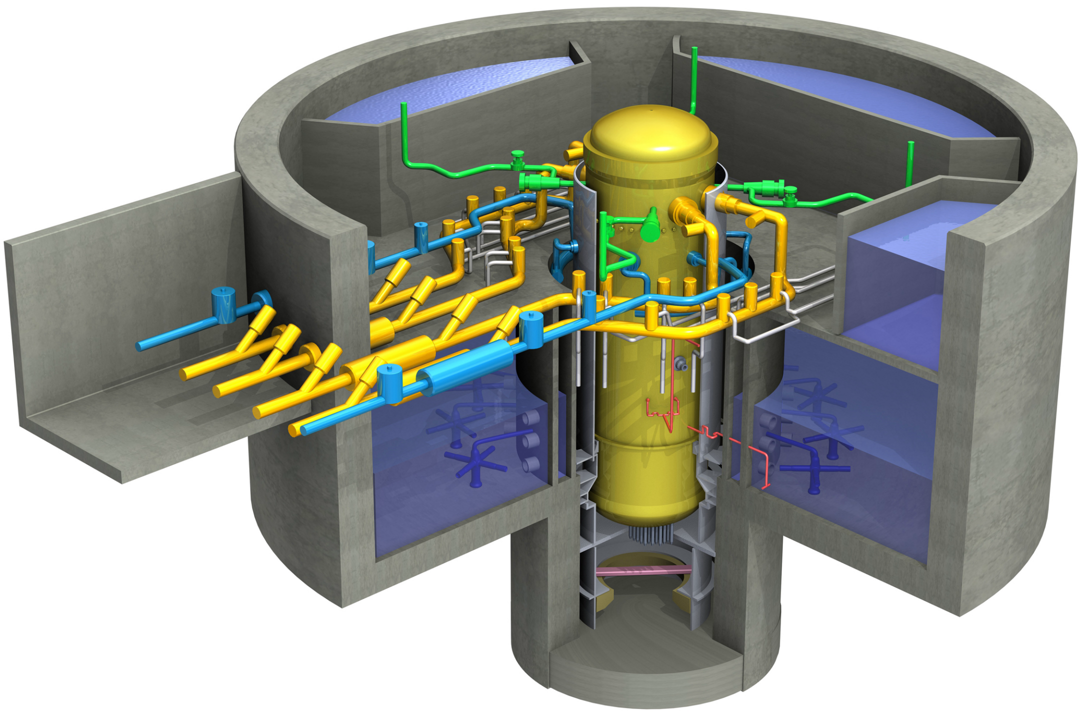
GE-Hitachi Nuclear Energy

26A6642BY
Revision 4
September 2007



ESBWR Design Control Document
Tier 2

Chapter 19
Probabilistic Risk Assessment and Severe Accidents

Contents

Contents

Contents

Contents

List of Tables

List of Figures

Abbreviations And Acronyms List

10 CFR	Title 10, Code of Federal Regulations
ADS	Automatic Depressurization System
AOO	Anticipated Operational Occurrence
ARI	Alternate Rod Insertion
ATWS	Anticipated Transients Without Scram
BiMAC	Basemat Internal Melt Arrest and Coolability
BWR	Boiling Water Reactor
CCF	Common Cause Failure
CCFP	Conditional Containment Failure Probability
CDF	Core Damage Frequency
CET	Containment Event Tree
CFR	Code of Federal Regulations
COL	Combined Operating License
CRD	Control Rod Drive
CRDM	Control Rod Drive Mechanism
CST	Condensate Storage Tank
CV	Containment Vessel
DC	Direct Current
DCH	Direct Containment Heating
DCS	Drywell Cooling System
DG	Diesel-Generator
DPV	Depressurization Valve
DW	Drywell
EPRI	Electric Power Research Institute
EVE	Ex-Vessel Steam Explosion
FAPCS	Fuel and Auxiliary Pools Cooling System
FMCRD	Fine Motion Control Rod Drive
FPS	Fire Protection System
FV	Fussell-Vesely Importance
GDC	General Design Criteria

Abbreviations And Acronyms List

GDCS	Gravity-Driven Cooling System
GEEN	General Electric Energy Nuclear
HCLPF	High Confidence Low Probability of Failure
HFE	Human Factors Engineering
HP	High Pressure
HVAC	Heating, Ventilation and Air Conditioning
HX	Heat Exchanger
I&C	Instrumentation and Control
IAS	Instrument Air System
IC	Isolation Condenser
ICD	Interface Control Diagram
ICS	Isolation Condenser System
LAPP	Loss of Alternate Preferred Power
LDW	Lower Drywell
LOCA	Loss of Coolant Accident
LOPP	Loss of Preferred Power
LP	Low Pressure
LPCI	Low Pressure Coolant Injection
MCS	Minimal Cutset
MOV	Motor-Operated Valve
MSL	Main Steamline
NBS	Nuclear Boiler System
PCCS	Passive Containment Cooling System
PCS	Power Conversion System
PRA	Probabilistic Risk Assessment
PWR	Pressurized Water Reactor
RAP	Reliability Assurance Program
RAW	Risk Achievement Worth
RCCV	Reinforced Concrete Containment Vessel
RCCWS	Reactor Component Cooling Water System
RCPB	Reactor Coolant Pressure Boundary

