for extreme accident temperatures because the temperature can act directly inside the penetration and on the inside surface of the closure connections.

These analyses indicate that tearing of the liner at the connections of thickened support plates around the equipment hatch penetrations is not the failure mechanism that limits the pressure capacity of the equipment hatch. This analysis result apparently conflicts with experimental data for over-pressurization tests on the 1:6 scale model reported in Reference 19C-20. There are several differences between the test conditions for this Sandia 1:6 scale model and the configuration for the ESBWR equipment hatch penetrations. First, the Sandia 1:6 scale model did not have any internal support structures connected to the RCCV. Under internal pressure, the barrel section on this type of containment undergoes “ballooning” deformation, which develops large hoop strain at the locations of the penetrations. In the ESBWR, the drywell equipment hatch is located just above the diaphragm floor connection with the RCCV wall, and the RCCV is integral with the reactor building floors connecting to the exterior of the RCCV. This internal and external support for the ESBWR configuration restricts the radial deformation and hoop strains near the equipment hatch. Secondly, the Sandia 1:6 scale model employed stud type anchorages for the liner, while the ESBWR design

uses continuous vertical T-beams for anchoring the liner to the RCCV wall. The continuous vertical anchorages along the edges of the thickened plates at the penetrations provide more support for this connection than the stud type anchorages. Finally, these analyses also consider thermal loads due to elevated temperatures, whereas the Sandia 1:6 scale tests were conducted at uniform ambient temperatures. The thermal loads cause compressive membrane stress in the liner that counteracts the tension stress under the pressure loads. Thus, while the level of tension strain needed in the analysis to cause failure may be similar to that determined from the Sandia 1:6 scale model testing, the pressure levels required to develop that strain in the ESBWR analyses is larger as a relative factor on the design pressure.

19C.5 Pressure Fragility Summary

The fragility of the ESBWR primary containment system to over-pressurization under accident conditions is summarized in Table 19C-13. This table provides the median value and a 95% confidence value for the failure pressures causing the various failure modes leading to a breach in the containment boundary. The failure pressures are provided in terms of a factor on the design pressure of 0.31 MPaG (45 psig) and as the actual gauge pressure (MPaG). Additional failure mechanisms for tearing of the liner, either at the equipment hatch penetration or drywell head connections, and tearing of the steel components for the equipment hatch and drywell head were also considered but were not controlling. Figure 19C-16 plots the fragility for the various failure modes for the 260°C (500°F) steady state thermal condition. The median pressure capacity for this condition is limited by leakage at the drywell head flange which is caused by bolt yielding. The subsequent failure modes, in order of increasing median failure pressure limits, are: 1) tearing of the liner at the connection of the RCCV wall to the top slab, 2) failure of the RCCV wall at the connection with the top slab due to shear failure of the upper pool girders supporting the top slab, and 3) leakage at the bolted flange connection of the equipment hatch type penetrations due to flange separation. Under normal operating (ambient) thermal conditions, the pressure capacity is limited by tearing of the liner at the RCCV wall connection with the top slab. For the 538°C (1000°F) transient thermal condition, the pressure capacity is limited by leakage at the bolted flange connection in the equipment hatch. In this scenario, the inside of the equipment hatch penetration is exposed to the extreme temperatures considered, and capacity is significantly reduced by thermally-induced stress at this bolted connection.

19C.6 References

19C-1 ANACAP-U, Version 2.5, Theory Manual, ANA-QA-145, ANATECH Corp., San Diego, CA, 1998.

19C-2 ABAQUS/Standard, Version 5.8, Hibbitt, Karlssen, and Sorensen, Inc., Pawtucket, RI, 1998.

19C-3 Rodabaugh, E. C., and Desai, K. D., "Realistic Seismic Design Margins of Pumps, Valves, and Piping," NUREG/CR-2137, USNRC, Washington, DC, June 1981.

19C-4 Chu, T. Y., Pilch, M. M., et. al., "Lower Head Failure Experiments and Analyses," NUREG/CR-5582, USNRC, Washington, DC, February 1999.

19C-5 Brister, P. M., "Code Design Criteria in the USA, Evaluation of Strength Properties," Proceedings of the 3rd International Conference on Pressure Vessel Technology, Tokyo, Japan, April 18-22, 1977.

19C-6 Interim Guidelines Advisory No. 2, Chapter 8. Metallurgy and Welding, SAC 99-01, Applied Technology Council, University of California, Berkely, CA, 1994.

19C-7 Luecke, W. E., et. al., "Mechanical Properties of Structural Steels," NIST NCSTARR 1-3D, Federal Building and Fire Safety Investigation of the World Trade Center Disaster, National Institute of Standards and Technology, Washington, DC, September 2005.

19C-8 Bournonville, M., Dahnke, J., and Darwin, D., "Statistical Analysis of the Mechanical Properties and Weight of Reinforcing Bars," Report SL 04-1, Structural Engineering and Engineering Mechanics, University of Kansas, December 2004.

19C-9 Brinkman, C. R., Sikka, V. K., and King, R. T., "Mechanical Properties of Liquid-Metal Fast Breeder Reactor Primary Piping Materials," Nuclear Technology, Vol. 33, pages 77-95, April 1977.

19C-10 ITER Material Properties Handbook for Series 300 Stainless Steel, Document No. S 74 RE 1.

19C-11 Freskakis, G. H., "State-of-the-Art Report on High Temperature Concrete Design," Burns and Roe, Inc., Oradell, NJ, for U. S. Department of Energy, DOE/CH/94000-1, November 1985.

19C-12 "High Performance Steels for Bridges: HPS 70W," International Steel Group, Inc., Technical Specification Overview.

19C-13 James, R. J., Zhang, L., Rashid, Y. R., "Impact of High Velocity Objects into Concrete Structures – Methodology and Application," Proceedings of ASME International Mechanical Engineering Congress and Exposition, Washington, D. C., November, 2003.

19C-14 James, R. J. and Rashid, Y. R., "Severe Impact Dynamics of Reinforced Concrete Structures," Sixth European Conference on Structural Dynamics, Paris, France, September 2005.

19C-15 James, R. J., Zhang, L., Rashid, Y. R., Cherry, J. L., “Seismic Analysis of a Prestressed Concrete Containment Vessel Model,” NUREG/CR-6639, U. S. Nuclear Regulatory Commission, Washington, D. C., August 1999.

19C-16 James, R. J., Zhang, L, Rashid, Y. R., Cherry, J. L., “Seismic Analysis of a Reinforced Concrete Containment Vessel,” NUREG/CR-6707, U. S. Nuclear Regulatory Commission, Washington, D. C., August 1999.

19C-17 Dameron, R. A., Dunham, R. S., Rashid, Y. R, Sullaway, M. F., “Criteria and Guidelines for Predicting Concrete Containment Leakage,” Fourth Workshop on Containment Integrity, Sponsored by USNRC, Arlington, VA, June 1988.

19C-18 Parks, M. B., Walther, H. P., and Lambert, L. D., “Experiments to Determine the Leakage Behavior of Pressure-Unseating Equipment Hatches,” Transactions of the 11th International Conference on Structural Mechanics in Reactor Technology, SMiRT11, Volume F, August 1991.

19C-19 Pfeiffer, P. A., Kennedy, J. M., and Marchertas, A. H., “Thermal Effects in Concrete Containment Analysis,” NUREG/CP-0095, and Fourth Workshop on Containment Integrity, Sponsored by USNRC, Arlington, VA, June 1988.

19C-20 Clauss, D. B., “Round-Robin Analysis of the Behavior of a 1:6-Scale Reinforced Concrete Containment Model Pressurized to Failure: Posttest Evaluations,” NUREG/CR-5341, U. S. Nuclear Regulatory Commission, Washington, D. C., October 1989.

Table 19C-1 Summary of Thermal Material Properties

Material	Weight Density		Specific Heat		Thermal Conductivity	
	(lbf/ft^3)	(MN/m^3)	(Btu/lbm-^{o}F)	(J/kg-K)	(Btu/hr-ft-^{o}F)	(W/m-K)
Concrete	150	0.0235	0.210	879	0.92	1.6
Carbon Steel Liner	490	0.0770	0.110	460	30.9	53.5
Stainless Steel Liner	490	0.0770	0.118	494	9.42	16.3
Structural Steel	490	0.0770	0.110	460	30.9	53.5

SI units are the controlling units and English units are for reference only.

Table 19C-2 Summary of Elastic Mechanical Properties for Steels

	Ambient Conditions		260°C (500°F) Conditions		538°C (1000°F) Conditions	
	Median	**95%**	**Median**	**95%**	**Median**	**95%**
Carbon Steel						
Modulus (GPa)	203.4	200.0	185.1	182.0	122.1	120.0
Poisson's Ratio	0.289	0.289	0.295	0.295	0.304	0.304
Stainless Steel						
Modulus (GPa)	200.0	198.6	180.0	178.8	158.0	156.9
Poisson's Ratio	0.295	0.295	0.311	0.311	0.331	0.331
Bolting Material						
Modulus (GPa)	204.77	201.33	190.44	184.09	161.77	148.24
Poisson's Ratio	0.289	0.289	0.295	0.295	0.304	0.304

SI to English Unit Conversion (SI units are the controlling units and English units are for reference only):

1 Pa = 1.45038×10^{-4} psi

Table 19C-3 Summary of Plastic Mechanical Properties for Steels

	Ambient Conditions		260°C (500°F) Conditions		538°C (1000°F) Conditions	
	Median	**95%**	**Median**	**95%**	**Median**	**95%**
SA516 Grade 70						
Yield Stress (MPa)	335.3	295.3	301.8	265.3	261.5	211.2
Tensile Strength (MPa)	531.3	491.9	488.8	460.2	438.3	350.2
Elongation (%)	20.3	17.0	20.5	16.4	33.7	24.0
A572 Grade 50						
Yield Stress (MPa)	397.2	344.8	317.8	254.1	226.4	157.0
Tensile Strength (MPa)	521.4	451.0	516.2	438.8	318.0	233.6
Elongation (%)	22.5	18.0	25.0	20.0	30.0	24.0
A36						
Yield Stress (MPa)	339.3	287.1	271.4	214.0	193.4	130.8
Tensile Strength (MPa)	472.4	416.8	467.7	406.5	288.2	221.5
Elongation (%)	35.4	26.0	40.3	30.0	45.3	34.0
A709 HPS 70W						
Yield Stress (MPa)	554.8	495.9	443.9	357.0	316.3	226.1
Tensile Strength (MPa)	652.1	629.0	645.6	560.4	397.8	306.9
Elongation (%)	23.8	19.0	26.3	21.0	28.8	23.0
A615 Grade 60 Rebar						
Yield Stress (MPa)	473.1	437.9	378.5	315.3	269.7	199.7
Tensile Strength (MPa)	724.1	669.0	716.9	596.0	441.7	326.5
Elongation (%)	12.5	8.6	13.0	9.0	14.0	10.0
SA240 SS 304L						
0.2% Yield Stress (MPa)	200.0	179.4	137.5	106.6	108.3	78.2
Tensile Strength (MPa)	487.5	453.2	376.7	344.4	337.5	303.2
Elongation (%)	57.5	48.6	39.2	29.6	35.8	26.2
SA437 Grade B4B Bolting						
Yield Stress (MPa)	769.5	724.1	666.5	616.6	516.8	462.3
Tensile Strength (MPa)	1045.4	1000.0	901.5	851.5	692.9	638.5
Elongation (%)	15.5	13.0	16.6	14.1	17.6	15.2

SI to English Unit Conversion (SI units are the controlling units and English units are for reference only):

1 Pa = 1.45038×10^{-4} psi

Table 19C-4 Summary of Concrete Material Properties

Material/Property	Ambient Conditions		260°C (500°F) Conditions		538°C (1000°F) Conditions	
	Median	95%	Median	95%	Median	95%
RCCV Concrete (5 ksi)						
Comp Strength (MPa)	43.80	34.48	32.91	25.41	23.46	16.02
Strain at Peak Comp (%)	0.19	0.20	0.27	0.36	0.46	0.68
Modulus (GPa)	31.33	27.80	16.71	10.85	7.11	3.50
Tensile Strength (MPa)	4.12	3.66	3.10	2.39	2.21	1.51
Fracture Strain (xE-6)	131.6	99.1	185.3	139.6	310.6	234.0
Poisson's Ratio	0.22	0.18	0.22	0.18	0.22	0.18
Basemat Concrete (4 ksi)						
Comp Strength (MPa)	35.04	27.59	26.33	20.33	18.77	12.81
Strain at Peak Comp (%)	0.19	0.20	0.27	0.36	0.46	0.68
Modulus (GPa)	28.02	24.86	14.95	9.70	6.36	3.13
Tensile Strength (MPa)	3.69	3.27	2.77	2.14	1.98	1.35
Fracture Strain (xE-6)	131.6	99.1	185.3	139.6	310.6	234.0
Poisson's Ratio	0.22	0.18	0.22	0.18	0.22	0.18

SI to English Unit Conversion (SI units are the controlling units and English units are for reference only):
1 Pa = 1.45038×10^{-4} psi

Table 19C-5 Summary of Material Limits and Failure Criteria

Criteria	Ambient Conditions		260°C (500°F) Conditions		538°C (1000°F) Conditions	
	Median	95%	Median	95%	Median	95%
Global Modeling						
Section Shear Strain (%)	0.55	0.44	0.55	0.44	0.55	0.44
Rebar Fracture Strain (%)	5.0	2.0	5.5	2.2	6.0	2.4
Liner Tearing Strain (%)	1.72	1.40	1.75	1.17	2.87	1.96
Local Detailed Modeling						
Liner Tearing Strain (%)	2.59	2.26	2.62	2.04	4.30	3.40
Steel Tearing Strain (%)	2.54	2.21	2.57	1.99	4.22	3.31
Flange Separation (mm) [or First Yield in Bolts]	0.60	0.55	0.60	0.55	0.60	0.55

SI to English Unit Conversion (SI units are the controlling units and English units are for reference only):
25.4 mm = 1 in

Table 19C-6 Summary of Variance for Modeling Uncertainty

Analysis Type	Lognormal Standard Deviations		
	Ambient Conditions	260°C (500°F) Conditions	538°C (1000°F) Conditions
Global Modeling	0.1232	0.1355	0.1478
Local Modeling	0.1370	0.1482	0.1595

Table 19C-7 Summary of Uncertainty Evaluations for RCCV Pressure Capacity

Parameter	Type	RCCV Failure due to Section Shear Failure in Upper Pool Girders		Liner Tear at Connection of RCCV Wall to Top Slab	
		Pressure, MPaG (psig)		Pressure, MPaG (psig)	
		(LF on P_d)	β	(LF on P_d)	β
Median Failure Pressure	Median Values	1.741 (252.5)	--	1.643 (238.3)	--
		(5.61)		(5.30)	
Concrete Strength (MPa)	Material Property	1.624 (235.5)	0.0993	1.590 (230.6)	0.0434
		(5.24)		(5.13)	
Rebar Yield Stress (MPa)	Material Property	1.907 (276.6)	0.002	1.640 (237.9)	0.0248
		(6.15)		(5.29)	
Section Shear Strain Limit (%)	Failure Criterion	1.615 (234.2)	0.1028	N/A	--
		(5.21)			
Rebar Rupture Strain (%)	Failure Criterion	N/A	--	N/A	--
Liner Tearing Strain (%)	Failure Criterion	N/A	--	1.587 (230.2)	0.0446
				(5.12)	
Modeling Uncertainty	Modeling Methods	--	0.1355	--	0.1355
Composite Lognormal Standard Deviation	Composite	--	0.1970	--	0.1512

Note:
1. The median pressure capacities are updated to reflect the current analyses, but the β values, previously computed relative to the previous median pressure capacities, do not change.

Table 19C-8 Summary of Pressure Fragility for RCCV and Liner

Failure Mode and Thermal Condition	PDF Lognormal Distribution		Failure Pressure, MPaG (psig) (Load Factor on P_d)	
	μ	β	Median Value	95% Confidence Value
RCCV Capacity due to Shear Failure in Pool Main Girder				
260°C (500°F) Steady State	1.705	0.1970	1.741 (252.5)	1.234 (178.9)
			(5.61)	(3.98)
Ambient Steady State	1.911	0.1887	2.133 (309.4)	1.536 (222.8)
			(6.88)	(4.95)
538°C (1000°F) Transient	1.807	0.2056	1.928 (279.6)	1.346 (195.2)
			(6.22)	(4.34)
Liner Tear at RCCV Wall Connection with Top Slab				
260°C (500°F) Steady State	1.656	0.1512	1.643(238.3)	1.267 (183.8)
			(5.30)	(4.09)
Ambient Steady State	1.648	0.1403	1.628(236.1)	1.280 (185.6)
			(5.25)	(4.13)
538°C (1000°F) Transient	1.752	0.1623	1.810 (262.5)	1.368 (198.4)
			(5.84)	(4.41)

Table 19C-9 Summary of Uncertainty Evaluations for Drywell Head Pressure Capacity

Parameter	Type	Leakage Due to Bolt Yielding		Leakage Due to Steel Tearing	
		Pressure, MPaG (psig) (LF on P_d)	β	Pressure, MPaG (psig) (LF on P_d)	β
Median Failure Pressure	Median Values	1.426 (206.8) (4.60)	--	2.291 (332.3) (7.39)	--
Steel Yield Stress (MPa)	Material Property	1.652 (239.6) (5.33)	-0.0244	2.114 (306.6) (6.82)	-0.0292
Steel Rupture Strain (%)	Failure Criterion	N/A	--	1.705 (247.3) (5.50)	0.1016
Drywell Head Temperature	Loading Condition	1.587 (230.2) (5.12)	0.00	--	--
Bolt Prestress (MPa)	Loading Condition	1.587 (230.2) (5.12)	0.00	1.975 (286.4) (6.37)	0.0123
Bolt Yield Stress (MPa)	Failure Criterion	1.507 (218.6) (4.86)	0.0317		--
Modeling Uncertainty	Modeling Methods	--	0.1482		0.1482
Composite Lognormal Standard Deviation	Composite	--	0.1535		0.1824

Note:
1. The median pressure capacities are updated to reflect the current analyses, but the β values, previously computed relative to the previous median pressure capacities, do not change.