Abbreviations And Acronyms List

REM	Radiation Dose Equivalence Measure
RG	Regulatory Guide
ROAAM	Risk-Oriented Accident Analysis Methodology
RPS	Reactor Protection System
RPV	Reactor Pressure Vessel
RTNSS	Regulatory Treatment of Non-Safety Systems
RWCU/SDC	Reactor Water Cleanup/Shutdown Cooling System
S/P	Suppression Pool
SA	Severe Accidents
SAM	Severe Accident Management
SAS	Service Air System
SDC	Shutdown Cooling
SLCS	Standby Liquid Control System
SMA	Seismic Margins Analysis
SRP	Standard Review Plan
SRV	Safety Relief Valve
SSC	Structures, Systems, and Components
SSE	Safe Shutdown Earthquake
TAF	Top of Active Fuel
TMI	Three Mile Island
TS	Technical Specification
TRM	Technical Requirements Manual
TSL	Technical Specification Leakage
UDW	Upper Drywell
UHS	Ultimate Heat Sink
URD	Utility Requirement Documents
VAC	Volts Alternating Current
VDC	Volts Direct Current

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.

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 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 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; and
- Contain a design-specific PRA.

Information on compliance with the TMI requirements is provided in ESBWR DCD Tier 2, Appendix 1A. Information on relevant unresolved safety issues is provided in ESBWR DCD Tier 2, 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 all 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 applicant 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 SRM.
- 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 RTNSS is sufficient and, if appropriate, identify the SSCs included in RTNSS.

- Support, as a minimum, regulatory oversight processes, and programs that are associated with plant operations, e.g., TS, 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 ITAAC; the RAP; TS; and 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 LWR design certification policy Severe Accidents 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; and
- 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; and
- 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 Energy Nuclear, "ESBWR Probabilistic Risk Assessment Chapters 1 through 7" NEDO-33201, Revision 2, April 2007.

Table 19.1-1
Systems and Functions Modeled

System	PRA Function
BiMAC Device	Mitigate potential core-concrete interaction. GDCS deluge valves provide a flow path from the GDCS pools to the BiMAC device upon initiation signal of high LDW temperature indicative of a core melt-through.
BOP Power Conversion	The preferred method of heat transfer following a transient including: Turbine Bypass Valves, Main Steam Lines, Circulating Water Pumps, FW pumps, Condensate pumps.
Containment Isolation Valves	Isolate Breaks in Feedwater, ICS, Main Steam, or RWCU 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 is required to avoid the failure of the containment boundary.
Control Rod Drive 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	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.

Table 19.1-1
Systems and Functions Modeled

System	**PRA Function**
Fuel and Auxiliary Pools Cooling System	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 RWCU/SDC loop B and then Feedwater loop A. After successful 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 is automatically initiated in response to a high suppression pool temperature signal and may be manually initiated following an accident.
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.
FPS Diesel Pump	After successful RPV depressurization, FPS 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. Provides emergency makeup water for the auxiliary refueling pools Provides makeup for reactor water inventory control though connection to FAPCS. FPS is used in the FAPCS injection mode as a backup suction source to the suppression pool. This is backed up by the ability to make up water to the pools using various water systems. In the PRA, the source provided by FPS is credited because it is completely independent, including support systems, of GDCS and the PCCS automatic water makeup.

Table 19.1-1
Systems and Functions Modeled

System	PRA Function
Gravity Driven Cooling System	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 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	Remove post-reactor isolation decay heat with three out of four ICs operating and to reduce reactor pressure and temperature to safe shutdown conditions. Automatic initiation of this function occurs on either low RPV water level, closure of 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 Level 1 is not reached.
Instrument Air, Service Air, High Pressure Nitrogen Supply	Valve Motive Power
Lower Drywell Hatches	The position of the LDW hatches must be controlled during shutdowns to ensure that they will close, if demanded, 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.

Table 19.1-1
Systems and Functions Modeled

System	PRA Function
Nuclear Boiler System	During an ATWS, RPV pressure is challenged by the unmitigated reactor power. Following a transient with loss of PCS and ICS, RPV pressure rises, which causes one or more 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 depressurize the RPV by opening SRVs to permit effective FACPS or FPS injection to the RPV. Automatically or manually actuated SRVs and DPVs reduce reactor pressure to allow for low pressure injection. ADS actuation logic initiates the depressurization.
Passive Containment Cooling System	The PCCS loops receive a steam-gas mixture supply directly from the DW. The PCCS loops are initially driven by the pressure difference created between the containment DW 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.
Plant Service Water System	Component Cooling
Power Distribution	AC Power, Uninterruptible AC Power, DC Power
Reactor Component Cooling System	Component Cooling for Reactor Building
Reactor Protection System	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 Reactor Protection System (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.

Table 19.1-1
Systems and Functions Modeled

System	PRA Function
RWCU/Shutdown Cooling Mode	RWCU/SDC provides decay heat removal in response to transients. After an ATWS, RWCU is isolated to prevent filtering out boron. After an ATWS, RWCU may be manually restarted to supply shutdown cooling.
Standby Liquid Control System	For ATWS events, the failure of control rods to insert in response to a valid trip demand is assumed and SLCS automatically initiates. Operator action - failure to successfully control power during an ATWS.
Standby AC Power	Standby Diesel Generators
Switchyard	The switchyard transmits AC power to and from the grid.
Turbine Component Cooling 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 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 DW and WW must maintain this DW to WW pressure differential. During a LOCA, the vacuum breakers open to allow the flow of gas from WW to DW to equalize the WW and DW pressure. If they subsequently do not completely close, as detected by proximity sensors, a control signal will close the upstream butterfly isolation valves to prevent extra 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. In order to maintain a PRA model that reasonably reflects the as-built and as-operated characteristics of the plant, controls are implemented to maintain the 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 (F-V) 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.

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 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.

(3) Anticipated Transients Without Scram (ATWS) events are low contributors to plant core damage frequency (CDF) because of the improved scram function and passive boron injection.

(4) The ESBWR design reduces the frequency and consequences of loss of coolant accidents (LOCA) due to 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 Passive Containment Cooling System is highly reliable due to redundant heat exchangers and totally passive component design.

(7) 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 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 Diverse Protection System, 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 Isolation Condenser and Passive Containment Cooling pool makeup.

(5) Added redundant drain line valves for Isolation Condenser System 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 locations of control and instrumentation cabinets and power supplies to ensure physical separation.

(8) Added the Basemat Internal Melt Arrest and Coolability device (BiMAC) 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 (Reference: DCD Tier 2 Appendix 19A);
- Provide an independent assessment of the set of surveillance intervals and allowed outage times in the technical specifications (Reference: DCD Tier 2 Chapter 16);
- Identify the most important operator action categories in support of the man-machine interface (Reference: DCD Tier 2 Chapter 18); and
- Assist in identifying the most appropriate level of defense-in-depth and diversity for the instrument and control systems (Reference: DCD Tier 2 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 (Reference: DCD Tier 2 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 (Reference: DCD Tier 2 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 (Reference: DCD Tier 2 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 theCOL 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

<u>Identification of Internal Initiating Events</u>

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 events categories are identified below.

- Transients
  - Generic Transient,
  - Loss of Feedwater,
  - Loss of Preferred Power,

- Loss of the Plant Service Water system, and
- Inadvertent Opening of a Relief Valve.

- Loss of Coolant Accidents

  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; and
  - 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; and
  - Interfacing Systems LOCA.

- Anticipated Transients Without Scram (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 Transient with the Power Conversion System Unavailable, and the Transient due to Complete Loss of Air Systems are grouped with the General Transient for this reason. Also, the Interfacing Systems LOCA initiating event is grouped with the Break Outside Containment in RWCU Line 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 is defined as the acceptance criterion for the RPV overpressure protection.
- Core Cooling

  - A peak cladding temperature of 2200°F is defined as the criterion for establishing the adequacy of coolant inventory.

- 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.

<u>Event Tree Development of Internal Events</u>

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; and
- 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 systems and several non-safety 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 (CCF) 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, the use 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 Isolation Condensers. 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.

Important operator actions involve recognizing the need for depressurization or providing low pressure injection in particular scenarios; failure to restart feedwater pumps during certain ATWS scenarios; and pre-initiator valve mispositioning events in the FAPCS, CRD, and RCCW systems. Information on important operator actions is incorporated into the human factors engineering program.

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.

- Inadvertent Opening of a Relief Valve
  - Scram is successful
  - High Pressure Injection fails
  - Depressurization is successful
  - Low Pressure Injection fails
- General Transient with ATWS

  - Scram fails
  - SLCS fails
- Loss of Feedwater
  - Scram is successful
  - Isolation Condensers fail
  - Depressurization is successful
  - Low Pressure Injection fails
- Inadvertent Opening of a Relief Valve
  - Scram is successful
  - High Pressure Injection fails
  - Active Low Pressure Injection fails
  - Depressurization fails
- General Transient with ATWS
  - Scram fails
  - One or more SRVs sticks open
  - Failure to maintain RPV water level
- Inadvertent Opening of a Relief Valve
  - Scram is successful
  - High Pressure Injection fails
  - Active Low Pressure Injection fails
  - Depressurization fails
- Loss of Preferred Power with ATWS
  - Scram fails
  - One or more SRVs stick open
  - Failure to maintain level
- Inadvertent Opening of a Relief Valve
  - Scram is successful
  - High Pressure Injection fails
  - Depressurization is successful
  - Low Pressure Injection fails

- Line Break in Feedwater Line B
  - Scram is successful
  - LOCA depressurizes RPV – fails Feedwater
  - Low Pressure Injection fails
- Loss of Preferred Power
  - Scram is successful
  - Isolation Condensers fail
  - Depressurization is successful
  - Low Pressure 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 m) 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.

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 (that is, in conventional BWRs) are found to have a small, but relatively measurable contribution to LRF due to the failure of passive design features.

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 to >100 Sv 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.