Table 19C-10 Summary of Pressure Fragility for Drywell Head

Failure Mode and Thermal Condition	PDF Lognormal Distribution		Failure Pressure, MPaG (psig) (Load Factor on P_d)	
	μ	β	Median Value	95% Confidence Value
Leakage Due to Bolt Yielding				
260°C (500°F) Steady State	1.514	0.1535	1.426 (206.8)	1.095 (158.8)
			(4.60)	(3.53)
Ambient Steady State	1.846	0.1428	1.983 (287.6)	1.552 (225.1)
			(6.40)	(5.01)
538°C (1000°F) Transient	1.760	0.1645	1.826 (264.8)	1.374 (199.3)
			(5.89)	(4.43)

Table 19C-11 Summary of Uncertainty Evaluations for Equipment Hatch Pressure Capacity

Parameter	Type	Leakage Due to Bolt Yielding		Leakage Due to Flange Distortion	
		Pressure, MPaG(psig) (LF on P_d)	β	Pressure, MPaG(psig) (LF on P_d)	β
Median Failure Pressure	Median Values	2.635 (382.2)	--	1.882 (273.0)	--
		(8.50)		(6.07)	
Steel Yield Stress (MPa)	Material Property	N/A	--	1.866 (270.6)	0.0050
				(6.02)	
Bolt Prestress (MPa)	Loading Condition	2.635(382.2)	0.000	1.776(257.6)	0.0350
		(8.50)		(5.73)	
Bolt Yield Stress (MPa)	Failure Criterion	2.542 (368.7)	0.0218	1.882 (273.0)	0.00
		(8.20)		(6.07)	
Flange Separation (mm)	Failure Criterion	N/A	--	1.810 (262.5)	0.0235
				(5.84)	
Modeling Uncertainty	Modeling Methods	--	0.1482	--	0.1482
Composite Lognormal Standard Deviation	Composite	--	0.1498	--	0.1542

Table 19C-12 Summary of Pressure Fragility for Equipment Hatch

Failure Mode and Thermal Condition	PDF Lognormal Distribution		Failure Pressure, MPaG (psig) (Load Factor on P_d)	
	μ	β	Median Value	95% Confidence Value
Leakage at Bolted Flanges due to Flange Separation				
260°C (500°F) Steady State	1.791	0.1542	1.882 (273.0)	1.443 (209.3)
			(6.07)	(4.65)
Ambient Steady State	1.860	0.1435	2.012 (291.8)	1.573 (228.1)
			(6.49)	(5.07)
538°C (1000°F) Transient	1.324	0.1651	1.181 (171.3)	0.888 (128.8)
			(3.81)	(2.86)

Table 19C-13 Summary of ESBWR Fragility for Over-Pressurization

Failure Mode	Failure Pressure Factor on P_d Followed by Gauge Pressure, MPaG (psig)					
	Ambient Conditions		260°C (500°F) Steady State		538°C (1000°F) Transient	
	Median	95%HC	Median	95%HC	Median	95%HC
DW Head Leakage due to Bolt Yielding	6.40	5.01	4.60	3.53	5.89	4.43
	1.983 (287.6)	1.552 (225.1)	1.426 (206.8)	1.095 (158.8)	1.826 (264.8)	1.374 (199.3)
Liner Tearing RCCV Wall at Top Slab	5.25	4.13	5.30	4.09	5.84	4.41
	1.628 (236.1)	1.280 (185.6)	1.643 (238.3)	1.267 (183.8)	1.810 (262.5)	1.368 (198.4)
EQ Hatch Leakage - Flange Separation	6.49	5.07	6.07	4.65	3.81	2.86
	2.012 (291.8)	1.573 (228.1)	1.882 (273.0)	1.443 (209.3)	1.181 (171.3)	0.888 (128.8)
RCCV Wall at Top Slab Connection	6.88	4.95	5.61	3.98	6.22	4.34
	2.133 (309.4)	1.536 (222.8)	1.741 (252.5)	1.234 (179.0)	1.928 (279.6)	1.346 (195.2)

Figure 19C-1 Calculation of Variance due to Modeling Uncertainty

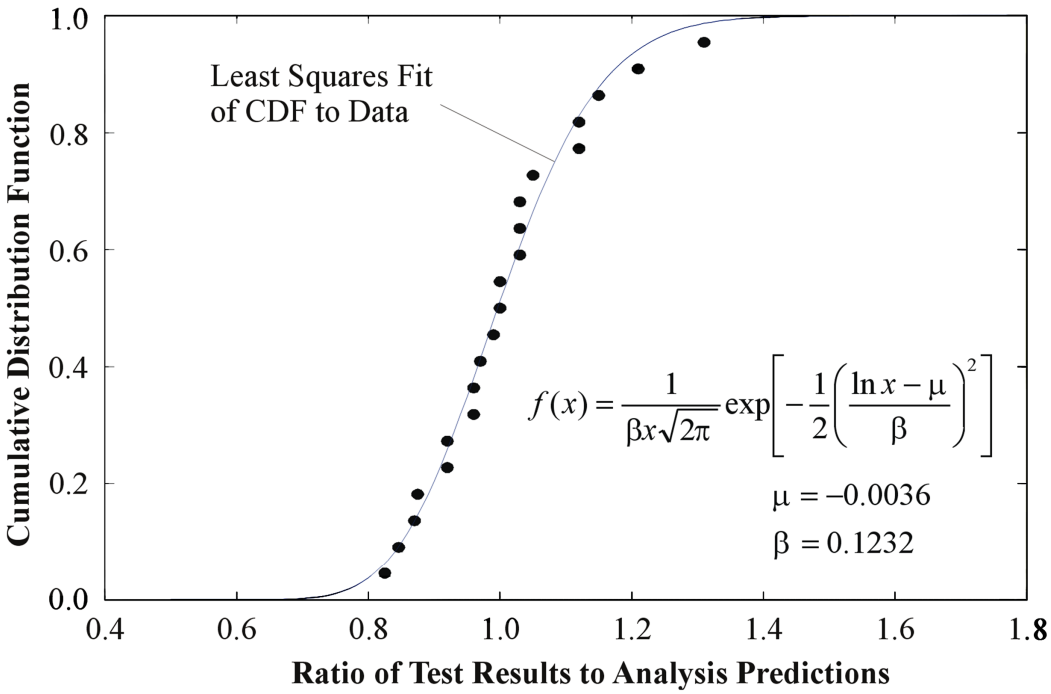


Figure 19C-2 Finite Element Model Showing the 260°C (500°F) Steady State Thermal Condition

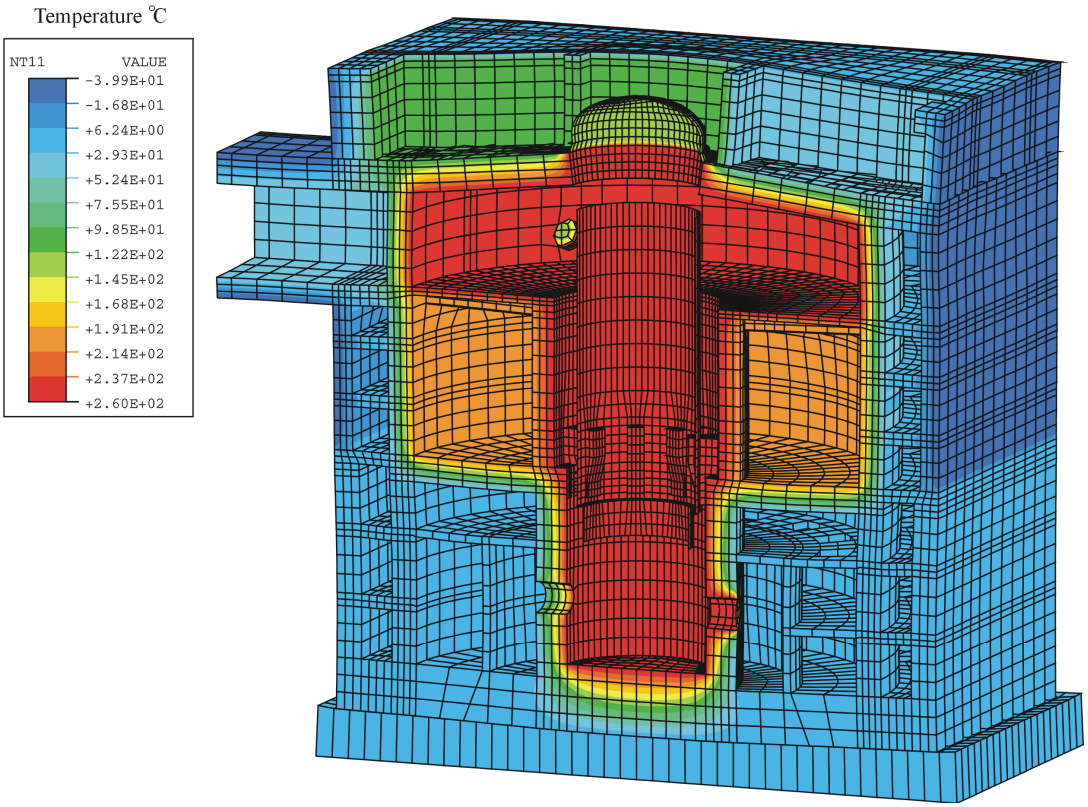


Figure 19C-3 Structural Response of RCCV at 1.24 MPaG (180 psig) Pressure

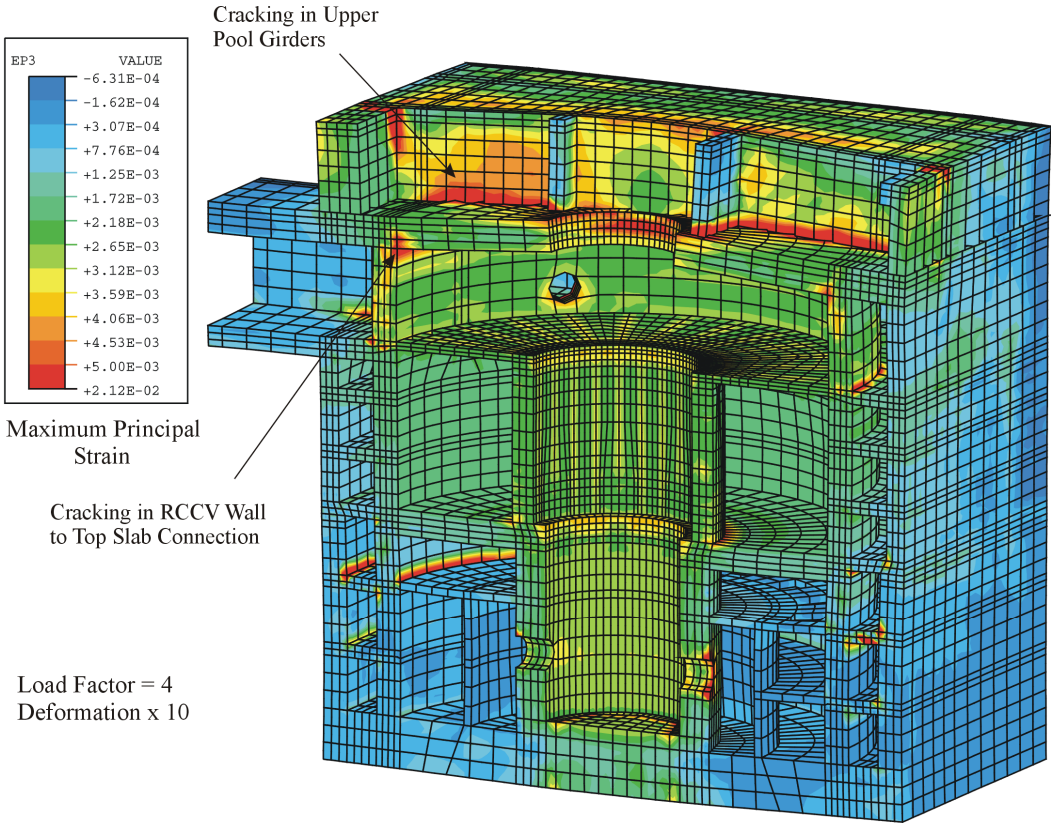


Figure 19C-4 Critical Location for Liner Tearing in RCCV

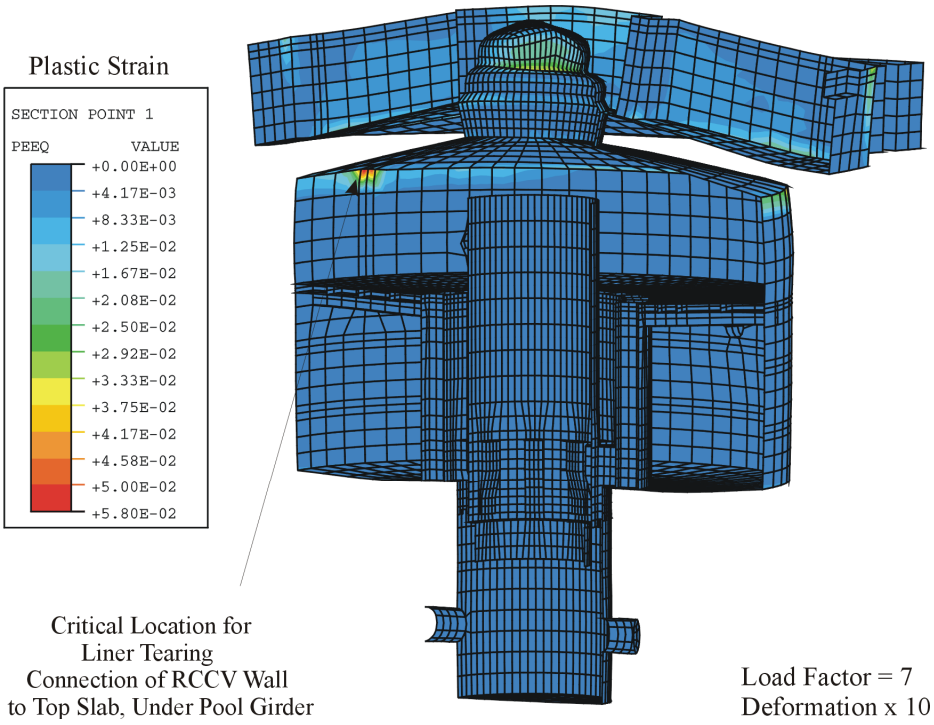


Figure 19C-5 Pressure Fragility for RCCV Wall Capacity with Temperature

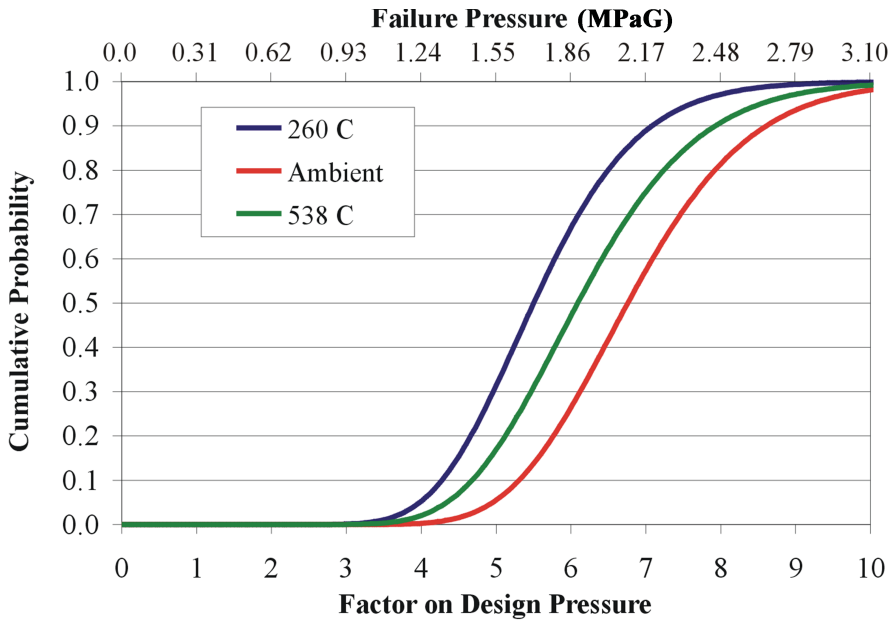


Figure 19C-6 Pressure Fragility for RCCV Liner Tearing with Temperature

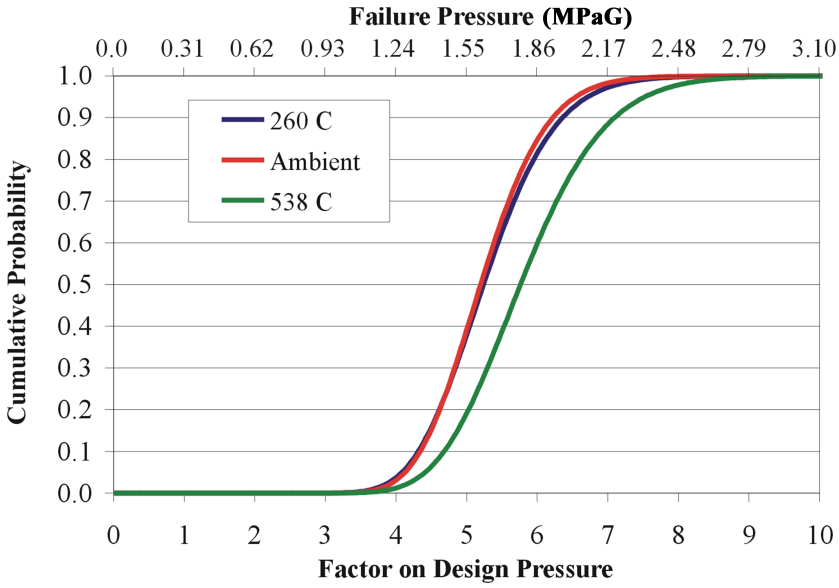


Figure 19C-7 Local Finite Element Model for Drywell Head

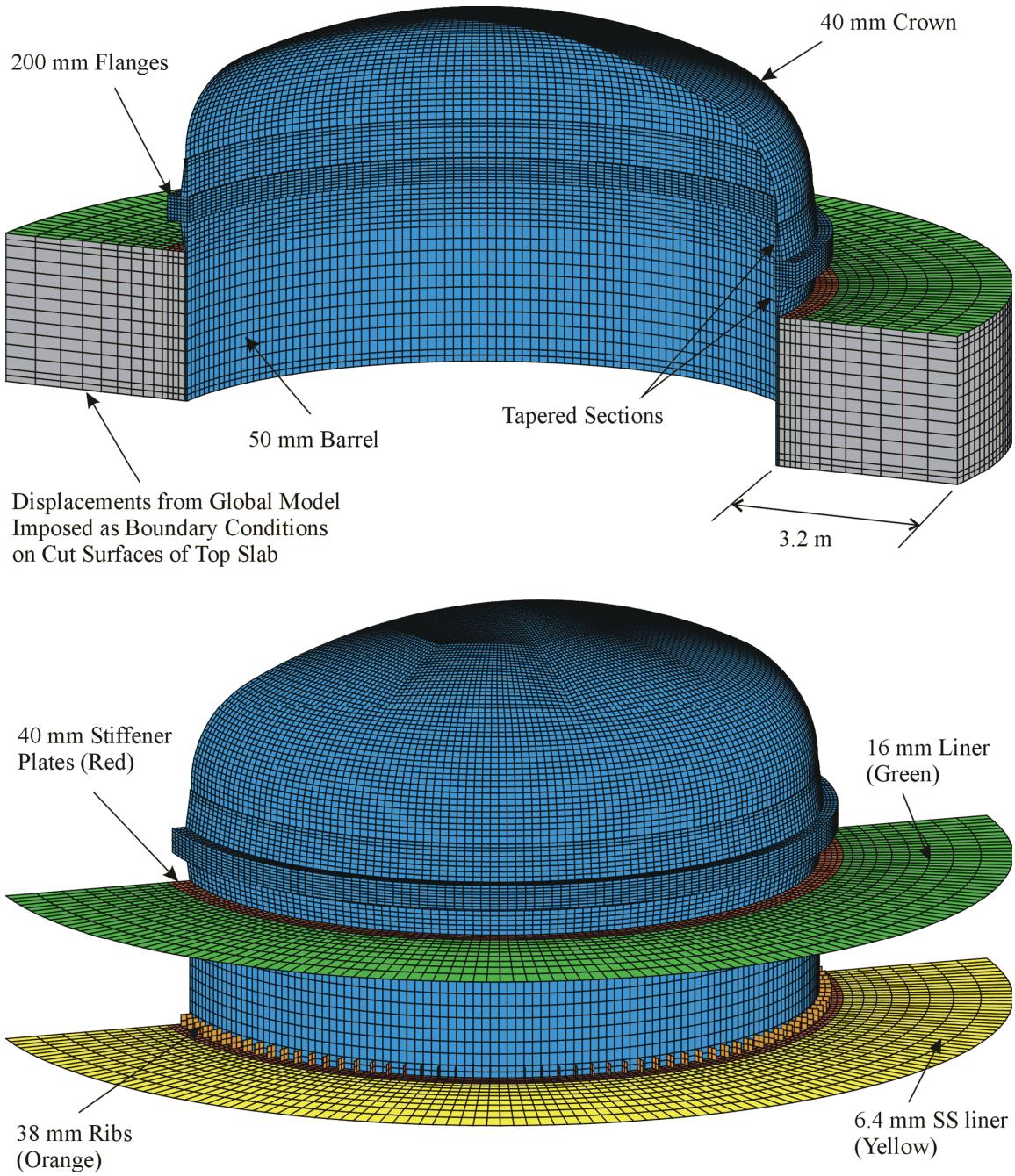


Figure 19C-8 Thermal Contours and Deformation for 260°C (500°F) Thermal Condition

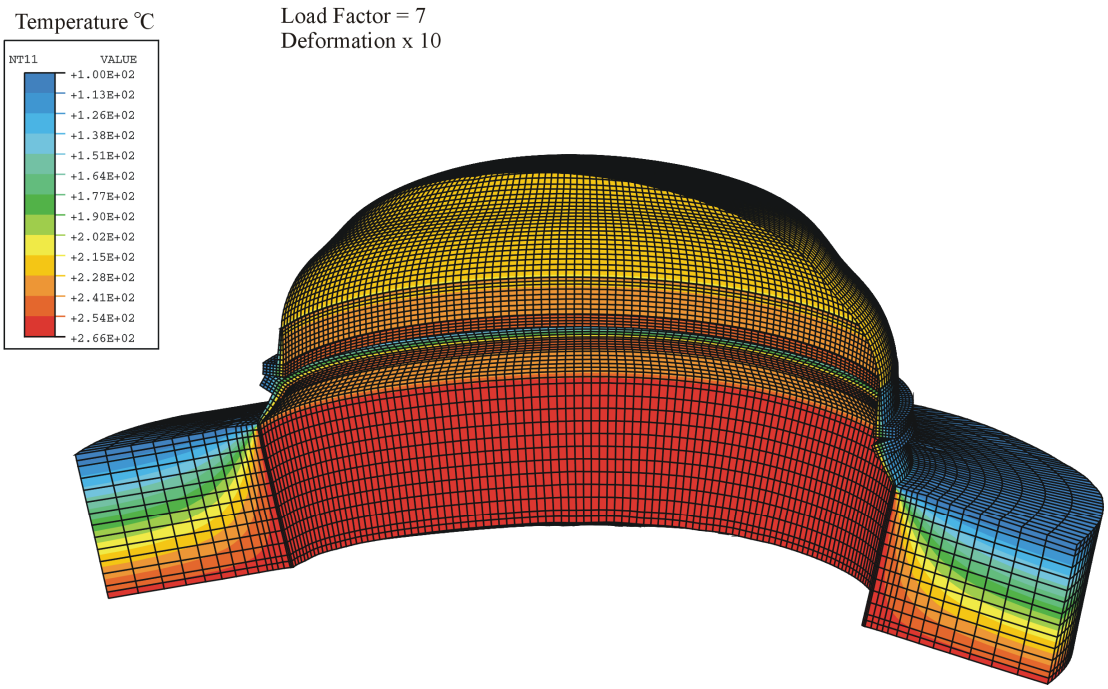


Figure 19C-9 Equivalent Plastic Strains in Steel Components at 2.17 MPaG (315 psig)

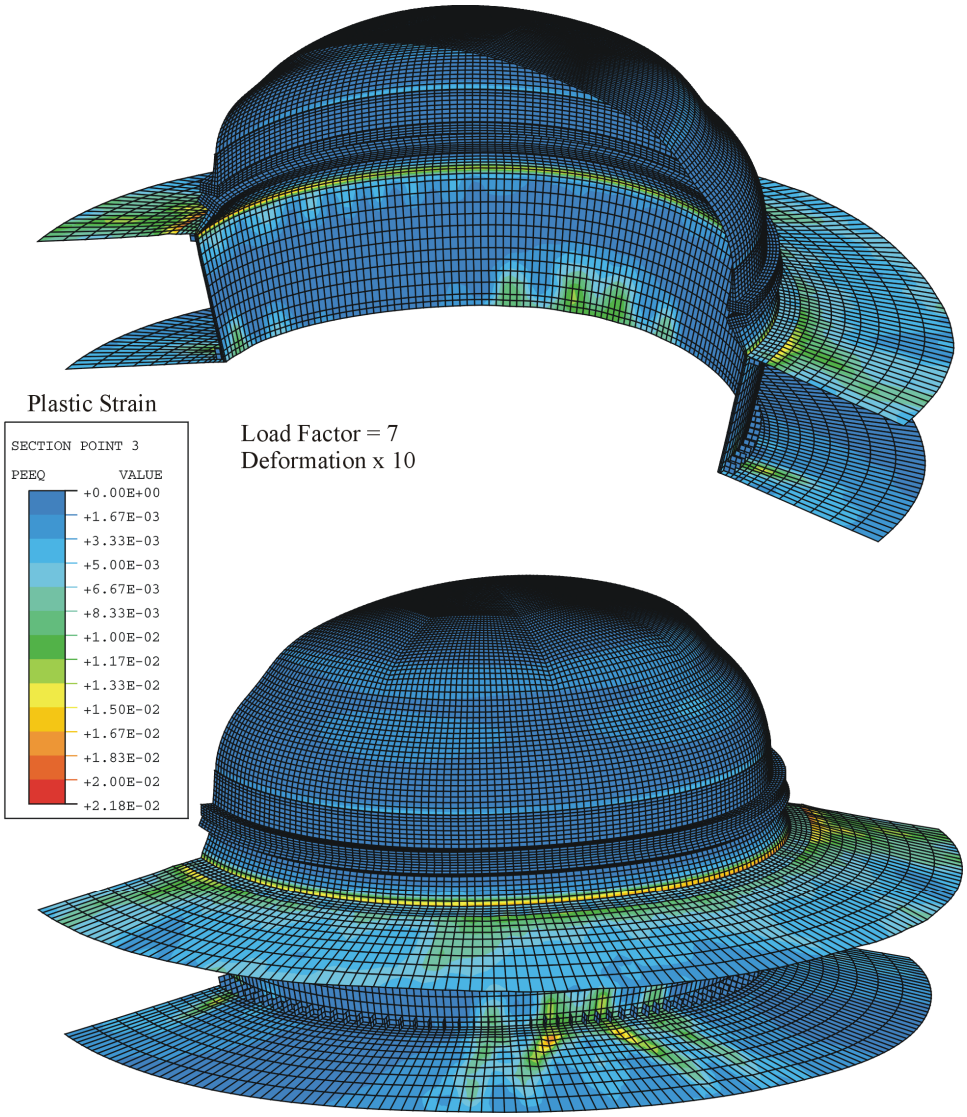


Figure 19C-10 Bolt Stresses in Drywell Head for 260°C (500°F) Thermal Condition

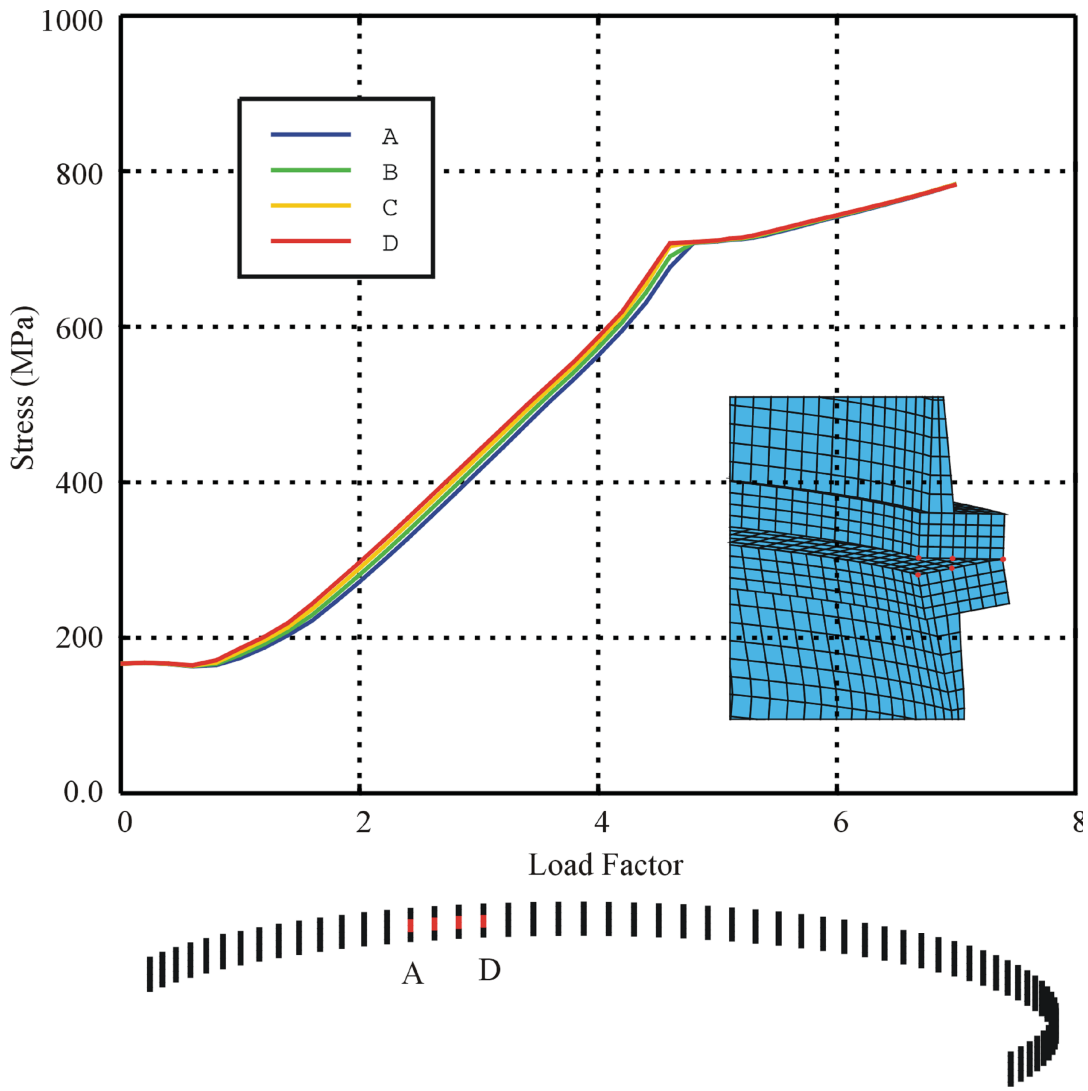


Figure 19C-11 Pressure Fragility with Temperature for Leakage at Drywell Head

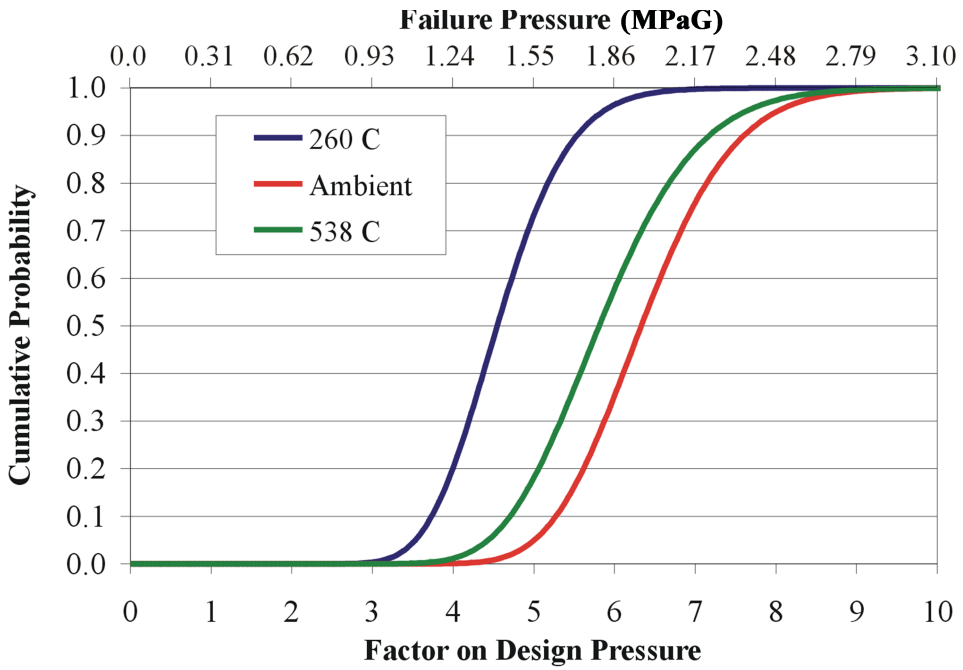


Figure 19C-12 Local Model of Drywell Equipment Hatch

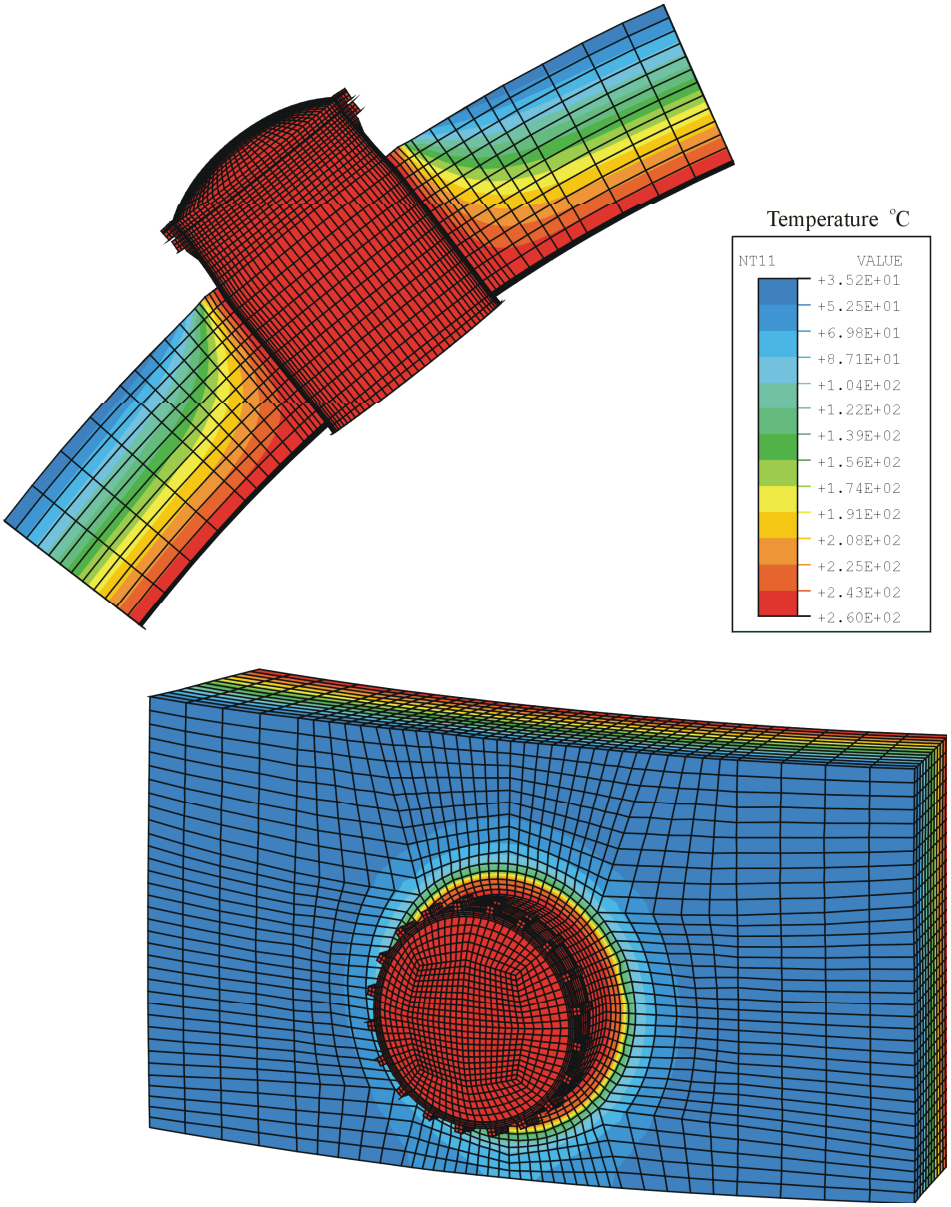


Figure 19C-13 Plastic Strains in EQ Hatch Steel Components, 260°C (500°F) Conditions