Anticipated Transients Without Scram (ATWS) events are low contributors to plant core damage frequency (CDF) because of improvements in the scram function and passive boron injection.

The ESBWR design reduces the frequency and consequences of loss of coolant accidents (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 Passive Containment Cooling System is highly reliable due to redundant heat exchangers and totally 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.

<u>Significant Core Damage Sequences of External Event Fire</u>

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-initiated accident sequences begin with a fire in the Reactor Building that damages one electrical division. Subsequent failures of the digital control system and GDCS injection require the use of alternate low pressure injection, which fails due to operator error.

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

Due to the bounding method that is used to calculate the fire CDF, it is considered to be unnecessary to extrapolate offsite consequences.

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

Due to the low CDF, there are no significant flood-initiated accident sequences. The most important flood sequences during at-power conditions involve Service Water piping leaks at the Service Water structure which result in the loss of an entire train.

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 have been relocated outside of 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

Due to the bounding method that is used to calculate the flood CDF and its very low value compared to that of internal events CDF, it is considered to be unnecessary to extrapolate offsite consequences.

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 diesel driven fire protection pump for alternate RPV injection, and the DC batteries with a 72-hour operational life.

Significant Core Damage Sequences of External Event High Wind

There are no important sequences identified in the high wind analysis.

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 are not analyzed for large release frequency.

Significant Offsite Consequences of External Event High Wind

Due to the bounding method that is used to calculate the high wind CDF and its very low value compared to that of internal events CDF, it is considered to be unnecessary to extrapolate offsite consequences.

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 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).

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 referencing the ESBWR certified design shall compare 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. (COL 19.2.6-1-H) 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.

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 consequences 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 key insights regarding the seismic capability of the ESBWR:

- The ESBWR is inherently capable of safe shutdown in response to strong magnitude earthquakes; and

- 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 Operations, 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, the containment, and systems that support operation of the NSSS, and containment.

19.2.4.1 Significant Core Damage Sequences During Shutdown Mode

19.2.4.1.1 Internal Events During Shutdown

The important initiating events in the internal events shutdown PRA are:

- Instrument Line Break Below TAF – Mode 6, Flooded;
- Instrument Line Break Below TAF – Mode 5;
- RWCU/SDC Drain Line Break Below TAF – Mode 6, Flooded;
- Instrument Line Break Below TAF – Mode 6, Unflooded; and
- RWCU/SDC Drain Line Break Below TAF – Mode 5.

Thhe accident sequences involve line breaks below the top of active fuel, with failure to close the lower drywell equipment hatch (which is assumed to be open during Mode 6), and subsequent failure to flood containment to above top of active fuel. The fourth sequence involves loss of preferred power, with failure to align fire protection system water for injection to the RPV.

The most important operator action in the ESBWR shutdown analysis is to close the lower drywell hatches upon the detection of a break in the RCS. Other operator actions are non-significant contributors to internal events shutdown CDF.

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

19.2.4.1.2 Fire During Shutdown

Important fire initiating events in the shutdown internal fires PRA are fires in the Turbine Building that cause a loss of RWCU Shutdown Cooling, and fires in the Service Water structure that cause a loss of Service Water. Failure of the corresponding safety system division is assumed, along with failure of one train of RWCU/SDC and CRD, depending on the particular zone that contains the fire.

The important operator actions in the shutdown internal fires PRA are failure to use CRD injection and failure to use the diesel driven makeup pump for low pressure injection.

19.2.4.1.3 Flooding During Shutdown

The important flood initiating events in the shutdown internal flooding PRA are a failure of a GDCS pool during Mode 6-Unflooded and a CRD break in the Reactor Building during Mode 6. However, the total contribution flood during shutdown sequences is negligible.

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.

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.

19.2.4.1.5 Seismic Events 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.

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.

19.2.4.1.6 Shutdown PRA Assumptions

Compared to Residual Heat Removal System in BWRs, the RWCU/SDCS in the ESBWR does not have the potential for diverting RPV inventory to the suppression pool through the SP 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/SDCS 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

The dominant contributors to shutdown CDF involve sequences during Mode 6 (Refueling Mode). The dominant initiating events are line breaks from lines penetrating the reactor vessel below the top of the core. In the line break sequences, the critical action is to isolate the lower drywell, by closing the lower drywell hatches, so a boundary can be established to permit flooding above the top of active fuel. The resultant release during a severe accident is considered a containment bypass release.

The offsite consequences from shutdown risk are judged to be negligible on the following basis:

- The significant shutdown events occur during Mode 6, which does not begin until approximately 96 hours after shutdown. The decay of fission products after 96 hours reduces the source term to less than 1% of the value at power operating conditions. Therefore, a postulated core damage event during shutdown would have a significantly lower source term and resultant offsite consequences than a containment bypass at full power.
- The lower drywell hatches are only open for a limited period of time during Mode 6 to allow under-vessel maintenance activities on the control rod drive mechanisms and neutron monitoring instrumentation. The details of exposure time are not developed in the design phase, but administrative controls will be implemented to limit the time that the hatches are open, as well as provide compensatory guidance if a line break occurs while the hatches are open. Therefore, the frequency of containment bypass events during shutdown can be significantly reduced.