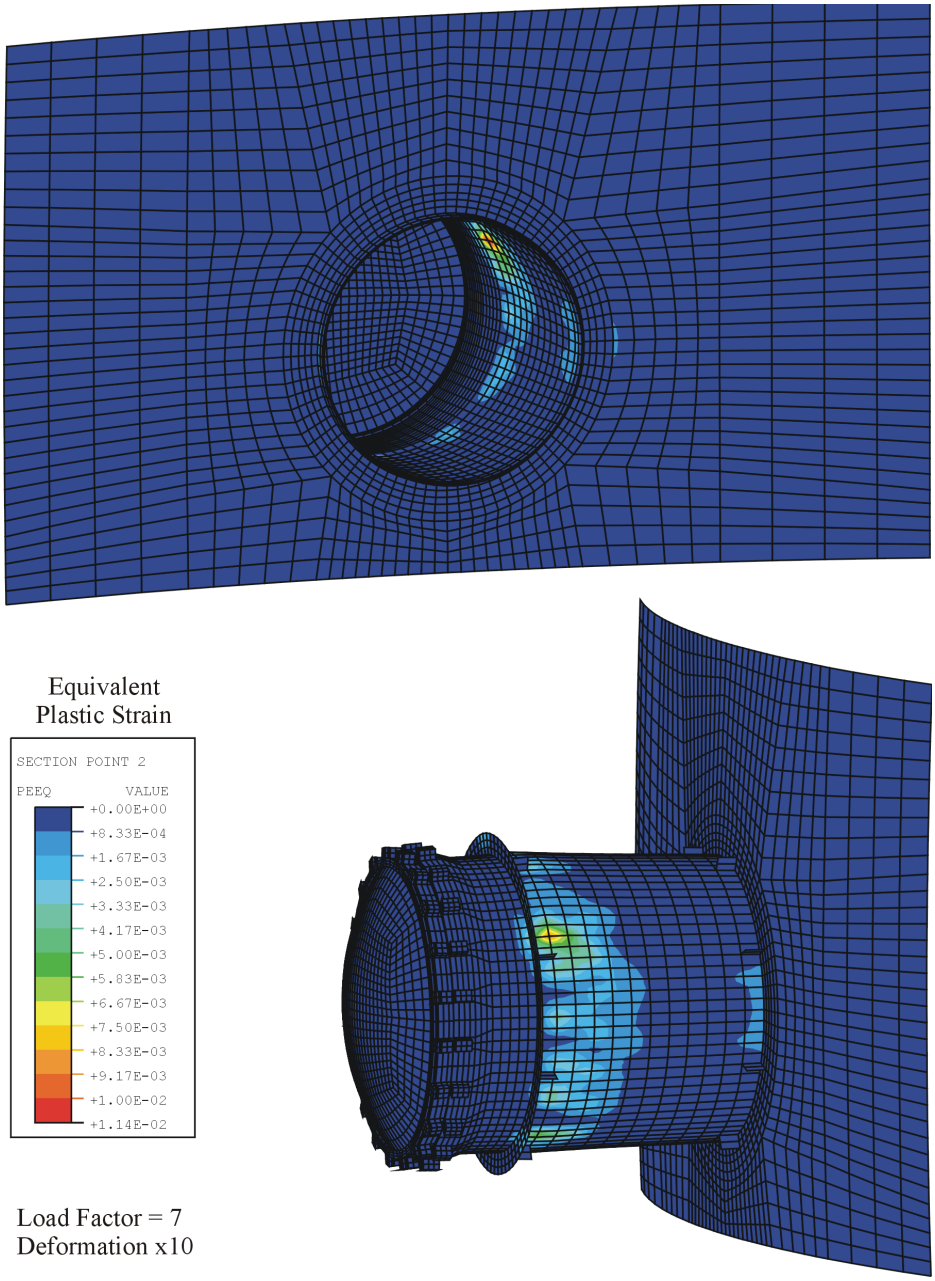


Figure 19C-14 Plastic Strains in Liner for Local Effects Slice Model

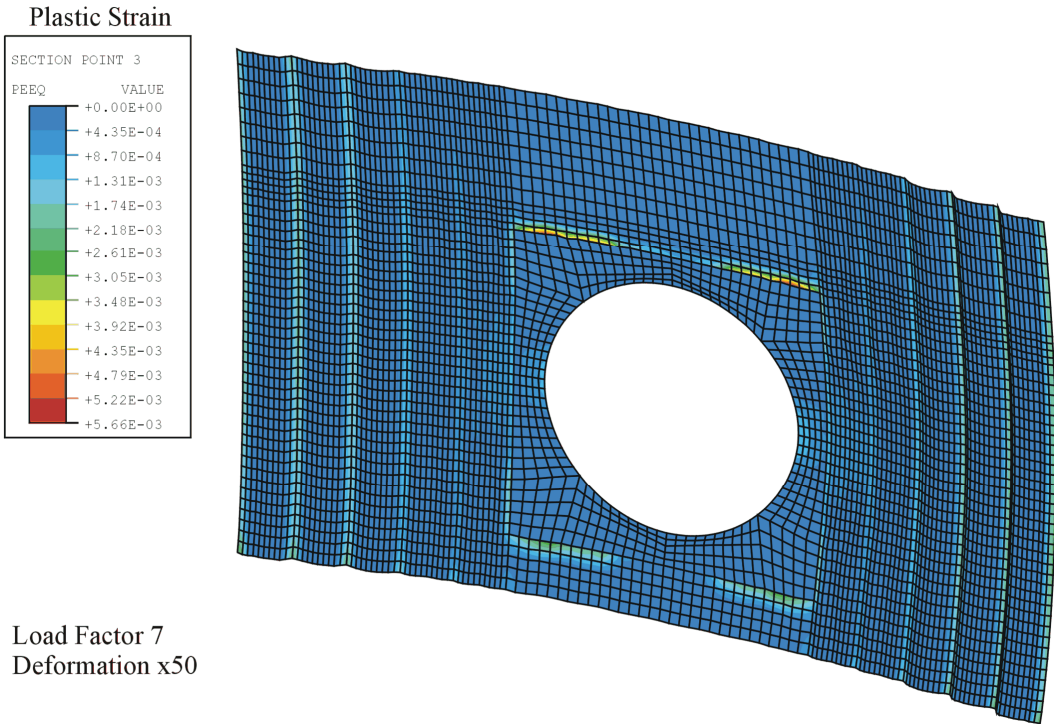


Figure 19C-15 Pressure Fragility with Temperature for Leakage at Equipment Hatch

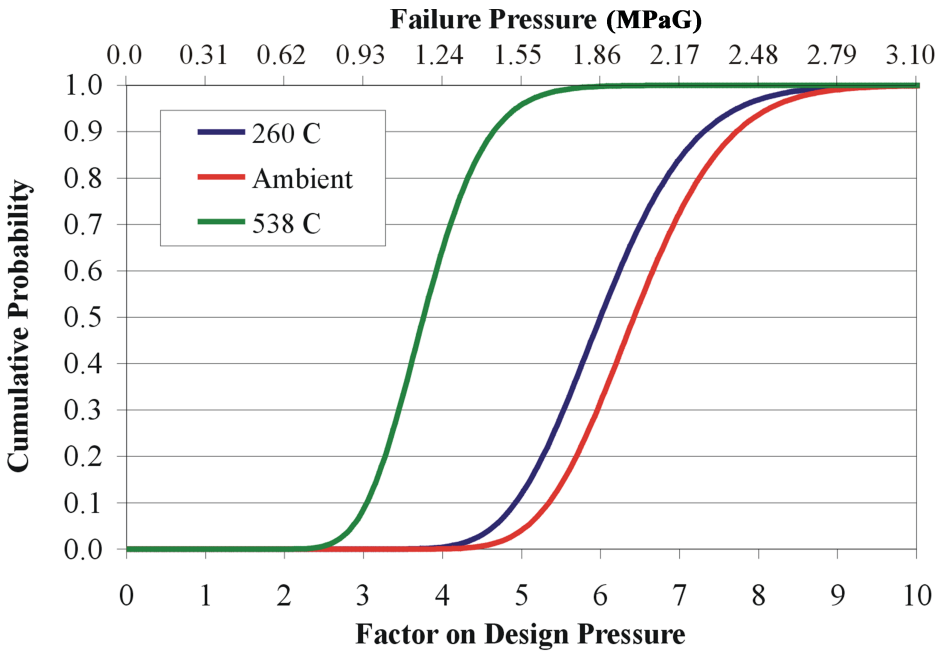
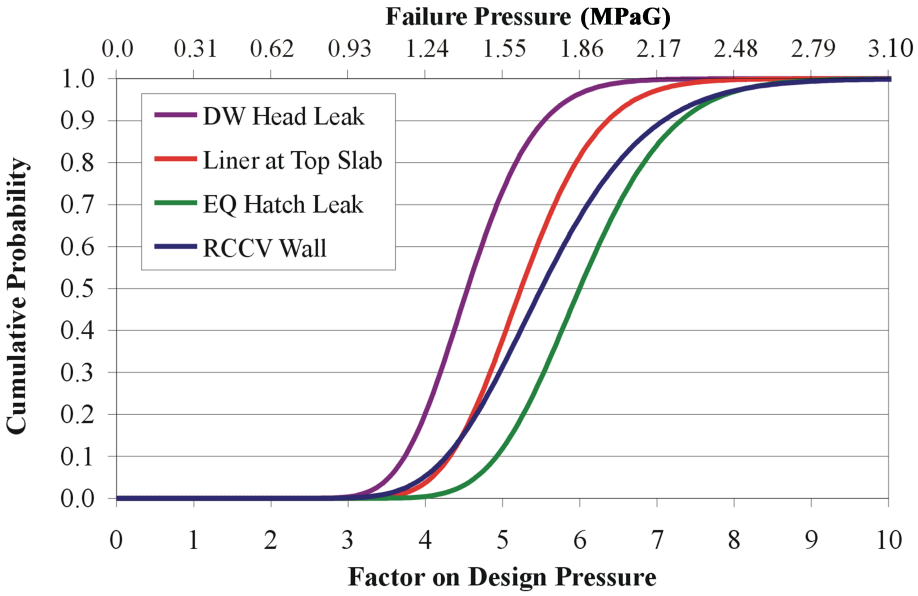


Figure 19C-16 Pressure Fragility at 260°C (500°F) Steady State Thermal Conditions



Appendix 19D Assessment of Malevolent Aircraft Impact

19D.1 Introduction and Background

A design-specific assessment of the intentional impact of a large commercial aircraft on the ESBWR has been performed in accordance with 10 CFR 50.150(a) and the results are provided herein in accordance with 10 CFR 52.47(a)(28). The assessment treats this as a beyond design basis event and has been performed using realistic analysis to demonstrate that, in the event that an ESBWR is struck by a large commercial aircraft, design features and functional capabilities exist to ensure that necessary functions are maintained. The following functions are the acceptance criteria on which the conclusions of this assessment are based:

- The reactor core remains cooled, or the containment remains intact
- Spent fuel cooling or spent fuel pool integrity is maintained

Specific assumptions used in the assessment of aircraft impact are based on requirements and guidance provided by the NRC and the Nuclear Energy Institute (NEI). The NRC provided the physical characteristics, including the loading function of the impacting aircraft, in July of 2007 (Reference 19D-1). The methodology for assessing effects for aircraft impact is described in NEI 07-13, “Methodology for Performing Aircraft Impact Assessments for New Plant Designs,” Revision 7 (Reference 19D-2).

This appendix describes the design features and functional capabilities of the ESBWR identified in the detailed assessment that assure the reactor core remains cooled or the reinforced concrete containment vessel (RCCV) remains intact, and spent fuel cooling or spent fuel pool integrity is maintained. In the following discussion, these identified design features are designated as "key design features."

19D.2 Scope of the Assessment

The evaluation of plant damage caused by the impact of a large, commercial aircraft is a complex problem involving phenomena associated with structural damage resulting from the initial impact, shock induced vibration, and the effects of aviation fuel fed fires. The analysis of the aircraft impact considers structural damage, taking into account:

- Assessment of the effects of aircraft fuselage and wing structure.
- Assessment of the effects of shock-induced vibration on systems, structures, and components (SSC).
- Assessment of the penetration of hardened aircraft components, such as engine rotors.
- Assessment of the extent of damage from fires fed by aviation fuel.

The assessment is further complicated by numerous locations where an aircraft could potentially strike critical ESBWR structures.

19D.3 Assessment Methodology

Results of a structural damage assessment predict that perforation of the Reactor Building (RB), Fuel Building (FB) and Control Building (CB) is possible in various locations and, therefore, realistic assessments of the damage to the corresponding internal SSCs caused by (1) secondary impacts, (2) induced vibration, and (3) burning aviation fuel were performed. Finite element models of the RB and FB were developed and various impact locations were analyzed to determine if external RB and FB walls would be perforated and, if perforation were to occur, the extent of internal damage within the impacted structure. Finite element models were not necessary for the CB because the acceptance criteria are met independent of any postulated equipment damage in the CB. Once damage from the initial impact was determined, the methods described in NEI 07-13 (Reference 19D-2) were followed to assess effects on SSCs credited in mitigating the event and to assure that the required SSCs remain functional despite secondary physical, fire and vibration effects of the aircraft impact on core cooling capability of the existing design.

19D.4 Results of Assessment

The following key design features and functional capabilities ensure that the ESBWR design can meet the acceptance criteria stated in Section 19D.1 following an intentional impact of a large commercial aircraft.

19D.4.1 RCCV

The RCCV, as described in Sections 3.8 and 6.2**,** is a key design feature that would protect safety systems located inside the RCCV from an impact of a large commercial aircraft. Since the RB entirely surrounds the RCCV, a direct strike on the RCCV is not possible. The assessment considered the effects of secondary impacts to the RCCV walls and to openings on the refueling floor. It concludes that, for all postulated primary strike locations, secondary strikes upon the RCCV would not result in missile penetration of the RCCV. Direct damage to the systems within the RCCV and exposure to an aviation-fuel-fed fire are prevented.

The assessment also finds that safety-related components inside the RCCV, including the reactor pressure vessel and associated emergency core cooling system (ECCS) piping, are unaffected by shock induced vibrations resulting from impact of a large commercial aircraft.

19D.4.2 Site Arrangement and Plant Structural Design

The design and arrangement of major structures associated with the ESBWR, as described in Section 1.2 and Figures 1.1-1 and 1.2-1 through 1.2-20, are key design features. Specifically, the assessment credited arrangement and design of the following building features to limit the location and effects of potential aircraft impacts on the RB:

1. The location and design of the RB structure, as described in Section 3.8 and shown on Figures 1.1-1 and 1.2-1 through 1.2-11 are key design features that protect the RCCV from

the impact of a large commercial aircraft. This includes protection provided by exterior walls, interior walls, intervening structures and barriers on large openings in the RB exterior walls.

2. The location and design of the Turbine Building structure, as shown on Figures 1.1-1 and 1.2-12 through 1.2-20, are key design features that protect the north wall (0° azimuth) of elevations 4650, 9060, 13570, 17500, 27000, 34000 the RB from the impact of a large commercial aircraft.
3. The location and design of the FB Building structure, as described in Section 3.8 and Appendix 3G and as shown on Figures 1.1-1 and 1.2-1 through 1.2-10, are key design features that protect the south wall (180° azimuth) elevations 4650, 9060, 13570, 17500 of the RB from the impact of a large commercial aircraft.

19D.4.3 Fire Barriers and Fire Protection Features

There are ESBWR design features that ensure successful safe shutdown capabilities for postulated aircraft impact damage scenarios. In particular, the ESBWR safety-related control systems incorporate four redundant divisions, and each division is spatially separated in its own quadrant in the RB and physical separation is provided either at a quadrant or compartment level. Although combustibles, fire and smoke could propagate vertically to floors above and below the damaged area, propagation horizontally (same elevation) to adjacent quadrants is controlled by 3-hour rated fire barriers.

Damage from an aircraft impact, including pressure from jet fuel deflagration, would be contained such that at least one division of safety-related equipment within one quadrant of the RB is unaffected. This key design feature ensures that at least one division of safety-related controls is available. In addition, the safe shutdown components that must actuate are located in the RB and within the cylinder of the RCCV, including supporting walls from elevation -11500 to 27000, or main steam tunnel, and thus would not be affected by the aircraft damage, vibration, or fire effects. Therefore, key design features ensure that the worst case effects of an aircraft impact are adequately confined by ensuring that the damage does not disable safety-related equipment in all four quadrants of the RB. The design and location of specific fire barriers that separate safety-related divisions within the RB are key design features for protection of core cooling equipment from the impact of a large commercial aircraft. The design and location of fire barriers are described in Section 9.5.1 and Appendix 9A, and shown on Figures 9A.2-1 through 9A.2-11. Fire barriers must contain fire damage and, depending on their location, must withstand the pressure effects (not physically damaged) that are postulated to occur in an aircraft impact. Fire propagation is confined within an area encompassed by two barriers if two typical fire doors are in series, such that the second fire door is the confinement boundary. Fire propagation is also confined within an area with one barrier if all elements of the barrier including the wall, the fire door, and the associated penetration seals are constructed with materials that can withstand a differential pressure of 0.034 MPa (5 psi). Fire barriers that are key design features are listed in Table 19D-1.

The locations of the RB HVAC Clean Area HVAC Subsystem (CLAVS) and the Contaminated Area HVAC Subsystem (CONAVS) trains are also key design features because they are separated such that no HVAC ducts penetrate the walls between the east and west sides of the RB.

Fire barriers are not considered to be key design features for the other site buildings, including the CB and FB because they are not needed to satisfy the acceptance criteria.

19D.4.4 Core Cooling Features

The design and physical separation of the Emergency Core Cooling systems described in Section 6.3, the Isolation Condenser System (ICS) including the IC/PCCS pools, described in Section 5.4.6; the locations of the inner and outer expansion pools, shown in Figure 1.2-8; the Control Rod Drive System described in Section 4.6, the Main Steam Isolation Valves (MSIV) described in Section 5.4.5; and the Safety-Related Instrumentation and Control System described in Section 7.1 are key design features for assuring core cooling following a reactor trip in response to an aircraft impact event.

In addition, the actions of scramming the reactor, closing the MSIVs and commencing operation of the ICS ensure the fuel in the reactor core is kept cooled.

These design features also assure core cooling if the reactor is already shut down and is being cooled while the reactor is in Mode 5 via the shutdown cooling mode of the Reactor Water Cleanup/Shutdown Cooling System (RWCU/SDC) described in Section 5.4.8, or the Fuel and Auxiliary Pools Cooling System (FAPCS) alternate shutdown cooling mode described in Section 9.1.3.2.

During Mode 6, ICS is unavailable. Loss of the shutdown cooling function of RWCU/SDC is discussed in Section 15.2.2.9. In the event that both RWCU/SDC trains are unavailable and the FAPCS alternate shutdown cooling or low pressure injection modes are unavailable, then the Gravity Driven Cooling System is capable of providing sufficient inventory to ensure core cooling for at least 72 hours.

19D.4.5 Spent Fuel Pool Cooling

In accident scenarios where the Fuel and Auxiliary Pools Cooling System (FAPCS) is unavailable, the inventory of water in the spent fuel pool provides passive heat removal. Make-up inventory for passive heat removal for the spent fuel pool is available from the Fire Protection System.

19D.4.6 Spent Fuel Pool Integrity

The spent fuel pool structure is located entirely below grade, as shown on Figures 1.2-1 through 1.2-4, and is a key design feature that assures that the integrity of the spent fuel pool is maintained in the event of the impact of a large commercial aircraft.

19D.5 Conclusions of Assessment

This assessment concludes that key design features and functional capabilities of the ESBWR ensure adequate protection of public health and safety in the event of an impact of a large commercial aircraft, as defined by the NRC. The acceptance criteria are satisfied by ensuring core cooling capability, and spent fuel pool integrity are maintained, based on best estimate evaluations. The assessment resulted in identification of key design features and functional capabilities described in Section 19D.4, changes to which are required to be controlled in accordance with 10 CFR 50.150(c).

19D.6 References

19D-1 Letter from D. Matthews, NRC to R. Brown, GEH, Subject: “Transmittal of Beyond Design Basis, Large Commercial Aircraft Characteristics,” July 31, 2007.

19D-2 NEI 07-13, “Methodology for Performing Aircraft Impact Assessments for New Plant Designs,” Revision 7, May 2009.

Table 19D-1 Fire and Other Barrier Key Design Features

{{{Security-Related Information - Withheld Under 10 CFR 2.390}}}
{{{Security-Related Information - Withheld Under 10 CFR 2.390}}}

Appendix 19AA Summary of Plant-Specific PRA Review

19AA.1 Introduction

In accordance with 10 CFR 52.79(a)(46), this appendix provides a summary of plant-specific PRA and its results.

19AA.2 Development of the ESBWR and Plant-Specific PRAs

The following Fermi site-specific PRA attributes were compared to the ESBWR PRA to determine if the ESBWR PRA is suitable for assessing risks and insights for Fermi 3:

- Loss of Preferred Power (LOPP) frequency – to determine if the site has unusual off-site power availability problems. The LOPP frequency is divided into plant-centered, switchyard, grid-related, and weather-related initiating events.
- Loss of Service Water frequency – to determine if any unusual characteristics would apply to a particular site, with consideration to loss of ultimate heat sink, and the effects of extreme seasonal temperatures.
- Seismic fragilities – to determine whether the site specific design response spectra affects the ESBWR Seismic Margins Analysis (SMA) or the PRA. Note that HCLPF values will be confirmed as described in Subsection 19.2.3.2.4.
- Other Known Site-Specific Issues – to identify site-specific initiating events that are not identified in the ESBWR PRA, such as unique offsite consequence issues.

These parameters represent site-specific features that have the potential to affect the PRA. To ensure that the ESBWR PRA is a bounding standard design, the site-specific values for these parameters were reviewed.

The ESBWR LOPP frequencies are based on NUREG/CR-6890, “Reevaluation of Station Blackout Risk at Nuclear Power Plants.” The Fermi 3 LOPP frequencies were compared to the ESBWR frequencies to identify any outliers. The data shows that grid-related losses are significantly more frequent than plant-centered, switchyard, or weather-related losses of power. Although there is a variance in the values for the LOPP frequencies, their range is acceptable. The conclusions in Subsection 19.2.3.1, Risk from Internal Events, remain valid for the minor variances in LOPP frequencies.

The ESBWR Loss of Service Water frequency is based on NUREG/CR-5750, “Rates of Initiating Events at U. S. Nuclear Power Plants: 1987-1995.” Loss of Service Water contributes less than one percent to the ESBWR Core Damage Frequency (CDF). Variances between the reported values depend on the design configuration (e.g., redundancy) of the current plants versus the ESBWR design, or external influences such as loss or degradation of heat sink. A review of the Fermi 3 design did not identify any site specific vulnerabilities that would cause the Loss of Service Water frequency to be higher than assumed in the ESBWR PRA. The Fermi 3 Plant Service Water

System (PSWS) is designed so that neither a single active nor single passive failure results in a complete loss of plant component cooling and/or plant dependence on any safety-related system. This is achieved through the use of redundant components, automatic valves and piping cross-connects for increased reliability. Additional PSWS design features to improve system reliability include:

- The PSWS is designed for remote operation from the main control room (MCR), for ease of restoration of its function after a component failure without a plant operating mode or power level change, and to operate even during a LOPP.
- The PSWS is designed to take suction from closed-cycle treated water systems and is not susceptible to raw water failure mechanisms (e.g., intake blockage). During normal operation the Circulating Water System supplies water to the PSWS. Makeup water to the Circulating Water System and the PSWS is provided from Lake Erie by the Plant Cooling Tower Makeup System. The PSWS is designed to operate for up to 7 days without makeup.
- The PSWS heat load is rejected to the Circulating Water System during normal operation, which is cooled by a Natural Draft Cooling Tower (Normal Power Heat Sink). Upon loss of the Circulating Water System, the PSWS heat load is rejected by the PSWS Mechanical Draft Cooling Towers (Auxiliary Heat Sink).
- During normal operation, one of two PSWS pumps per train is operating. The standby pump will automatically start upon detection of low PSWS pressure, loss of power to the operating pump, or a trip of the operating pump.
- The PSWS pumps each have a self-cleaning strainer which operates automatically. The pump discharge strainers have a remote manual override feature for their automatic cleaning cycle.

These items would reduce the Loss of Service Water frequency because of the redundant features included in the design and design features that minimize dependence on Lake Erie as a source of water for the PSWS.The conclusions in Subsection 19.2.3.1, Risk from Internal Events, remain valid for the minor variances in Loss of Service Water frequencies.

The ESBWR design incorporates a seismic response spectrum that bounds the potential U.S. sites. The conclusions in Subsection 19.2.3.2.4, Evaluation of External Event Seismic, remain valid for site-specific differences in seismic response.

There are no unusual terrain features that would affect meteorological data or plume dispersion. The conclusions in Section 19.2.5 for offsite consequences remain valid for any potential differences between site features.

In addition to the bounding treatment of PRA parameters, there are no departures from the standard design in any systems considered in the PRA model. Therefore, there are no site-specific design features that affect the PRA because the boundary of the certified design covers all of the SSCs necessary for the PRA.

19AA.3 Internal Flooding

19AA.3.1 Internal Flooding Associated with the Yard Area

The yard flood zone is essentially all outside areas of the site, and thus the site plot drawing (UFSAR Figure 2.1-204) illustrates the areas of concern. In addition Subsection 8.4.1.1 stipulates that the plant grade level is above the design flood level. The only components located in the yard that support a safety function are the manual fire hose connections to the Reactor Building and Fuel Building. These connections are also above design flood level. These connections provide the capability to connect another source of water to the Isolation Condenser/Passive Containment Cooling System (IC/PCCS) pools and the Spent Fuel Pool after seven days following a postulated accident. This timeframe is beyond the time required to be considered for the PRA; therefore, external flooding in the yard does not affect PRA equipment.