19.2.4.4 Summary of Important Results and Insights of Shutdown Mode

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 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 decay heat removal function during this mode.

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. 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 Technical Specification leakage (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 individual, societal, and radiation dose limits by several orders of magnitude.

19.2.6 COL Information

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

The COL Holder referencing the ESBWR certified design shall compare 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. (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 NEDO-33306, "Severe Accident Mitigation Alternatives," Revision 1, August 2007

Table 19.2-1
Comparison of ESBWR Features With Existing BWRs

NUREG-1560 IPE Key Observations	ESBWR Features
General Observation The variation in the [IPE] 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.

Table 19.2-1
Comparison of ESBWR Features With Existing BWRs

NUREG-1560 IPE Key Observations	ESBWR Features
<u>Loss of Preferred Power</u> 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. Diesel-driven fire water has been added as a diverse makeup system. The core can be kept covered without any AC sources, which results in LOPP initiated CDF that is very much lower than BWRs.
<u>ATWS</u> 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.
<u>Internal Floods</u> 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

NUREG-1560 IPE Key Observations	ESBWR Features
<u>LOCAs</u> 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 ECCS. The reliability of depressurization and injection functions is significantly improved, with no reliance on operator action. ESBWR design reduces the potential for LOCA by removing the recirculation system altogether.
<u>ISLOCA</u> 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.
<u>Early Containment Failure</u> 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.

Table 19.2-1
Comparison of ESBWR Features With Existing BWRs

NUREG-1560 IPE Key Observations	ESBWR Features
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.	The probability of a loss of containment heat removal is significantly reduced because the Passive Containment Cooling System is highly reliable due to redundant heat exchangers and totally passive component design.
High pressure and temperature loads caused by core-concrete interactions are important for late failure in BWR containments.	The BiMAC device is designed to prevent core-concrete interactions.
Containment venting is important for avoiding late uncontrolled failure in some Mark I containment.	Containment venting is possible in the ESBWR, but the importance has been minimized by the PCCS reliability.
Human Actions	
Only a few specific human actions are consistently important for either BWRs or PWRs as reported in the IPEs. 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, SLCS, Suppression Pool Cooling).

Table 19.2-1
Comparison of ESBWR Features With Existing BWRs

NUREG-1560 IPE Key Observations	ESBWR Features
<u>Station Blackout</u> 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 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 • Independent of AC Power to operate
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 Pool 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 • Fire water 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)

Table 19.2-3
Risk Insights and Assumptions

Insight or Assumption	Disposition
Dominant initiating events for internal events: %T-IORV, %T-GEN, %T-FDW, and %T-LOPP are applied using operating experience data. LOCA frequencies (%LL-S-FDWB) are also applied using operating experience data. Overall, none of the dominant initiating events are considered to have unique risk insights.	Insight
The most important Level 2 initiating events are %T-IORV, %T-GEN, and %T-FDW; however, they result in controlled releases. The most important large release initiating event is %LL-S-FDWB, which represents a Large LOCA in Feedwater Line B.	Insight
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 Technical Specification leakage (TSL).	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 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.	Insight
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.	Insight
Anticipated Transients Without Scram (ATWS) events are low contributors to plant core damage frequency (CDF) because of the improved scram function and passive boron injection.	Insight

Table 19.2-3
Risk Insights and Assumptions

Insight or Assumption	Disposition
The ESBWR design reduces the frequency and consequences of loss of coolant accidents (LOCA) due to large diameter piping by removing the recirculation system altogether.	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
The probability of a loss of containment heat removal is significantly reduced because the Passive Containment Cooling System is highly reliable due to redundant heat exchangers and totally passive component design.	Insight
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 than conventional BWRs.	Insight
Dominant 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.	Insight
The most significant seismic margins contributor is seismic-induced loss of DC power, and ATWS due to seismic-induced failure of the fuel channels and seismic-induced failure of the SLC tank.	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. These data are binned into the LOCA initiator classes, as summarized in Section 2, Table 2.3-2. Sensitivity study results indicate that changes in the LOCA frequencies have the potential to impact CDF.	Insight

Table 19.2-3
Risk Insights and Assumptions

Insight or Assumption	Disposition
Sensitivity study results indicate that changes in the human error failure probabilities, particularly pre-initiators, have the potential to impact CDF.	Insight
Sensitivity studyresults indicate that squib valve failure rate estimates have the potential to impact CDF	Insight
Sensitivity study results indicate that changes in test and maintenance unavailability do not significantly impact the CDF or insights.	Insight
Accident sequences in which DPVs are challenged contribute to approximately 61% of the CDF. In two-thirds of the cases the DPVs are demanded and are successful, and in one-third of the cases the DPVs are demanded and have failed.	Insight
Core damage sequences involving failure of ICS are Class I or III sequences where high pressure makeup has failed and either failure to depressurize occurs or low pressure injection is not available. Given that ICS is failed, the failure of PCCS, or failure to provide make-up to the pools are not significant contributors to core damage frequency.	Insight
FAPCS and FPS 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
CRD injection is unaffected by containment overpressurization failure. This is an important assumption, based on the containment failure analysis, that supports the use of CRD in these sequences.	Design Requirement
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 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

Table 19.2-3
Risk Insights and Assumptions

Insight or Assumption	Disposition
The ESBWR design features as described in DCD Tier 2 Section 7.1.3 help minimize the adverse affect on safe shutdown due to fire-induced spurious actuations. First of all, the ESBWR instrumentation and control system is digital. A spurious signal cannot be induced by the fire damages in a fiber optic cable. The hard wires are minimized to limit the consequences of a postulated fire. Typically the main control room (MCR) communicates with the safety-related and nonsafety-related DCIS rooms with fiber optics. From the DCIS rooms to the components, fiber optics will also be used up to the Remote Multiplexing Units (RMUs) in the plant. Hard wires then are used to control the subject components. Typically two load drivers are actuated simultaneously in order to actuate the component. To eliminate spurious actuations, these two load drivers are located in different fire areas. Therefore, a fire in a single fire area cannot cause spurious actuation.	Design Requirement
Since the main control room communicates with the DCIS rooms via fiber-optic cables, no spurious actuations due to electrical shorting will be originated from a MCR fire.	Design Requirement
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
The Class IV (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. It is shown in Appendix 8A that the frequency of ATWS sequences experiencing RPV rupture at high pressure is negligible, so only failures at low pressure were analyzed.	Operational Program
Venting is assumed to occur when the containment pressure reaches 90% of the ultimate containment strength.	Operational Program

Table 19.2-3
Risk Insights and Assumptions

Insight or Assumption	Disposition
During shutdown conditions, a fire barrier may not be intact due to maintenance activities. However, an added fire watch would not only increase the success probability of fire detection and suppression, but also help restore the fire barrier in time to prevent fire propagation. Shutdown fire risks related to the fire barriers are evaluated and managed in accordance with the outage risk management program of 10CFR50.65(a)(4).	Operational Program
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
An important recovery action during shutdown is to recover at least one train after loss of both operating RWCU/SDCS trains.	Operational Program
An important recovery action during shutdown is to recover Service Water function after loss of PSW.	Operational Program
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
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).	Operational Program
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 decay heat removal function during this mode.	Operational Program

Table 19.2-3
Risk Insights and Assumptions

Insight or Assumption	Disposition
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
It is assumed that, during shutdown, manual and automatic depressurization (ADS) of the vessel are available while the vessel head is in place.	Operational Program
It is assumed that the actuation of the GDCS due to an RPV Level 1 water level signal is available during the entire shutdown period.	Operational Program

Table 19.2-4
ESBWR Systems and Structures in Seismic Margins Analysis with Plan Level HCLPF > 1.67(1)

PLANT STRUCTURES
- Reactor Building
- Containment
- RPV Pedestal
- Control Building
- Reactor Pressure Vessel Support

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 Plan Level HCLPF > 1.67[1]

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/PCC POOL INTERCONNECTION
- Valve (motor operated)
FIRE PROTECTION WATER SYSTEM
- Pump (diesel driven)

Note:

1. A minimum HCLPF value of 1.67*SSE will be met for the equipment shown.

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; and
- Elimination of the scram discharge volume in the CRD system.

DCD 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 DCD 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 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-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 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.

DCD 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 AC-Independent Fire Water Addition System

The Fire Protection System (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 through the feedwater line and into the reactor pressure vessel. This system must be manually aligned. This is appropriate because the sequences in which 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 IC failures. This system plays a major role in preventing core damage.

19.3.1.8 Isolation Condenser System

The ESBWR ICS is described in DCD 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, following any of the following events:

- Sudden reactor isolation from power operating conditions;
- Station blackout (unavailability of all AC power);
- Anticipated Transient Without Scram (ATWS); and
- 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

19.3.2.1.1 Introduction to 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 is shown to be negligible considering the inerted containment and time period required to generate enough oxygen to create a combustible gas mixture.

Because the ESBWR containment is inerted, the prevention of a combustible gas deflagration 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 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.

<u>Analysis Assumptions</u>

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(O2) = 0.25 molecules/100eV;
- Initial containment O2 concentration = 4%;
- Allowed containment O2 concentration = 5%;
- Stripping of drywell non-condensable gases to wet-well vapor space;
- Fuel clad-coolant reaction up to 100%;
- Iodine release up 100%; and
- Adequate gas mixing throughout containment.

<u>Analysis Results</u>

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 is shown to be unrealistic considering the inerted containment and time period required to generate enough oxygen to create a combustible gas mixture.

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 ICs 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; and
- 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 Technical Specification leakage (TSL). This conclusion is based on the following insights:

(1) The combustible gas generation analysis indicates that a combustible gas mixture within containment would not occur within 24 hours after the occurrence of a severe accident. Thus, containment failure by this mechanism is not considered further.

(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 more than 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 more than 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 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 (BiMAC)

The BiMAC device is a passively-cooled barrier to core debris on the lower drywell (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) Sacrificial refractory layer. A refractory material is located on top of the BiMAC pipes to protect 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 refractory material is selected to have high structural integrity and high resistance to melting.

(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, are positioned and protected in the same manner as the rest of the LDW liner (Figure 19.3-1) These considerations are in the conceptual stage and may be revised in final design.