19AA.3.2 Internal Flooding Associated with the Yard Area

The Service Water Structure is a site-specific design feature. It is treated in a bounding manner in the ESBWR PRA to demonstrate that site-specific differences in Service Water Structure design do not have a significant effect on the PRA results. The Service Water Structure houses the four Service Water pumps and their associated power supplies and controls. Because Service Water is a RTNSS function, in accordance with Table 19A-4, the design and installation of the Service Water Structure is required to include protection from the effects of external and internal flooding.

In the ESBWR PRA model, the Service Water Structure is conservatively considered to be one flood zone. All four pumps are assumed to fail in an internal flood. Thus, the ESBWR PRA is bounding for design differences in the Service Water Structure. In addition, the ESBWR PRA model does not credit operator actions to mitigate a flooding event, so differences in building location are not significant.

The conclusion in Subsection 19.2.3.2.2 is that there are no significant flood-initiated accident sequences due to the low CDF. Overall, the potential effects of Service Water Structure design differences are accounted for by using a bounding analysis, and therefore, are not significant to the ESBWR PRA.

In summary, the ESBWR PRA provides a reasonable representation of the parameters and conditions that are specific to the Fermi site.

19 ACM Availability Controls Manual

The availability Controls Manual is transferred to the UFSAR from the DCD in its entirety with no changes.

19ACM AVAILABILITY CONTROLS MANUAL

TABLE OF CONTENTS

USE AND APPLICATION
1.1 Definitions....19ACM 1.0-1
1.2 Logical Connectors....19ACM 1.0-2
1.3 Completion Times....19ACM 1.0-3
1.4 Frequency....19ACM 1.0-4

2.0 Not Used

3.0 LIMITING CONDITION FOR OPERATION (ACLCO) APPLICABILITY....19ACM 3.0-1
3.0 SURVEILLANCE REQUIREMENT (ACSR) APPLICABILITY....19ACM 3.0-3

3.1 Not Used

3.2 Not Used

3.3 INSTRUMENTATION
3.3.1 Alternate Rod Insertion (ARI)....19ACM 3.3-1
3.3.2 Anticipated Transient Without Scram (ATWS) / Standby Liquid Control (SLC) System Actuation....19ACM 3.3-4
3.3.3 Feedwater Runback....19ACM 3.3-9
3.3.4 Diverse Protection System (DPS)....19ACM 3.3-11

3.4 Not Used

3.5 EMERGENCY CORE COOLING SYSTEMS (ECCS)
3.5.1 Gravity-Driven Cooling System (GDCS) Deluge Function....19ACM 3.5-1

3.6 CONTAINMENT SYSTEMS
3.6.1 Lower Drywell Hatches....19ACM 3.6-1
3.6.2 Passive Autocatalytic Recombiners (PARs)....19ACM 3.6-3
3.6.3 Passive Containment Cooling System (PCCS) Vent Fans....19ACM 3.6-6
3.6.4 Hydrogen Mitigation – Ignitors....19ACM 3.6-8

3.7 PLANT SYSTEMS
3.7.1 Emergency Makeup Water....19ACM 3.7-1
3.7.2 Fuel and Auxiliary Pools Cooling System (FAPCS) – Operating....19ACM 3.7-5
3.7.3 Fuel and Auxiliary Pools Cooling System (FAPCS) – Shutdown....19ACM 3.7-6
3.7.4 Reactor Building HVAC Accident Exhaust Filtration....19ACM 3.7-9
3.7.5 Control Room Heating and Ventilation System (CRHAVS) Post 72-Hour Long-Term Cooling....19ACM 3.7-12

19ACM AVAILABILITY CONTROLS MANUAL

TABLE OF CONTENTS

3.8 ELECTRICAL POWER SYSTEMS
3.8.1 Standby Diesel Generators – Operating 19ACM 3.8-1
3.8.2 Standby Diesel Generators – Shutdown 19ACM 3.8-3
3.8.3 Ancillary Diesel Generators 19ACM 3.8-6

4.0 DESIGN FEATURES
4.1 Basemat-Internal Melt Arrest and Coolability (BiMAC) Device 19ACM 4.0-1

ACM 1.0 USE AND APPLICATION

AC 1.1 Definitions

- NOTES -

1. Definitions are defined in Section 1.1 of the Technical Specifications (TS) and are applicable throughout the Availability Controls Manual (ACM) and ACM Bases. Only definitions specific to the ACM will be defined in this section.

2. The defined terms of this section and the TS appear in capitalized type and are applicable throughout the ACM and the ACM Bases.

3. When a term is defined in both the TS and the ACM, the ACM definition takes precedence within the ACM and the ACM Bases.

Term	Definition
ACTIONS	ACTIONS shall be that part of an Availability Control that prescribes Required Actions to be taken under designated Conditions within specified Completion Times.
AVAILABLE— AVAILABILITY	A system, subsystem, train, division, component, or device shall be AVAILABLE or have AVAILABILITY when it is capable of performing its specified risk informed function(s) and when all necessary attendant instrumentation, controls, normal or emergency electrical power, cooling and seal water, lubrication, and other auxiliary equipment that are required for the system, subsystem, train, division, component, or device to perform its specified risk informed function(s) are also capable of performing their related support function(s).

ACM 1.0 USE AND APPLICATION

AC 1.2 Logical Connectors

Logical Connectors are discussed in Section 1.2 of the Technical Specifications and are applicable throughout the Availability Controls Manual and Bases.

ACM 1.0 USE AND APPLICATION

AC 1.3 Completion Times

Completion Times are discussed in Section 1.3 of the Technical Specifications and are applicable throughout the Availability Controls Manual and Bases.

ACM 1.0 USE AND APPLICATION

AC 1.4 Frequency

Frequency is discussed in Section 1.4 of the Technical Specifications and is applicable throughout the Availability Controls Manual and Bases.

ACM 3.0 AVAILABILITY CONTROL LIMITING CONDITION FOR OPERATION (ACLCO) APPLICABILITY

ACLCO 3.0.1 ACLCOs shall be met during the MODES or other specified conditions in the Applicability, except as provided in ACLCO 3.0.2.

ACLCO 3.0.2 Upon discovery of a failure to meet an ACLCO, the Required Actions of the associated Conditions shall be met, except as provided in ACLCO 3.0.5 and ACLCO 3.0.6.

If the ACLCO is met or is no longer applicable prior to expiration of the specified Completion Time(s), completion of the Required Action(s) is not required, unless otherwise stated.

ACLCO 3.0.3 When an ACLCO is not met and the associated ACTIONS are not met, an associated ACTION is not provided, or if directed by the associated ACTIONS, action shall be initiated to:

a. Restore compliance with the ACLCO or associated ACTIONS;

b. Assess and manage the risk of the resulting unit configuration, and

---

- NOTE -

ACLCO 3.0.3.c shall be completed if ACLCO 3.0.3 is entered.

---

c. Enter the circumstances into the Corrective Action Program.

Exceptions to this ACLCO are stated in the individual ACLCOs.

ACLCO 3.0.4 When an ACLCO is not met, entry into a MODE or other specified condition in the Applicability shall only be made:

a. When the associated ACTIONS to be entered permit continued operation in the MODE or other specified condition in the Applicability for an unlimited period of time;

ACLCO Applicability

ACLCO 3.0.4 (continued)

b. After performance of a risk assessment addressing unavailable systems and components, consideration of the results, determination of the acceptability of entering the MODE or other specified condition in the Applicability, and establishment of risk management actions, if appropriate; exceptions to this ACLCO are stated in the individual ACLCOs; or

c. When an allowance is stated in the individual value, parameter, or other ACLCO.

This ACLCO shall not prevent changes in MODES or other specified conditions in the Applicability that are required to comply with TS or ACM ACTIONS or that are part of a shutdown of the unit.

ACLCO 3.0.5 Equipment removed from service or declared unavailable to comply with ACTIONS may be returned to service under administrative control solely to perform testing required to demonstrate its AVAILABILITY or the AVAILABILITY of other equipment. This is an exception to ACLCO 3.0.2 for the system returned to service under administrative control to perform the testing required to demonstrate AVAILABILITY.

ACLCO 3.0.6 When a supported system ACLCO is not met solely due to a support system ACLCO not being met, the Conditions and Required Actions associated with this supported system are not required to be entered. Only the support system ACLCO ACTIONS are required to be entered. This is an exception to ACLCO 3.0.2 for the supported system. In this event, a risk evaluation shall be performed in accordance with the Maintenance Rule Program. If an unacceptable risk is determined to exist, the appropriate Conditions and Required Actions of the ACLCO in which the loss of risk mitigation exists are required to be entered.

When a support system's Required Action directs a supported system to be declared unavailable or directs entry in Conditions and Required Actions for a supported system, the applicable Conditions and Required Actions shall be entered in accordance with ACLCO 3.0.2.

ACM 3.0 AVAILABILITY CONTROL SURVEILLANCE REQUIREMENT (ACSR) APPLICABILITY

ACSR 3.0.1	ACSRs shall be met during the MODES or other specified conditions in the Applicability for individual ACLCOs, unless otherwise stated in the ACSR. Failure to meet an ACSR, whether such failure is experienced during the performance of the ACSR or between performances of the ACSR, shall be failure to meet the ACLCO. Failure to perform an ACSR within the specified Frequency shall be failure to meet the ACLCO except as provided in ACSR 3.0.3. ACSRs do not have to be performed on unavailable equipment or variables outside specified limits.
ACSR 3.0.2	The specified Frequency for each ACSR is met if the ACSR is performed within 1.25 times the interval specified in the Frequency, as measured from the previous performance or as measured from the time a specified condition of the Frequency is met. For Frequencies specified as “once,” the above interval extension does not apply. If a Completion Time requires periodic performance on a “once per . . .” basis, the above Frequency extension applies to each performance after the initial performance. Exceptions to this ACSR are stated in the individual ACSRs.
ACSR 3.0.3	If it is discovered that an ACSR was not performed within its specified Frequency, then compliance with the requirement to declare the ACLCO not met may be delayed, from the time of discovery, up to 24 hours or up to the limit of the specified Frequency, whichever is greater. This delay period is permitted to allow performance of the ACSR. A risk evaluation shall be performed for any ACSR delayed greater than 24 hours and the risk impact shall be managed. If the ACSR is not performed within the delay period, the ACLCO must immediately be declared not met, and the applicable Condition(s) must be entered. When the ACSR is performed within the delay period and the ACSR is not met, the ACLCO must immediately be declared not met, and the applicable Conditions must be entered.

ACSR Applicability

ACSR 3.0.4	Entry into a MODE or other specified condition in the Applicability of an ACLCO shall only be made when the associated ACSRs have been met within their Specified Frequency, except as provided by ACSR 3.0.3. When an ACLCO is not met due to ACSRs not having been met, entry into a MODE or other specified condition in the Applicability shall only be made in accordance with ACLCO 3.0.4. This provision shall not prevent entry into MODES or other specified conditions in the Applicability that are required to comply with TS or ACM ACTIONS or that are part of a shutdown of the unit.

ACM B 3.0 AVAILABILITY CONTROL LIMITING CONDITION FOR OPERATION (ACLCO) APPLICABILITY

BASES

ACLCOs	ACLCO 3.0.1 through ACLCO 3.0.6 establish the general requirements applicable to all ACLCOs in Sections 3.1 through 3.8 and apply at all times, unless otherwise stated.
ACLCO 3.0.1	ACLCO 3.0.1 establishes the Applicability statement within each individual Requirement as the requirement for when the ACLCO is required to be met (i.e., when the unit is in the MODES or other specified conditions of the Applicability statement of each Control).
ACLCO 3.0.2	ACLCO 3.0.2 establishes that upon discovery of a failure to meet an ACLCO, the associated ACTIONS shall be met. The Completion Time of each Required Action for an ACTIONS Condition is applicable from the point in time that an ACTIONS Condition is entered. The Required Actions establish those remedial measures that must be taken within specified Completion Times when the requirements of an ACLCO are not met. This Requirement establishes that: a. Completion of the Required Actions within the specified Completion Times constitute compliance with a Control; and b. Completion of the Required Actions is not required when an ACLCO is met within the specified Completion Time, unless otherwise specified. There are two basic types of Required Actions. The first type of Required Action specifies a time limit in which the ACLCO must be met. This time limit is the Completion Time to restore an unavailable system or component to AVAILABLE status or to restore variables to within specified limits. If this type of Required Action is not completed within the specified Completion Time, remedial actions to document the failure to comply with the Availability Controls Manual (ACM) requirements are required. (Whether stated as a Required Action or not, correction of the entered Condition is an action that may always be considered upon entering ACTIONS.) The second type of Required Action specifies the

BASES

ACLCO 3.0.2 (continued)

remedial measures that permit continued operation of the unit that is not further restricted by the Completion Time. In this case, compliance with the Required Actions provides an acceptable justification for continued operation.

Completing the Required Actions is not required when an ACLCO is met or is no longer applicable, unless otherwise stated in the individual Control.

The nature of some Required Actions of some Conditions necessitates that, once the Condition is entered, the Required Actions must be completed even though the associated Conditions no longer exist. The individual ACLCO ACTIONS specify the Required Actions where this is the case.

The Completion Times of the Required Actions are also applicable when a system or component is removed from service intentionally. The reasons for intentionally relying on the ACTIONS include, but are not limited to, performance of ACSRs, preventive maintenance, corrective maintenance, or investigation of operational problems. Entering ACTIONS for these reasons must be done in a manner that does not compromise safety. Individual Controls may specify a time limit for performing an ACSR when equipment is removed from service or bypassed for testing. In this case, the Completion Times of the Required Actions are applicable when this time limit expires, if the equipment remains removed from service or bypassed.

When a change in MODE or other specified condition is required to comply with Required Actions, the unit may enter a MODE or other specified condition in which another Control becomes applicable. In this case, the Completion Times of the associated Required Actions would apply from the point in time that the new Control becomes applicable and the ACTIONS Condition(s) is entered.

BASES

ACLCO 3.0.3

ACLCO 3.0.3 establishes the actions that must be implemented when an ACLCO is not met and:

a. An associated Required Action and Completion Time is not met and no other Condition applies; or

b. The condition of the unit is not specifically addressed by the associated ACTIONS. This means that no combination of Conditions stated in the ACTIONS can be made that exactly corresponds to the actual condition of the unit. Sometimes, possible combinations of Conditions are such that entering ACLCO 3.0.3 is warranted; in such cases, the ACTIONS specifically state a Condition corresponding to such combinations and also that ACLCO 3.0.3 be entered immediately.

This Requirement requires: a) an Action to initiate efforts to restore compliance with the ACLCO or associated ACTIONS; b) assessing and managing the risk of the resulting unit configuration in accordance with the maintenance rule program (refer to Bases for ACLCO 3.0.4.b for discussion of risk evaluation scope); and c) an Action that requires entering the circumstances into the Corrective Action Program (CAP). These actions ensure that the appropriate resources will continue to be focused on restoring compliance with the ACLCO or associated ACTIONS and that the circumstances concerning failure to comply with the Availability Controls Manual (ACM) requirements will be reviewed. This review will be conducted in accordance with the procedural guidance for CAP notifications.

Exceptions to ACLCO 3.0.3 are addressed in the individual Requirements.

ACLCO 3.0.4

ACLCO 3.0.4 establishes limitations on changes in MODES or other specified conditions in the Applicability when an ACLCO is not met. It allows placing the unit in a MODE or other specified condition stated in that Applicability (i.e., the Applicability desired to be entered) when unit conditions are such that the requirements of the ACLCO would not be met, in accordance with ACLCO 3.0.4.a, ACLCO 3.0.4.b, or ACLCO 3.0.4.c.

BASES

ACLCO 3.0.4 (continued)

ACLCO 3.0.4.a allows entry into a MODE or other specified condition in the Applicability with the ACLCO not met when the associated ACTIONS to be entered permit continued operation in the MODE or other specified condition in the Applicability for an unlimited period of time. Compliance with Required Actions that permit continued operation of the unit for an unlimited period of time in a MODE or other specified condition provides an acceptable level of safety for continued operation. This is without regard to the status of the unit before or after the MODE change. Therefore, in such cases, entry into a MODE or other specified condition in the Applicability may be made in accordance with the provisions of the Required Actions.

ACLCO 3.0.4.b allows entry into a MODE or other specified condition in the Applicability with the ACLCO not met after performance of a risk assessment addressing unavailable systems and components, consideration of the results, determination of the acceptability of entering the MODE or other specified condition in the Applicability, and establishment of risk management actions, if appropriate.

The risk assessment may use quantitative, qualitative, or blended approaches, and the risk assessment will be conducted using the plant program, procedures, and criteria in place to implement 10 CFR 50.65(a)(4), which requires that risk impacts of maintenance activities be assessed and managed. The risk assessment, for the purposes of ACLCO 3.0.4.b, must take into account all inoperable Technical Specification equipment regardless of whether the equipment is included in the normal 10 CFR 50.65(a)(4) risk assessment scope. The risk assessments will be conducted using the procedures and guidance endorsed by Regulatory Guide 1.182, "Assessing and Managing Risk Before Maintenance Activities at Nuclear Power Plants." Regulatory Guide 1.182 endorses the guidance in Section 11 of NUMARC 93-01, "Industry Guideline for Monitoring the Effectiveness of Maintenance at Nuclear Power Plants." These documents address general guidance for conduct of the risk assessment, quantitative and qualitative guidelines for establishing risk management actions, and example risk management actions. These include actions to plan and conduct other activities in a manner that controls overall risk, actions to increase risk awareness by shift and management personnel, actions to reduce the duration of the condition, actions to minimize the magnitude of risk increases (establishment of backup success paths or compensatory measures), and a determination that the proposed MODE change is acceptable.

BASES

ACLCO 3.0.4 (continued)

Consideration should also be given to the probability of completing restoration such that the requirements of the ACLCO would be met prior to the expiration of ACTIONS Completion Times that would require exiting the Applicability.

ACLCO 3.0.4.b may be used with single or multiple systems and components unavailable. NUMARC 93-01 provides guidance relative to consideration of simultaneous unavailability of multiple systems and components.

The results of the risk assessment shall be considered in determining the acceptability of entering the MODE or other specified condition in the Applicability, and any corresponding risk management actions. The ACLCO 3.0.4.b risk assessments do not have to be documented.

The ACLCOs allow continued operation with equipment unavailable in MODE 1 for the duration of the Completion Time. Since this is allowable, and since in general the risk impact in that particular MODE bounds the risk of transitioning into and through the applicable MODES or other specified conditions in the Applicability of the ACLCO, the use of the ACLCO 3.0.4.b allowance should be generally acceptable, as long as the risk is assessed and managed as stated above.

ACLCO 3.0.4.c allows entry into a MODE or other specified condition in the Applicability with the ACLCO not met based on a Note in the Control which states ACLCO 3.0.4.c is applicable. These specific allowances permit entry into MODES or other specified conditions in the Applicability when the associated ACTIONS to be entered do not provide for continued operation for an unlimited period of time and a risk assessment has not been performed. This allowance may apply to all the ACTIONS or to a specific Required Action of a Control. The risk assessments performed to justify the use of ACLCO 3.0.4.b usually only consider systems and components. For this reason, ACLCO 3.0.4.c is typically applied to Controls which describe values and parameters.

The provisions of this Control should not be interpreted as endorsing the failure to exercise the good practice of restoring systems or components to AVAILABLE status before entering an associated MODE or other specified condition in the Applicability.

BASES

ACLCO 3.0.5

ACLCO 3.0.5 establishes the allowance for restoring equipment to service under administrative controls when it has been removed from service or declared unavailable to comply with ACTIONS. The sole purpose of this Control is to provide an exception to ACLCO 3.0.2 (e.g., to not comply with the applicable Required Action(s)) to allow the performance of required testing to demonstrate:

a. The AVAILABILITY of the equipment being returned to service; or

b. The AVAILABILITY of other equipment.

The administrative controls ensure the time the equipment is returned to service in conflict with the requirements of the ACTIONS is limited to the time absolutely necessary to perform the required testing to demonstrate AVAILABILITY. This Control does not provide time to perform any other preventive or corrective maintenance.

ACLCO 3.0.6

ACLCO 3.0.6 establishes an exception to ACLCO 3.0.2 for supported systems that have a support system ACLCO specified in the ACM. This exception is provided because ACLCO 3.0.2 would require that the Conditions and Required Actions of the associated unavailable supported system ACLCO be entered solely due to the unavailability of the support system. This exception is justified because the actions that are required to ensure the plant risk is appropriately controlled are specified in the support system ACLCO Required Actions. These Required Actions may include entering the supported system Conditions and Required Actions or may specify other Required Actions.

When a support system is unavailable and there is an ACLCO specified for it in the ACM, the supported system(s) are required to be declared unavailable if determined to be unavailable as a result of the support system unavailability. However, it is not necessary to enter into the supported system Conditions and Required Actions unless directed to do so by the support system Required Actions. The potential confusion and inconsistency of requirements related to the entry into multiple support and supported system ACLCO Conditions and Required Actions are eliminated by providing all the actions that are necessary to ensure the plant is maintained in a safe condition in the support system Required Actions.

BASES

ACLCO 3.0.6 (continued)

However, there are instances where a support system Required Action may either direct a supported system to be declared unavailable or direct entry into Conditions and Required Actions for the supported system. This may occur immediately or after some specified delay to perform some other Required Action. Regardless of whether it is immediate or after some delay, when a support system Required Action directs a supported system to be declared unavailable or directs entry into Conditions and Required Actions for a supported system, the applicable Conditions and Required Actions shall be entered in accordance with ACLCO 3.0.2.

The Maintenance Rule Program ensures unacceptable risk is detected and appropriate actions are taken. Upon entry into ACLCO 3.0.6, an evaluation shall be made to determine if unacceptable risk exists. Additionally, other limitations, remedial actions, or compensatory actions may be identified as a result of the support system unavailability and corresponding exception to entering supported system Conditions and Required Actions. The Maintenance Rule Program implements the requirements of ACLCO 3.0.6.

ACM 3.0 AVAILABILITY CONTROLS SURVEILLANCE REQUIREMENT (ACSR) APPLICABILITY

BASES

ACSRs

ACSR 3.0.1 through ACSR 3.0.4 establish the general requirements applicable to all ACSRs in Sections 3.1 through 3.10 and apply at all times, unless otherwise stated.

ACSR 3.0.1

ACSR 3.0.1 establishes the requirement that ACSRs must be met during the MODES or other specified conditions in the Applicability for which the requirements of the ACLCOs apply, unless otherwise specified in the individual ACSRs. This ACSR is to ensure that ACSRs are performed to verify the AVAILABILITY of systems and components, and that variables are within specified limits. Failure to meet an ACSR within the specified Frequency, in accordance with ACSR 3.0.2, constitutes a failure to meet an ACLCO.

Systems and components are assumed to be AVAILABLE when the associated ACSRs have been met. Nothing in this ACSR, however, is to be construed as implying that systems or components are AVAILABLE when:

a. The systems or components are known to be unavailable, although still meeting the ACSRs; or

b. The requirements of the ACSRs are known to be not met between required ACSR performances.

ACSRs do not have to be performed when the unit is in a MODE or other specified condition for which the requirements of the associated ACLCO are not applicable, unless otherwise specified.

Unplanned events may satisfy the requirements (including applicable acceptance criteria) for a given ACSR. In this case, the unplanned event may be credited as fulfilling the performance of the ACSR. ACSRs, including ACSRs invoked by Required Actions, do not have to be performed on unavailable equipment because the ACTIONS define the remedial measures that apply. ACSRs have to be met and performed in accordance with ACSR 3.0.2, prior to returning equipment to AVAILABLE status.

BASES

ACSR 3.0.1 (continued)

Upon completion of maintenance, appropriate post-maintenance testing is required to declare equipment AVAILABLE. This includes ensuring applicable ACSRs are not failed and their most recent performance is in accordance with ACSR 3.0.2. Post-maintenance testing may not be possible in the current MODE or other specified conditions in the Applicability due to the necessary unit parameters not having been established. In these situations, the equipment may be considered AVAILABLE provided testing has been satisfactorily completed to the extent possible and the equipment is not otherwise believed to be incapable of performing its function. This will allow operation to proceed to a MODE or other specified condition where other necessary post-maintenance testing can be completed.

ACSR 3.0.2

ACSR 3.0.2 establishes the requirements for meeting the specified Frequency for ACSRs and any Required Action with a Completion Time that requires the periodic performance of the Required Action on a “once per . . .” interval.

ACSR 3.0.2 permits a 25% extension of the interval specified in the Frequency. This extension facilitates ACSR scheduling and considers plant operating conditions that may not be suitable for conducting the ACSR (e.g., transient conditions or other ongoing ACSR or maintenance activities).

The 25% extension does not significantly degrade the reliability that results from performing the ACSR at its specified Frequency. This is based on the recognition that the most probable result of any particular ACSR being performed is the verification of conformance with the ACSR. The exception to ACSR 3.0.2 are those ACSRs for which the 25% extension of the interval specified in the Frequency does not apply. These exceptions are stated in the individual ACSRs. The requirements of regulations take precedence over the ACM. The ACM cannot in and of itself extend a test interval specified in the regulations.

As stated in ACSR 3.0.2, the 25% extension also does not apply to the initial portion of a periodic Completion Time that requires performance on a "once per . . ." basis. The 25% extension applies to each performance after the initial performance. The initial performance of the Required Action, whether it is a particular ACSR or some other remedial action, is considered a single action with a single Completion Time. One reason for

BASES

ACSR 3.0.2 (continued)

not allowing the 25% extension to this Completion Time is that such an action usually verifies that no loss of function has occurred by checking the status of redundant or diverse components or accomplishes the function of the unavailable equipment in an alternative manner.

The provisions of ACSR 3.0.2 are not intended to be used repeatedly merely as an operational convenience to extend ACSR intervals (other than those consistent with refueling intervals) or periodic Completion Time intervals beyond those specified.

ACSR 3.0.3

ACSR 3.0.3 establishes the flexibility to defer declaring affected equipment unavailable or an affected variable outside the specified limits when an ACSR has not been completed within the specified Frequency. A delay period of up to 24 hours or up to the limit of the specified Frequency, whichever is greater, applies from the point in time it is discovered that the ACSR has not been performed in accordance with ACSR 3.0.2, and not at the time that the specified frequency was not met.

This delay period provides adequate time to complete ACSRs that have been missed. This delay period permits the completion of an ACSR before complying with Required Actions or other remedial measures that might preclude completion of the ACSR.

The basis for this delay period includes consideration of unit conditions, adequate planning, availability of personnel, the time required to perform the ACSR, the safety significance of the delay in completing the required ACSR, and the recognition that the most probable result of any particular ACSR being performed is the verification of conformance with the requirements. When an ACSR with a Frequency based not on time intervals, but upon specified unit conditions or operational situations (e.g., prior to entering MODE 1 after each fueling loading), is discovered not to have been performed when specified, ACSR 3.0.3 allows the full delay period of up to the specified frequency to perform the ACSR. However, since there is not a time interval specified, the missed ACSR should be performed at the first reasonable opportunity.

ACSR 3.0.3 provides a time limit for, and allowances for, the performance of ACSRs that become applicable as a consequence of MODE changes imposed by Required Actions.

BASES

ACSR 3.0.3 (continued)

Failure to comply with specified Frequencies for ACSRs is expected to be an infrequent occurrence. Use of the delay period established by ACSR 3.0.3 is a flexibility which is not intended to be used as an operational convenience to extend ACSR intervals. While up to 24 hours or the limit of the specified Frequency is provided to perform the missed ACSR, it is expected that the missed ACSR will be performed at the first reasonable opportunity. The determination of the first reasonable opportunity should include consideration of the impact on unit risk (from delaying the ACSR as well as any unit configuration changes required or shutting the unit down to perform the ACSR) and impact on any analysis assumptions, in addition to unit conditions, planning, availability of personnel, and the time required to perform the ACSR. This risk impact should be managed through the program in place to implement 10 CFR 50.65(a)(4) and its implementation guidance Regulatory Guide 1.182, "Assessing and Managing Risk Before Maintenance Activities at Nuclear Power Plants." This Regulatory Guide addresses consideration of temporary and aggregate risk impacts, determination of risk management action thresholds, and risk management action up to and including plant shutdown. The missed ACSR should be treated as an emergent condition as discussed in the Regulatory Guide. The risk evaluation may use quantitative, qualitative, or blended methods. The degree of depth and rigor of the evaluation should be commensurate with the importance of the component. Missed ACSRs for important components should be analyzed quantitatively. If the results of the risk evaluation determine the risk increase is significant this evaluation should be used to determine the safest course of action. All missed ACSRs will be placed in the COL Holder Corrective Action Program.

If an ACSR is not completed within the allowed delay period, the equipment is considered unavailable or the variable is considered outside the specified limits, and the Completion Times of the Required Actions for the applicable ACLCO Conditions begin immediately upon expiration of the delay period. If an ACSR is failed within the delay period, then the equipment is unavailable, or the variable is outside the specified limits, and the Completion Times of the Required Actions for the applicable ACLCO Conditions begin immediately upon the failure of the ACSR.

Completion of the ACSR within the delay period allowed by this ACSR, or within the Completion Time of the ACTIONS, restores compliance with ACSR 3.0.1.

BASES

ACSR 3.0.4

ACSR 3.0.4 establishes the requirement that all applicable ACSRs must be met before entry into a MODE or other specified condition in the Applicability.

This ACSR ensures that system and component AVAILABILITY requirements and variable limits are met before entry into MODES or other specified conditions in the Applicability for which these system and components ensure safe operation of the unit. The provisions of this ACSR should not be interpreted as endorsing the failure to exercise the good practice of restoring systems or components to AVAILABLE status before entering an associated MODE or other specified condition in the Applicability.

A provision is included to allow entry into a MODE or other specified Condition in the Applicability when an ACLCO is not met due to an ACSR not being met in accordance with ACLCO 3.0.4. However, in certain circumstances, failing to meet an ACSR will not result in ACSR 3.0.4 restricting a MODE change or other specified condition change. When a system, subsystem, division, component, device, or variable is unavailable or outside its specified limits, the associated ACSRs are not required to be performed, per ACSR 3.0.1, which states that ACSRs do not have to be performed on unavailable equipment. When equipment is unavailable, ACSR 3.0.4 does not apply to the associated ACSRs since the requirement for the ACSRs to be performed is removed. Therefore, failing to perform the ACSRs within the specified Frequency does not result in an ACSR 3.0.4 restriction to changing MODES or other specified conditions of the Applicability. However, since the ACLCO is not met in this instance, ACLCO 3.0.4 will govern any restrictions that may (or may not) apply to MODE or other specified condition changes. ACSR 3.0.4 does not restrict changing MODES or other specified conditions of the Applicability when an ACSR has not been performed within the specified Frequency, provided the requirement to declare the ACLCO not met has been delayed in accordance with ACSR 3.0.3.

The provisions of ACSR 3.0.4 shall not prevent changes in MODES or other specified conditions in the Applicability that are required to comply with ACTIONS. In addition, the provisions of ACSR 3.0.4 shall not prevent changes in MODES or other specified conditions in the Applicability that result from any unit shutdown. In this context, a unit shutdown is defined as a change in MODE or other specified condition in the Applicability associated with transitioning from MODE 1 to MODE 2, MODE 2 to MODE 3, and MODE 3 to MODE 4.

BASES

ACSR 3.0.4 (continued)

The precise requirements for performance of ACSRs are specified such that exceptions to ACSR 3.0.4 are not necessary. The specific time frames and conditions necessary for meeting the ACSRs are specified in the Frequency, in the ACSR, or both. This allows performance of ACSRs when the prerequisite conditions specified in an ACSR procedure require entry into the MODE or other specified condition in the Applicability of the associated ACLCO prior to the performance or completion of an ACSR. An ACSR that could not be performed until after entering the ACLCO Applicability would have its Frequency specified such that it is not "due" until the specific conditions needed are met.

Alternately, the ACSR may be stated in the form of a Note as not required (to be met or performed) until a particular event, condition, or time has been reached. Further discussion of the specific formats of ACSR annotation is found in Section 1.4, "Frequency."

ACM 3.3 INSTRUMENTATION

AC 3.3.1 Alternate Rod Insertion (ARI)

ACLCO 3.3.1 The function of the ARI valves in the Control Rod Drive (CRD) System shall be AVAILABLE.

APPLICABILITY: MODES 1 and 2.

ACTIONS

CONDITION	REQUIRED ACTION	COMPLETION TIME
A. The function of one or more CRD System ARI valves unavailable.	A.1 Restore CRD System ARI valves to AVAILABLE status.	7 days
B. Required Action and associated Completion Time not met.	B.1 Enter ACLCO 3.0.3.	Immediately

SURVEILLANCE REQUIREMENTS

SURVEILLANCE		FREQUENCY
ACSR 3.3.1.1	---------- **- NOTE -** Only required to be met in MODE 1. ---------- MODE 2 Surveillance Requirements of Technical Specification (TS) 3.3.1.4, "Neutron Monitoring System (NMS) Instrumentation," Table 3.3.1.4-1, for Functions 1.a and 1.b are applicable.	In accordance with applicable SRs

SURVEILLANCE		FREQUENCY
ACSR 3.3.1.2	Verify each CRD System ARI valve vents on receipt of an actual or simulated actuation signal.	24 months on a STAGGERED TEST BASIS for each solenoid
ACSR 3.3.1.3	Perform LOGIC SYSTEM FUNCTIONAL TEST.	24 months

ACM B 3.3 INSTRUMENTATION

AC B 3.3.1 Alternate Rod Insertion (ARI)

BASES

This availability control addresses AVAILABILITY of the Alternate Rod Insertion (ARI) function of the ARI valves in the Control Rod Drive (CRD) system. The ARI function of the Control Rod Drive (CRD) system provides an alternate means for actuating hydraulic scram that is diverse and independent from the Reactor Protection System (RPS). The ARI function of the Anticipated Transient Without Scram (ATWS) mitigation logic is implemented as nonsafety-related logic that is processed by the Diverse Protection System (DPS) (reference DCD Tier 2, Subsection 7.8.1.1.2). The DPS generates the signal to open the ARI valves in the CRD system on any of the following: persistent high power with a Selected Control Rod Run-in (SCRRI) command issued; persistent high power following an RPS scram demand; high reactor dome pressure; low reactor vessel water Level 2; or manual operator action. Following receipt of any of these signals, solenoid operated valves on the scram air header actuate to depressurize the header, allowing the Hydraulic Control Unit (HCU) scram valves to open. The control rod drives then insert the control rods hydraulically.

The ARI function is a nonsafety-related function that satisfies the significance criteria for Regulatory Treatment of Non-Safety Systems, and therefore requires regulatory oversight. The short-term availability controls for this function, which are specified as Completion Times, are acceptable to ensure that the availability of this function is consistent with the functional unavailability in the ESBWR PRA. The surveillance requirements also provide an adequate level of support to ensure that component performance is consistent with the functional reliability in the ESBWR PRA.

ACM 3.3 INSTRUMENTATION

AC 3.3.2 Anticipated Transient Without Scram (ATWS) / Standby Liquid Control (SLC) System Actuation

ACLCO 3.3.2 The ATWS/SLC Functions in Table 3.3.2-1 shall be AVAILABLE.

APPLICABILITY: MODES 1 and 2.

ACTIONS

CONDITION	REQUIRED ACTION	COMPLETION TIME
A. One or more ATWS/SLC Functions unavailable.	A.1 Restore ATWS/SLC Function(s) to AVAILABLE status.	7 days
B. Required Action and associated Completion Time not met.	B.1 Enter ACLCO 3.0.3.	Immediately

SURVEILLANCE REQUIREMENTS

SURVEILLANCE		FREQUENCY
ACSR 3.3.2.1	Verify SLC actuation on receipt of an actual or simulated actuation signal.	24 months
ACSR 3.3.2.2	Verify Reactor Water Cleanup / Shutdown Cooling (RWCU/SDC) isolation on receipt of an actual or simulated actuation signal.	24 months

SURVEILLANCE		FREQUENCY
ACSR 3.3.2.3	Verify ADS Inhibit function actuation on receipt of an actual or simulated actuation signal.	24 months
ACSR 3.3.2.4	Perform LOGIC SYSTEM FUNCTIONAL TEST.	24 months

Table 3.3.2-1
Anticipated Transient Without Scram / Standby Liquid Control System

FUNCTION
1. SLC Actuation
2. RWCU/SDC Isolation
3. ADS Inhibit

ACM B 3.3 INSTRUMENTATION

AC B 3.3.2 Anticipated Transient Without Scram (ATWS) / Standby Liquid Control (SLC) System Actuation

BASES

The Standby Liquid Control (SLC) System provides a diverse backup capability for reactor shutdown, independent of normal reactor shutdown with control rods. It also provides makeup water to the reactor pressure vessel (RPV) to mitigate the consequences of a LOCA. Operability of the SLC System, including the squib-actuated valves, is addressed in Technical Specification (TS) 3.1.7, "Standby Liquid Control (SLC) System." For Anticipated Transient Without Scram (ATWS) mitigation, the Safety System Logic and Control Engineered Safety Feature (SSLC/ESF) initiation of the Automatic Depressurization System (ADS) is inhibited automatically. The ADS Inhibit function supports proper operation of the SLC System for diverse backup reactor shutdown. This availability control addresses only the actuation logic associated with the ATWS/SLC actuation of SLC for diverse backup reactor shutdown (reference DCD Tier 2 Subsection 7.8.1.1.1), isolation of Reactor Water Clean-Up / Shutdown Cooling (RWCU/SDC) on ATWS/SLC initiation (reference DCD Tier 2 Subsection 7.4.1.2), and the actuation logic associated with the ATWS/SLC ADS inhibit function (reference DCD Tier 2 Subsection 7.8.1.1.1.2).

There are ATWS mitigation logic processors in each of four divisional Reactor Trip and Isolation Function (RTIF) cabinets. The ATWS mitigation logic processors are separate and diverse from RPS circuitry. Each ATWS mitigation logic processor uses discrete programmable logic devices for ATWS mitigation logic processing. The programmable logic devices provide voting logic, control logic, and time delays for evaluating the plant conditions for automatic initiation of SLC boron injection. Although there are four divisions of the ATWS/SLC platform for each Function, only two divisions are required for a Function to be considered AVAILABLE. The two required divisions are those divisions associated with the DC and Uninterruptible AC Electrical Power Distribution Divisions required by LCO 3.8.6, "Distribution Systems – Operating," and LCO 3.8.7, "Distribution Systems – Shutdown."

Automatic initiation of the ATWS/SLC occurs on High RPV dome pressure and a Startup Range Neutron Monitor (SRNM) ATWS permissive, or Low RPV water level (L2) and a SRNM ATWS permissive for 3 minutes or greater. To avoid reducing boron concentration during SLC operation, the ATWS/SLC system logic also transmits an isolation signal to the RWCU/SDC via the Leak Detection and Isolation System (LD&IS).

ADS Inhibit required by this availability control is automatically initiated by the following signals:

- A coincident low RPV water level (Level 2) signal and Average Power Range Monitor (APRM) ATWS permissive signal (i.e., an APRM signal that is above a specified setpoint from the NMS).

BASES

- A coincident high RPV pressure and APRM ATWS permissive signal that persists for 60 seconds.

MCR switches manually inhibit the ADS under ATWS conditions.

The short-term availability controls for this function, which are specified as Completion Times, are acceptable to ensure that the availability of this function is consistent with the functional unavailability in the ESBWR PRA. The surveillance requirements also provide an adequate level of support to ensure that component performance is consistent with the functional reliability in the PRA.

ACM 3.3 INSTRUMENTATION

AC 3.3.3 Feedwater Runback (FWRB)

ACLCO 3.3.3 The feedwater runback function shall be AVAILABLE.

APPLICABILITY: MODE 1

ACTIONS

CONDITION	REQUIRED ACTION	COMPLETION TIME
A. Feedwater runback function unavailable.	A.1 Restore feedwater runback function to AVAILABLE status.	7 days
B. Required Action and associated Completion Time not met.	B.1 Enter ACLCO 3.0.3.	Immediately

SURVEILLANCE REQUIREMENTS

SURVEILLANCE		FREQUENCY
ACSR 3.3.3.1	Verify feedwater runback function actuation on receipt of an actual or simulated actuation signal.	24 months
ACSR 3.3.3.2	Perform LOGIC SYSTEM FUNCTIONAL TEST.	24 months

ACM B 3.3 INSTRUMENTATION

AC B 3.3.3 Feedwater Runback (FWRB)

BASES

The feedwater runback logic provides a quick power reduction in response to Anticipated Transient Without Scram (ATWS) conditions. This availability control addresses the Diverse Protection System (DPS) logic and Feedwater Control System (FWCS) components associated with the feedwater runback function.