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 line break outside containment, this system is designed with a third, diverse isolation valve. 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, Section I, SECY-90-16 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 NEDO-33201 Revision 1, Section 8.2, "Frequency of Overpressure and Bypass Release Categories," and Section 8.3 of the DCD, "Containment Performance Against Overpressure."

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 19.3-1and 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:

- <u>Reactivity control</u> is required to terminate the nuclear reaction, thus limiting the core energy to decay heat.
- <u>Depressurization of the RPV</u> 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.
- <u>Core cooling,</u> if provided prior to RPV failure, could limit the progression of a severe accident so that a damaged core is retained in the RPV.
- <u>Cooling of the lower drywell debris bed</u> 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.
- <u>Cooling of the upper drywell debris bed</u> 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 Section 6.3.2.8.

19.3.4.2.3 Core Cooling

Core cooling in a severe accident can be accomplished by the Gravity Drain 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 tanks) 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 Section 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 Sections 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 Section 6.2.4; the LD&IS system is described in Section 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 Section 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 Section 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. 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 Section 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.

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 EPG/SAG 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 DCD Tier 2 Sections 7.3 and 7.4, 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 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 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.

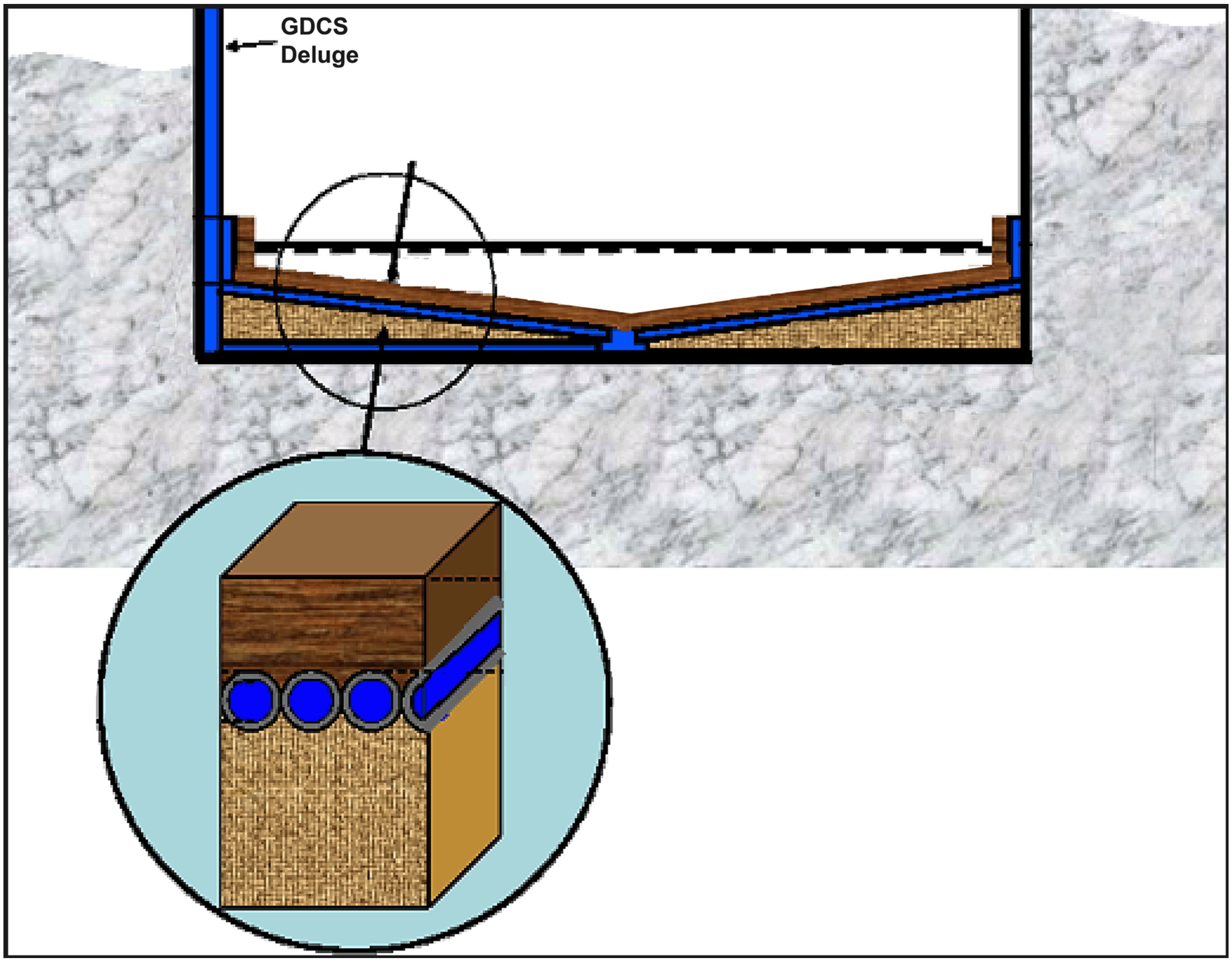


Figure 19.3-1. BiMAC Pipes and Protective Ceramic Layer

Note: Dimensions are for conceptual design purposes and may be revised

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

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; and
- Document the PRA model and the procedures which 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 PRA will be updated 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 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 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 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 PRA is technically adequate for support to other COL Holder programs such as the Maintenance Rule (Section 17.6).