The feedwater runback function of the ATWS mitigation logic is implemented as nonsafety-related logic that is processed by the DPS (reference DCD Tier 2 Subsections 7.8.1.1.1.1 and 7.8.1.2). The DPS generates an actuation signal on any of the following: persistent high power with a Selected Control Rod Run-In / Select Rod Insert (SCRRI/SRI) command issued, persistent high power following an RPS scram demand, or an ATWS/SLC actuation signal. The FWCS initiates a runback of feedwater pump feedwater demand to zero and closes the Low Flow Control Valve (LFCV) and Reactor Water Cleanup/Shutdown Cooling (RWCU/SDC) overboard flow control valve when it receives a valid actuation signal.

The ATWS/SLC logic also provides actuation of the Standby Liquid Control (SLC) System for diverse backup reactor shutdown. The ATWS/SLC function is addressed in AC 3.3.2, " Anticipated Transient Without Scram (ATWS)/Standby Liquid Control (SLC) System Actuation."

The feedwater runback function is a nonsafety-related function that satisfies the significance criteria for Regulatory Treatment of Non-Safety Systems, and therefore requires regulatory oversight. The short-term availability controls for this function, which are specified as Completion Times, are acceptable to ensure that the availability of this function is consistent with the functional unavailability in the PRA. The surveillance requirements also provide an adequate level of support to ensure that component performance is consistent with the functional reliability in the PRA.

ACM 3.3 INSTRUMENTATION

AC 3.3.4 Diverse Protection System (DPS)

ACLCO 3.3.4 The DPS Functions in Table 3.3.4-1 shall be AVAILABLE.

APPLICABILITY: MODES 1, 2, 3, and 4.

ACTIONS

CONDITION	REQUIRED ACTION	COMPLETION TIME
A. One or more DPS Functions unavailable.	A.1 Restore DPS Function(s) to AVAILABLE Status.	30 days
B. Required Action and associated Completion Time not met.	B.1 Enter ACLCO 3.0.3.	Immediately

SURVEILLANCE REQUIREMENTS

SURVEILLANCE		FREQUENCY
ACSR 3.3.4.1	Perform CHANNEL CHECK.	12 hours
ACSR 3.3.4.2	Perform CHANNEL FUNCTIONAL TEST.	31 days
ACSR 3.3.4.3	Perform CHANNEL CALIBRATION.	24 months
ACSR 3.3.4.4	Perform LOGIC SYSTEM FUNCTIONAL TEST.	24 months

DPS
AC 3.3.4

Table 3.3.4-1 (page 1 of 1)
Diverse Protection System

FUNCTION
1. Reactor Scram
2. Main Steam Isolation Valve Closure
3. Safety Relief Valve Actuation
4. Fine Motor Control Rod Drive Run-in Actuation
5. Isolation Condenser System Actuation
6. Isolation Condenser System Vent Actuation
7. Standby Liquid Control System Actuation (for Loss-of-Coolant Accident)
8. Automatic Depressurization System (ADS) Inhibit

ACM B 3.3 INSTRUMENTATION

AC B 3.3.4 Diverse Protection System (DPS)

BASES

DPS provides diverse actuation functions that enhance the plant's ability to mitigate dominant accident sequences involving the common cause failure of actuation logic or controls. The DPS Functions are implemented in a highly reliable triple redundant control system whose sensors, hardware, and software are diverse from their counterparts on any of the safety-related platforms.

The following diverse actuation Functions are provided by DPS:

- A set of protection logics that provide a diverse means to scram the reactor via control rod insertion (reference Subsection 7.8.1.2.1),
- A set of initiation logics that provide a diverse means to initiate certain engineered safety features (ESF) functions (safety relief valves, Isolation Condenser System, and Standby Liquid Control System (reference Subsection 7.8.1.2.2)),
- A set of initiation logics that provide a diverse means to initiate closure of the main steam isolation valves (reference Subsection 7.8.1.2.4),
- A set of initiation logics that provide a diverse means of control rod insertion by means of Fine Motor Control Rod Drive Run-in (reference Subsection 7.8.1.1.2), and
- A set of initiation logics that provide a diverse means of initiating venting of the Isolation Condenser System in order to mitigate the accumulation of radiolytic hydrogen and oxygen (reference Subsection 7.8.1.2.5).

For Anticipated Transient Without Scram (ATWS) mitigation, the DPS initiation of ADS is inhibited automatically. The ADS Inhibit Function required by this availability control is automatically actuated by nonsafety-related logic that is processed by the DPS (reference Subsection 7.8.1.2.3). The ADS Inhibit Function prevents an undesirable DPS initiation of the ADS during ATWS conditions.

The DPS Functions are nonsafety-related functions that satisfy the significance criteria for Regulatory Treatment of Non-Safety Systems, and therefore require regulatory oversight. The short-term availability controls for these Functions, which are specified as Completion Times, are acceptable to ensure that the availability of these Functions is consistent with the functional unavailability in the ESBWR PRA. The surveillance requirements also provide an adequate level of support to ensure that component performance is consistent with the functional reliability in the ESBWR PRA.

ACM 3.5 EMERGENCY CORE COOLING SYSTEM (ECCS)

AC 3.5.1 Gravity-Driven Cooling System (GDCS) Deluge Function

ACLCO 3.5.1 Six deluge valves shall be AVAILABLE.

APPLICABILITY: MODES 1, 2, 3, and 4.

ACTIONS

CONDITION	REQUIRED ACTION	COMPLETION TIME
A. Required deluge valves unavailable.	A.1 Restore required deluge valves to AVAILABLE Status.	7 days
B. Required Action and associated Completion Time not met.	B.1 Enter ACLCO 3.0.3.	Immediately

SURVEILLANCE REQUIREMENTS

SURVEILLANCE		FREQUENCY
ACSR 3.5.1.1	Perform CHANNEL CHECK on GDCS deluge associated drywell atmosphere thermocouples and lower drywell basemat thermocouples.	12 hours
ACSR 3.5.1.2	---------- **- NOTE -** Not required to be met for one squib firing circuit intermittently bypassed under administrative controls. ---------- Verify continuity of required firing circuits in squib-actuated valves.	31 days

SURVEILLANCE		FREQUENCY
ACSR 3.5.1.3	Perform CHANNEL CALIBRATION on GDCS deluge associated drywell atmosphere thermocouples and lower drywell basemat thermocouples.	24 months
ACSR 3.5.1.4	--- **- NOTE -** Squib actuation may be excluded. --- Verify required deluge valves actuate on an actual or simulated automatic initiation signal.	24 months
ACSR 3.5.1.5	Perform LOGIC SYSTEM FUNCTIONAL TEST.	24 months
ACSR 3.5.1.6	--- **- NOTE -** Squib actuation may be excluded. --- Verify the flow path for each deluge line is not obstructed.	24 months on a STAGGERED TEST BASIS for each deluge line

ACM B 3.5 EMERGENCY CORE COOLING SYSTEM (ECCS)

AC B 3.5.1 Gravity-Driven Cooling System (GDCS) Deluge Function

BASES

The deluge function provides a means of flooding the lower drywell region and the Basemat Internal Melt Arrest and Coolability (BiMAC) device with GDCS pool water in the event of a core melt sequence which causes failure of the lower vessel head and allows molten fuel to reach the lower drywell floor. Deluge line flow is initiated by thermocouples, which sense high lower drywell region basemat temperatures indicative of molten fuel on the lower drywell floor. Logic circuits actuate squib-type valves in the deluge lines upon detection of basemat temperatures exceeding setpoint values, provided another set of dedicated thermocouples also sense the drywell temperature to be higher than a preset value. The pyrotechnic material of the squib charge used in the deluge valve is different than what is used in the other GDCS squib valves to prevent common mode failure.

Only six of the deluge valves, and their associated instrumentation sensors and actuation logics, are required to be AVAILABLE to remove decay heat energy and the energy from zirconium-water reaction and allow for quenching of core debris. Three GDCS pools, located above the wetwell, at an elevation above the reactor core, contain the water that supports all four GDCS trains for the injection and deluge subsystems and is assured by Technical Specification LCO 3.5.2, "GDCS – Operating." Only two of these GDCS pools are required to support the availability of the six required deluge valves.

The deluge function is a nonsafety-related function that satisfies the significance criteria for Regulatory Treatment of Non-Safety Systems, and therefore requires regulatory oversight. The short-term availability controls for this function, which are specified as Completion Times, are acceptable to ensure that the availability of this function is consistent with the functional unavailability in the ESBWR PRA. The surveillance requirements also provide an adequate level of support to ensure that component performance is consistent with the functional reliability in the ESBWR PRA. The STAGGERED TEST BASIS for each deluge line requires verification of the flow path through each of the four deluge lines and its associated three tailpipes to be alternated every 24 months so that the deluge flow path for each GDCS train is verified every 96 months.

ACM 3.6 CONTAINMENT SYSTEMS

AC 3.6.1 Lower Drywell Hatches

ACLCO 3.6.1 The lower drywell personnel air lock and lower drywell equipment hatch shall be AVAILABLE for closure.

APPLICABILITY: MODES 5 and 6.

ACTIONS

CONDITION	REQUIRED ACTION	COMPLETION TIME
A. Required Drywell equipment hatch not AVAILABLE for closure.	A.1 Initiate action to suspend OPDRVs.	Immediately
	AND	
	A.2 Enter ACLCO 3.0.3.	Immediately

SURVEILLANCE REQUIREMENTS

SURVEILLANCE		FREQUENCY
ACSR 3.6.1.1	Verify lower drywell hatch administrative closure plan is in place.	12 hours
ACSR 3.6.1.2	Verify lower drywell equipment hatch can be secured closed.	30 days
ACSR 3.6.1.3	Verify lower drywell personnel airlock can be secured closed.	30 days

ACM B 3.6 CONTAINMENT SYSTEMS

AC B 3.6.1 Lower Drywell Hatches

BASES

An equipment hatch for removal of equipment during maintenance and an air lock for entry of personnel are provided in the lower drywell. These access openings are sealed under normal plant operation but may be opened when the plant is shut down. Closure of both hatches is required for the shutdown Loss-of-Coolant Accident (LOCA) below top of active fuel (TAF) initiators during MODES 5 and 6. These LOCAs involve breaks in the RWCU/SDC drain lines or instrument lines or CRD housing/maintenance activities. Once the event has been detected, personnel must correctly diagnose the situation, make the decision to close the hatches, and manually close the equipment hatch and the personnel air lock. Administrative controls assure trained personnel will be continuously located in the area of the doors and appropriate administrative controls are in place to communicate awareness of potential breaches and effect decisions to secure the hatches.

The lower drywell hatch closure function is a nonsafety-related function that satisfies the significance criteria for Regulatory Treatment of Non-Safety Systems, and therefore requires regulatory oversight. The short-term availability controls for this function, which are specified as Completion Times, are acceptable to ensure that the availability of this function is consistent with the functional unavailability in the ESBWR PRA. The surveillance requirements also provide an adequate level of support to ensure that component performance is consistent with the functional reliability in the ESBWR PRA.

ACM 3.6 CONTAINMENT SYSTEMS

AC 3.6.2 Passive Autocatalytic Recombiners (PARs)

ACLCO 3.6.2 PARs in the drywell compartment and PARs in the wetwell compartment shall be AVAILABLE.

APPLICABILITY: MODES 1, 2, 3, and 4.

ACTIONS

CONDITION	REQUIRED ACTION	COMPLETION TIME
A. One PAR in one or both compartments unavailable.	A.1 Restore PAR(s) to AVAILABLE status.	Prior to entering MODE 2 or MODE 4 from MODE 5
B. Two or more PARs in one or both compartments unavailable. OR Required Action and associated Completion Time of Condition A not met.	B.1 Enter ACLCO 3.0.3.	Immediately

SURVEILLANCE REQUIREMENTS

SURVEILLANCE		FREQUENCY
ACSR 3.6.2.1	Visually examine each PAR and verify there is no evidence of abnormal conditions.	24 months

SURVEILLANCE		FREQUENCY
ACSR 3.6.2.2	Verify performance of a representative sample of PAR catalyst plates.	24 months on a STAGGERED TEST BASIS for each compartment

ACM B 3.6 CONTAINMENT SYSTEMS

AC B 3.6.2 Passive Autocatalytic Recombiners (PARs)

BASES

The PARs function to reduce the hydrogen concentration in the containment by recombining radiolytic hydrogen and oxygen into water. The recombiners are of a catalytic type with replaceable catalyst.

The PARs function is a nonsafety-related function that provides defense-in-depth in to containment inerting by reducing hydrogen concentration produced during accident sequences, and therefore regulatory oversight is provided. The short-term availability controls for this function, which are specified as Completion Times, are acceptable to ensure that the availability of this function is consistent with the functional unavailability in the ESBWR PRA. The surveillance requirements also provide an adequate level of testing to ensure that component performance is consistent with the functional reliability in the ESBWR PRA. The STAGGERED TEST BASIS requires a representative sample of catalyst plates from one compartment be tested each 24 months, i.e., 24-month samples alternated between the drywell and wetwell PARs. The representative sample consists of one plate from each PAR in the compartment being tested.

ACM 3.6 CONTAINMENT SYSTEMS

AC 3.6.3 Passive Containment Cooling System (PCCS) Vent Fans

ACLCO 3.6.3 Five PCCS vent fans shall be AVAILABLE.

APPLICABILITY: MODES 1, 2, 3, and 4.

ACTIONS

CONDITION	REQUIRED ACTION	COMPLETION TIME
A. One required PCCS vent fan unavailable.	A.1 Restore required PCCS vent fan to AVAILABLE status.	Prior to entering MODE 2 or 4 from MODE 5
B. Two or more required PCCS vent fans unavailable.	B.1 Restore required PCCS vent fans to AVAILABLE status.	24 hours
C. Required Action and associated Completion Time not met.	C.1 Enter ACLCO 3.0.3.	Immediately

SURVEILLANCE REQUIREMENTS

SURVEILLANCE		FREQUENCY
ACSR 3.6.3.1	Operate each required PCCS vent fan ≥ 15 minutes.	92 days
ACSR 3.6.3.2	Verify required PCCS vent fan flow rate is greater than or equal to that assumed in long term containment heat removal analyses.	24 months on a STAGGERED TEST BASIS for each PCCS condenser

ACM B 3.6 CONTAINMENT SYSTEMS

AC B 3.6.3 Passive Containment Cooling System (PCCS) Vent Fans

BASES

A branch line from each of the 6 PCCS system vents in the drywell contains a fan isolation valve, a fan and discharge line that terminates in a submerged location in the GDCS pool. When in operation, the fan will actively circulate the drywell atmosphere (steam and non-condensables) through the PCCS condensers to enhance the rate of heat removal.

The PCCS vent fan function is a nonsafety-related function that provides the ability to reduce drywell pressure and temperature after 72 hours following a DBA by forced containment cooling through the PCCS system condensers. Satisfactory results are obtained by successful operation of four out of the six fans; therefore, the ACLCO requires the AVAILABILITY of five fans. PCCS vent fans provide post 72-hour reduction in containment pressure by redistributing noncondensable gases from the wetwell to the drywell; therefore, regulatory oversight is provided. The short-term availability controls for this function, which are specified as Completion Times, are acceptable to ensure that the availability of this function is consistent with the functional unavailability in the ESBWR PRA. The surveillance requirements also provide an adequate level of support to ensure that component performance is consistent with the functional reliability in the ESBWR PRA.

ACM 3.6 CONTAINMENT SYSTEMS

AC 3.6.4 Hydrogen Mitigation – Ignitors

ACLCO 3.6.4 One ignitor per Passive Containment Cooling System (PCCS) lower drum shall be AVAILABLE.

APPLICABILITY: MODES 1, 2, 3, and 4.

ACTIONS

- NOTE -

Separate Condition entry is allowed for each PCCS lower drum.

CONDITION	REQUIRED ACTION	COMPLETION TIME
A. One or more required ignitors unavailable.	A.1 Restore ignitor to AVAILABLE Status.	7 days
B. Required Action and associated Completion Time not met.	B.1 Enter ACLCO 3.0.3.	Immediately

SURVEILLANCE REQUIREMENTS

SURVEILLANCE		FREQUENCY
ACSR 3.6.4.1	Perform CHANNEL CHECK on associated drywell atmosphere thermocouples and lower drywell basemat thermocouples.	12 hours
ACSR 3.6.4.2	Energize each ignitor and perform current versus voltage measurements to verify required ignitors in service.	92 days

SURVEILLANCE		FREQUENCY
ACSR 3.6.4.3	Perform CHANNEL CALIBRATION on associated drywell atmosphere thermocouples and lower drywell basemat thermocouples.	24 months
ACSR 3.6.4.4	Perform LOGIC SYSTEM FUNCTIONAL TEST.	24 months
ACSR 3.6.4.5	Verify each required ignitor starts on an actual or simulated automatic initiation signal and operates at the required temperature.	24 months on a STAGGERED TEST BASIS for each PCCS Condenser

ACM B 3.6 CONTAINMENT

AC B 3.6.4 Hydrogen Mitigation - Ignitors

BASES

During the initial stages of a severe accident, there is essentially no water in the vicinity of the core, so radiolysis is greatly reduced. However, large quantities of hydrogen are released into the drywell due to metal-water reactions. The high abundance of hydrogen relative to oxygen effectively reduces the potential for detonation in the Passive Containment Cooling System (PCCS). Later in the postulated event, after the core melts through the vessel and interacts with the concrete, the GDCS deluge valves open and the core once again has the potential to resume radiolysis. Thereafter, relative concentrations of hydrogen and oxygen trend closer to a stoichiometric ratio at pressures much higher than during a Design Basis Accident. The PCCS condensers may experience some plastic deformation during a detonation under these conditions.

Ignitors in the lower drums of the PCCS condensers recombine the hydrogen and oxygen while they are still at lower concentrations, thus preventing a detonation that could result from the accumulation of high concentrations of these gases. Each PCCS condenser module has two lower drums, and each lower drum contains 2 ignitors. One ignitor per lower drum is required to be available to effectively recombine the hydrogen and oxygen to safe levels. The ignitors are actuated by the same drywell temperature signals and control system that actuate the GDCS Deluge Function (ACLCO 3.5.1).

The ignitor function is a nonsafety-related function that satisfies the significance criteria for Regulatory Treatment of Non-Safety Systems, and therefore requires regulatory oversight. The short-term availability controls for this function, which are specified as Completion Times, are acceptable to ensure that the availability of this function is consistent with the functional unavailability in the ESBWR PRA. The surveillance requirements also provide an adequate level of support to ensure that component performance is consistent with the functional reliability in the ESBWR PRA.

ACM 3.7 PLANT SYSTEMS

AC 3.7.1 Emergency Makeup Water

ACLCO 3.7.1 One diesel-driven firewater pump and one motor-driven firewater pump, supporting the emergency makeup water Functions listed in Table AC 3.7.1-1, shall be AVAILABLE.

APPLICABILITY: According to Table AC 3.7.1-1.

ACTIONS

CONDITION	REQUIRED ACTION	COMPLETION TIME
A. Required diesel-driven firewater pump unavailable. OR Required motor-driven firewater pump unavailable.	A.1 Restore required diesel-driven firewater pump to AVAILABLE status. AND A.2 Restore required motor-driven firewater pump to AVAILABLE status.	14 days 14 days
B. Firewater source total volume not within limit.	B.1 Restore firewater source total volume to within limit.	7 days
C. One or more emergency makeup water Function(s) unavailable.	C.1 ---------- **- NOTE -** Separate Condition entry is allowed for each emergency makeup water Function. ---------- Restore emergency makeup water Function(s) to AVAILABLE status.	 7 days

CONDITION	REQUIRED ACTION	COMPLETION TIME
D. Required Action and associated Completion Time not met.	D.1 Enter ACLCO 3.0.3.	Immediately

SURVEILLANCE REQUIREMENTS

SURVEILLANCE		FREQUENCY
ACSR 3.7.1.1	Verify firewater source total volume ≥ 3900 m^3 ($1.03x10^6$ gallons).	31 days
ACSR 3.7.1.2	Verify that each manual, power-operated, or automatic valve in the flow path that is not locked, sealed, or otherwise secured in its correct position is in the correct position or can be aligned to the correct position.	31 days
ACSR 3.7.1.3	Verify required diesel-driven firewater pump starts on a manual start signal and operates for ≥ 15 minutes.	92 days

Table AC 3.7.1-1 (page 1 of 1)
Emergency Makeup Water Sources

FUNCTION	APPLICABLE MODES OR OTHER SPECIFIED CONDITIONS
1. Isolation Condenser / Passive Containment Cooling System (IC/PCCS) Pools Makeup Water – Emergency Makeup	1,2,3,4
2. Spent Fuel Pool (SFP) – Emergency Makeup Water	When spent fuel assemblies are stored in the SFP

ACM B 3.7 PLANT SYSTEMS

AC B 3.7.1 Emergency Makeup Water

BASES

The Fire Protection Water Supply System can function in a backup capacity to provide additional water during the post-accident recovery period to provide makeup to the Isolation Condenser / Passive Containment Cooling System(IC/PCCS) pools to extend the safe shutdown state from 72 hours through 7 days. Post 72-hour inventory makeup is provided via safety-related connections to the Fire Protection System (FPS) and to offsite water sources.

During a loss of the Fuel and Auxiliary Pools Cooling System (FAPCS) cooling trains, the cooling to the Spent Fuel Pool (SFP) is accomplished by allowing the water to heat and boil off. Sufficient pool capacity exists for pool boiling to continue for at least 72 hours post-accident, at which point emergency makeup water can be provided through safety-related connections to the Fire Protection System.

In conjunction with the diesel-driven and motor-driven pump, the dedicated connections for FPS makeup include the Fire Pump Enclosure (FPE), the water supply, the suction pipe from the water supply to the pump, one of the supply pipes from the FPE to the Reactor Building, and the connections to the Fuel and Auxiliary Pools Cooling System (FAPCS). Water is pumped from the firewater storage tanks by the diesel-driven or motor-driven firewater pump in the FPE to the desired flow path. The two firewater storage tanks are required to contain a total volume of $\geq 3900\ m^3$ (1.03×10^6 gallons) of water to ensure a sufficient quantity of emergency makeup is available.

The maximum volume of water that would be required for makeup to the IC/PCCS pools and the SFP from 72 hours through 7 days is approximately $3900\ m^3$ (1.03×10^6 gallons) and the required delivery rate is approximately $46\ m^3/hr$ (200 gpm). The calculations performed to determine these values consider the maximum combined decay heat of the reactor at 102% rated power and the SFP. Design margin is then added to obtain a bounding combined decay heat of the RPV and SFP that is used to calculate a peak evaporation rate and total evaporation volume from the IC/PCCS pools and the SFP.

The emergency makeup water functions are nonsafety-related functions that satisfy the significance criteria for Regulatory Treatment of Non-Safety Systems, and therefore require regulatory oversight. The short-term availability controls for these functions, which are specified as Completion Times, are acceptable to ensure that the availability of these functions is consistent with the functional unavailability in the ESBWR PRA. The surveillance requirements also provide an adequate level of support to ensure that component performance is consistent with the functional reliability in the ESBWR PRA.

ACM 3.7 PLANT SYSTEMS

AC 3.7.2 Fuel and Auxiliary Pools Cooling System (FAPCS) - Operating

ACLCO 3.7.2 Two Fuel and Auxiliary Pools Cooling System (FAPCS) trains shall be AVAILABLE.

APPLICABILITY: MODES 1, 2, 3, and 4.

ACTIONS

CONDITION	REQUIRED ACTION	COMPLETION TIME
A. One FAPCS train unavailable.	A.1 Restore required FAPCS train to AVAILABLE status.	14 days
B. Two FAPCS trains unavailable.	B.1 Restore one FAPCS train to AVAILABLE status.	24 hours
C. Required Action and associated Completion Time not met.	C.1 Enter ACLCO 3.0.3.	Immediately

SURVEILLANCE REQUIREMENTS

SURVEILLANCE		FREQUENCY
ACSR 3.7.2.1	Verify that each manual, power-operated, or automatic valve in the flow path that is not locked, sealed, or otherwise secured in its correct position is in the correct position or can be aligned to the correct position.	31 days

ACM 3.7 PLANT SYSTEMS

AC 3.7.3 Fuel and Auxiliary Pools Cooling System (FAPCS) - Shutdown

ACLCO 3.7.3 Two Fuel and Auxiliary Pools Cooling System (FAPCS) trains shall be AVAILABLE.

APPLICABILITY: MODES 5 and 6.

ACTIONS

CONDITION	REQUIRED ACTION		COMPLETION TIME
A. One FAPCS train unavailable.	A.1	Restore FAPCS train to AVAILABLE status.	14 days
B. Two FAPCS trains unavailable.	B.1	Restore one FAPCS train to AVAILABLE status.	24 hours
C. Required Action and associated Completion Time not met.	C.1	Enter ACLCO 3.0.3.	Immediately
	AND		
	C.1	Initiate action to suspend operations with a potential for draining the reactor vessel (OPDRVs).	Immediately
	AND		
	C.2	Initiate action to restore Reactor Building to OPERABLE status.	Immediately

SURVEILLANCE REQUIREMENTS

SURVEILLANCE		FREQUENCY
ACSR 3.7.3.1	Verify that each manual, power-operated, or automatic valve in the flow path that is not locked, sealed, or otherwise secured in its correct position is in the correct position or can be aligned to the correct position.	31 days

ACM B 3.7 PLANT SYSTEMS

AC B 3.7.2 / B 3.7.3 Fuel and Auxiliary Pools Cooling System (FAPCS)

BASES

FAPCS is designed to provide the accident recovery functions of suppression pool cooling, low pressure coolant injection (LPCI) of suppression pool water into the reactor pressure vessel (RPV), and alternate shutdown cooling, in addition to its normal spent fuel cooling function. This availability control addresses the suppression pool cooling, LPCI, and alternate shutdown cooling functions of the FAPCS.

In the LPCI mode, the required FAPCS pump takes suction from the suppression pool and pumps it into the RPV via Reactor Water Cleanup/Shutdown Cooling (RWCU/SDC) loop A and then Feedwater loop B. In the suppression pool cooling mode, water is drawn from the suppression pool, cooled by the FAPCS, and returned to the suppression pool. The suppression pool cooling mode may be manually initiated following an accident.

In the alternate shutdown cooling mode, the FAPCS flow path is similar to that of the LPCI mode. Water is drawn from the suppression pool, cooled, and then discharged back to the RPV via the LPCI injection flow path. The warmer water in the RPV rises and then overflows into the suppression pool via two opened safety-relief valves on the main steam lines, completing a closed loop. The alternate shutdown cooling mode is manually initiated.

The FAPCS LPCI and suppression pool cooling functions are nonsafety-related functions that satisfy the significance criteria for Regulatory Treatment of Non-Safety Systems, and therefore require regulatory oversight. The short-term availability controls for these functions, which are specified as Completion Times, are acceptable to ensure that the availabilities of these functions are consistent with the functional unavailabilities in the ESBWR PRA. The surveillance requirements also provide an adequate level of support to ensure that component performance is consistent with the functional reliabilities in the ESBWR PRA.

ACM 3.7 PLANT SYSTEMS

AC 3.7.4 Reactor Building HVAC Accident Exhaust Filtration

ACLCO 3.7.4 Two Reactor Building Heating, Ventilation and Air Conditioning (HVAC) Accident Exhaust Filtration trains shall be AVAILABLE.

APPLICABILITY: MODES 1, 2, 3, and 4.

ACTIONS

CONDITION	REQUIRED ACTION	COMPLETION TIME
A. One Reactor Building HVAC Accident Exhaust Filtration train unavailable.	A.1 Restore Reactor Building HVAC Accident Exhaust Filtration train to AVAILABLE status.	14 days
B. Two Reactor Building HVAC Accident Exhaust Filtration trains unavailable.	B.1 Restore one Reactor Building HVAC Accident Exhaust Filtration train to AVAILABLE status.	24 hours
C. Required Action and associated Completion Time not met.	C.1 Enter ACLCO 3.0.3.	Immediately

SURVEILLANCE REQUIREMENTS

SURVEILLANCE		FREQUENCY
ACSR 3.7.4.1	Verify each required Reactor Building HVAC Accident Exhaust Filtration train starts on a manual signal and operates for ≥ 15 continuous minutes.	31 days
ACSR 3.7.4.2	Perform Reactor Building HVAC Accident Exhaust Filtration unit testing in accordance with Subsection 9.4.6.4.	In accordance with Subsection 9.4.6.4

ACM B 3.7 PLANT SYSTEMS

AC B 3.7.4 Reactor Building HVAC Accident Exhaust Filtration

BASES

Contaminated Area HVAC Subsystem (CONAVS) includes redundant Reactor Building HVAC Accident and Online Purge Exhaust Filtration units and exhaust fans (i.e., trains). During radiological events, exhaust air from contaminated areas may be manually diverted through the Reactor Building HVAC Accident or Online Purge Exhaust Filtration units. The Reactor Building Accident and Online Purge Exhaust Filtration units are equipped with pre-filters, high efficiency particulate air (HEPA) filters, high efficiency filters and carbon filters for mitigating and controlling particulate and gaseous effluents from the Reactor Building. After LOCA, one Reactor Building HVAC Accident Exhaust Filtration Unit (the redundant one is in standby) can be energized to exhaust the space air in the CONAVS area.

This accident function is a nonsafety-related function that provides building negative pressure control and exhaust filtering efficiency to ensure that theoretical control room doses are not exceeded for certain beyond design basis LOCAs. Failure to provide adequate filtration is considered to be an adverse system interaction satisfying the criteria for Regulatory Treatment of Non-Safety Systems, and therefore enhanced regulatory oversight is provided. The short-term availability controls for this function, which are specified as Completion Times, are acceptable to ensure that the availability of this function is consistent with the functional unavailability in the ESBWR PRA. The surveillance requirements also provide an adequate level of support to ensure that component performance is consistent with the functional reliability in the ESBWR PRA.

ACM 3.7 PLANT SYSTEMS

AC 3.7.5 Control Room Heating and Ventilation System (CRHAVS) Post 72-Hour Long-Term Cooling

ACLCO 3.7.5 Two trains of CRHAVS Post 72-Hour Long-Term Cooling shall be AVAILABLE.

APPLICABILITY: MODES 1, 2, 3, and 4

ACTIONS

CONDITION	REQUIRED ACTION	COMPLETION TIME
A. One CRHAVS Post 72-Hour Long-Term Cooling train not available	A.1 Restore CRHAVS Post 72-Hour Long-Term Cooling train to AVAILABLE status.	14 days
B. Required Action and associated Completion Time not met. <u>OR</u> Two CRHAVS Post 72-Hour Long-Term Cooling trains not AVAILABLE	B.1 Enter ACLCO 3.0.3.	Immediately

SURVEILLANCE REQUIREMENTS

SURVEILLANCE		FREQUENCY
ACSR 3.7.5.1	Verify each required CRHAVS Post 72-Hour Long-Term Cooling train starts on a manual signal and operates for ≥ 15 minutes.	31 days
ACSR 3.7.5.2	Verify that each CRHAVS Post 72-Hour Long-Term Cooling train has the capability to remove the required heat load.	24 months

ACM B 3.7 PLANT SYSTEMS

AC B 3.7.5 Control Room Heating and Ventilation System (CRHAVS) Post 72-Hour Long-Term Cooling

BASES

The CRHAVS Post 72-Hour Long-Term Cooling trains ensure that, after 72 hours, main control room, temperature is maintained at an acceptable level for personnel and post-accident monitoring equipment. Each CRHAVS Post 72-Hour Long-Term Cooling train consists of one recirculation air-handling unit (AHU) and one associated auxiliary cooling unit. During a loss of normal AC power, the power for either recirculation AHU fan with associated auxiliary cooling unit can be provided from the available ancillary diesel generator.

The CRHAVS Post 72-Hour Long-Term Cooling function is performed by nonsafety-related components that satisfy the significance criteria for Regulatory Treatment of Non-Safety Systems, and therefore requires regulatory oversight. The short-term availability controls for this function, which are specified as Completion Times, are acceptable to ensure that the availability of this function is consistent with the functional unavailability in the ESBWR PRA. The surveillance requirements also provide an adequate level of support to ensure that component performance is consistent with the functional reliability in the ESBWR PRA.

ACM 3.8 ELECTRICAL POWER SYSTEMS

AC 3.8.1 Standby Diesel Generators - Operating

ACLCO 3.8.1 One standby diesel generator shall be AVAILABLE.

APPLICABILITY: MODES 1, 2, 3, and 4

ACTIONS

CONDITION	REQUIRED ACTION	COMPLETION TIME
A. Required standby diesel generator unavailable.	A.1 Restore required standby diesel generator to AVAILABLE status.	14 days
B. Required Action and associated Completion Time not met.	B.1 Enter ACLCO 3.0.3.	Immediately

SURVEILLANCE REQUIREMENTS

SURVEILLANCE		FREQUENCY
ACSR 3.8.1.1	Verify that the fuel oil volume in the required standby diesel generator fuel tank is within limits.	31 days
ACSR 3.8.1.2	Verify that the required standby diesel generator starts and operates at rated load for ≥ 1 hour.	92 days
ACSR 3.8.1.3	Verify the fuel oil transfer system operates to transfer fuel oil from storage tank to the required standby diesel generator day tank.	92 days

SURVEILLANCE		FREQUENCY
ACSR 3.8.1.4	Verify required standby diesel generator starts and achieves rated speed and voltage upon receipt of an undervoltage signal and sequences its designed loads while maintaining voltage and frequency within design limits.	24 months
ACSR 3.8.1.5	Verify required standby diesel generator starts and operates at rated load for ≥ 24 hours.	24 months

ACM 3.8 ELECTRICAL POWER SYSTEMS

AC 3.8.2 Standby Diesel Generators - Shutdown

ACLCO 3.8.2 Two standby diesel generators shall be AVAILABLE.

APPLICABILITY: MODES 5 and 6

ACTIONS

CONDITION	REQUIRED ACTION		COMPLETION TIME
A. One standby diesel generator unavailable.	A.1	Restore standby diesel generator to AVAILABLE status.	14 days
B. Two standby diesel generators unavailable.	B.1	Restore one standby diesel generator to AVAILABLE status.	24 hours
C. Required Action and associated Completion Time not met.	C.1	Enter ACLCO 3.0.3.	Immediately
	AND		
	C.1	Initiate action to suspend operations with a potential for draining the reactor vessel (OPDRVs).	Immediately
	AND		
	C.2	Initiate action to restore Reactor Building to OPERABLE status.	Immediately

SURVEILLANCE REQUIREMENTS

SURVEILLANCE		FREQUENCY
ACSR 3.8.2.1	Verify that the fuel oil volume in the standby diesel generator fuel tank is within limits.	31 days
ACSR 3.8.2.2	Verify that the standby diesel generator starts and operates at rated load for ≥ 1 hour.	92 days
ACSR 3.8.2.3	Verify the fuel oil transfer system operates to transfer fuel oil from storage tank to each standby diesel generator day tank.	92 days
ACSR 3.8.2.4	Verify standby diesel generator starts and achieves rated speed and voltage upon receipt of an undervoltage signal and sequences its designed loads while maintaining voltage and frequency within design limits.	24 months
ACSR 3.8.2.5	Verify standby diesel generator starts and operates at rated load for ≥ 24 hours.	24 months

ACM B 3.8 ELECTRICAL POWER SYSTEMS

AC B 3.8.1 / B 3.8.2 Standby Diesel Generators

BASES

The Standby Diesel Generators (SDGs) provide backup AC power for Fuel and Auxiliary Pools Cooling System (FAPCS) in non-seismic PRA sequences (i.e., RTNSS Criterion C). No SDG-derived AC power is required for 72 hours after an abnormal event. In addition, the SDGs provide power to the Reactor Water Cleanup / Shutdown Cooling (RWCU/SDC) system operating in the shutdown cooling mode in the event of a loss of preferred power (LOPP).

The SDG function is a nonsafety-related function that satisfies the significance criteria for Regulatory Treatment of Non-Safety Systems, and therefore requires regulatory oversight. The short-term availability controls for this function, which are specified as Completion Times, are acceptable to ensure that the availability of this function is consistent with the functional unavailability in the ESBWR PRA. The surveillance requirements also provide an adequate level of support to ensure that component performance is consistent with the functional reliability in the ESBWR PRA.

One SDG is required to be AVAILABLE during MODES 1, 2, 3, and 4 to support FAPCS. Two SDGs are required be OPERABLE during MODES 5 and 6 when core heat removal is being performed by the RWCU/SDC system. Planned maintenance should not be performed on the SDGs during operation in MODES 5 or 6. The bases for this requirement is that the AC power is more risk important during shutdown MODES, especially when the RCS is open than during other MODES.

SDG starts required by ACSRs may be preceded by an engine prelube period prior to starting and warm-up period prior to loading to minimize wear and tear on the SDGs during testing. For the purpose of this testing, the SDGs must be started from standby conditions, that is, with the engine coolant and oil being continuously circulated and temperature maintained consistent with manufacturer recommendations. Testing required by ACSR 3.8.1.5 also demonstrates OPERABILITY of the associated fuel oil transfer pump and necessary SDG support system function(s).

ACM 3.8 ELECTRICAL POWER SYSTEMS

AC 3.8.3 Ancillary Diesel Generators

ACLCO 3.8.3 Two ancillary diesel generators shall be AVAILABLE.

APPLICABILITY: MODES 1, 2, 3, 4, 5, and 6.

ACTIONS

CONDITION	REQUIRED ACTION	COMPLETION TIME
A. One ancillary diesel generator unavailable.	A.1 Restore ancillary diesel generator to AVAILABLE status.	14 days
B. Two ancillary diesel generators unavailable.	B.1 Restore two ancillary diesel generators to AVAILABLE status.	24 hours
C. Required Action and associated Completion Time not met.	C.1 Enter ACLCO 3.0.3.	Immediately

SURVEILLANCE REQUIREMENTS

SURVEILLANCE		FREQUENCY
ACSR 3.8.3.1	Verify that the fuel volume is within limits for the ancillary diesel generators.	31 days
ACSR 3.8.3.2	Verify that each ancillary diesel generator starts and operates at rated load for ≥ 1 hour.	92 days

SURVEILLANCE		FREQUENCY
ACSR 3.8.3.3	Verify the fuel oil transfer system operates to transfer fuel oil from storage tank to each ancillary diesel generator day tank.	92 days
ACSR 3.8.3.4	Verify that each ancillary diesel generator starts and operates at rated load for ≥ 24 hours.	24 months

ACM B 3.8 ELECTRICAL POWER SYSTEM

AC B 3.8.3 Ancillary Diesel Generators

BASES

Upon a loss of power, the Ancillary Diesel Generators (ADGs) are required to support post 72-hour operation of core cooling, containment integrity, control room habitability, and post-accident monitoring.

The ancillary diesel generator function is a nonsafety-related function that satisfies the significance criteria for Regulatory Treatment of Non-Safety Systems, and therefore requires regulatory oversight. The short-term availability controls for this function, which are specified as Completion Times, are acceptable to ensure that the availability of this function is consistent with the functional unavailability in the ESBWR PRA. The surveillance requirements also provide an adequate level of support to ensure that component performance is consistent with the functional reliability in the ESBWR PRA.

ADG starts required by ACSRs may be preceded by an engine prelube period prior to starting and warm-up period prior to loading to minimize wear and tear on the ADGs during testing.

ACM 4.0 DESIGN FEATURES

AC 4.1 Basemat-Internal Melt Arrest and Coolability (BiMAC) Device

AC 4.1.1 Volume

The BiMAC is designed and shall be maintained with an available volume, up to a height of the vertical segments of the BiMAC pipes, sized to contain approximately 400% of the full-core debris.

AC 4.1.2 Protective Layer

The BiMAC is designed and shall be maintained with material located on top of the BiMAC pipes to protect against melt impingement during the initial corium relocation event.

AC 4.1.3 Cover Plate

The BiMAC is designed and shall be maintained with a cover providing protection for the BiMAC from CRD housings falling from the vessel.

AC 4.1.4 Piping

The BiMAC is designed and shall be maintained with piping inclined from horizontal to permit natural circulation flow.