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

Not Applicable

19.4.3.4 Operational Update Phase Changes

Not Applicable

19.4.4 COL Information

None

19.4.5 References

None

19.5 CONCLUSIONS

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 beyond 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 less than 0.1 for the composite of all 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

19A. REGULATORY TREATMENT OF NON-SAFETY SYSTEMS (RTNSS)

19A.1 INTRODUCTION

The purpose of this Section 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 function.

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 of SECY-94-084, "Policy and Technical Issues 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 seismic events. Criterion B is divided into two groupings:

- Criterion B1 addresses those functions that provide defense in depth for key safety functions (core cooling, decay heat removal and control room habitability) that are designed to Seismic Category II standards so there is reasonable assurance that they can perform their functions following a seismic event.

- Criterion B2 addresses components that provide additional information for operators to diagnose plant conditions, (post-accident monitoring) and thus have a less direct effect on the success of key safety functions. Reasonable assurance for long-term functionality of monitoring components is provided by other augmented seismic design criteria, as discussed below.

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 RTNSS equipment, a risk evaluation is performed to determine the appropriate regulatory controls.

19A.1.2 Selection of Important Non-Safety Systems

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, D and E are assessed using deterministic methods, including an assessment of containment performance. Criterion C is assessed probabilistically, by quantitative and qualitative methods based on information derived from the baseline PRA and also a focused PRA sensitivity study. The baseline PRA, described in DCD Tier 2 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 existing 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

ATWS events are described in Subsection 15.5.4 of the DCD. Based upon the results of the analyses, the proposed design for the ESBWR is satisfactory for mitigating the consequences of an ATWS. All performance requirements are met.

10 CFR 50.62 requires Boiling Water Reactors (BWRs) to have an automatic Recirculation Pump Trip (RPT), an Alternate Rod Insertion (ARI) system, and an automatic Standby Liquid Control System (SLCS) for ATWS prevention/mitigation. The ESBWR provides the following respective features:

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

In addition, the ESBWR design uses an electrical insertion of Fine Motion Control Rod Drives (FMCRDs) with sensors and logic that are diverse and independent of the RPS.

The ESBWR design does not use recirculation pumps, so RPT logic does not exist in the ESBWR. However, the ATWS automatic feedwater runback feature provides a reduction in water level, core flow and reactor power, similar to RPT in a forced circulation BWR. This feature prevents reactor vessel overpressure and possible short-term fuel damage for ATWS events.

The ATWS mitigation system and the Diverse Protection System (DPS) comprise the diverse I&C Systems. The diverse I&C systems are parts of the ESBWR defense-in-depth and diversity strategy and provide diverse backup to the Reactor Protection System (RPS) and the Safety System Logic and Control for the Engineered Safety Features (SSLC/ESF). The ATWS mitigating logic system is implemented with the safety-related and nonsafety-related Distributed Control and Information System. The nonsafety-related DPS processes the nonsafety-related portions of the ATWS mitigation logic and is designed to mitigate the possibility of digital protection system common mode failures.

The ATWS/Standby Liquid Control (SLC) mitigation logic provides a diverse means of emergency shutdown using the SLC for soluble boron injection. Alternate Rod Insertion (ARI), which hydraulically scrams the plant using the three sets of air header dump valves of the Control Rod Drive System (CRD), is also used for ATWS mitigation. The ARI logic is implemented in the DPS. The DPS also transmits the feedwater runback signal from the ATWS mitigation logic to the feedwater control system.

The ARI system, the feedwater runback logic, and the ATWS initiation controls for SLCS are selected as RTNSS equipment. The requirements for these systems and functions are consistent with those specified in the ATWS rule.

19A.2.2 Station Blackout Assessment

The ESBWR is designed to cope with a station blackout (SBO) event for 72 hours. The analysis in DCD Tier 2, 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. 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 that are required to be maintained in the long term are:

- Core Cooling,
- Decay heat removal,
- Control Room habitability, and
- Post-accident monitoring.

The ESBWR is designed so that passive systems are able to perform all safety functions for 72 hours after an initiating event without the need for active systems or operator actions. After 72 hours, nonsafety-related systems can be used to replenish the passive systems or to perform safety and post-accident recovery functions directly. Between 72 hours and 7 days, the resources for performing safety functions must be available on-site. After 7 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 and improving, the operating staff is protected, and the condition of the plant can be monitored. SSCs required to perform safety functions after 72 hours are designed to appropriate seismic design standards depending on whether Criterion B1 or B2 applies. In addition, SSC design must consider high wind criteria, and must be flood protected. They must also survive accident environmental conditions. Each safety function is analyzed below to identify nonsafety-related systems that are required after 72 hours to maintain the safety functions within limits. Such systems are candidates for RTNSS.

19A.3.1.1 *Core Cooling*

The safety function is to provide an adequate inventory of water to ensure that the fuel remains cooled and covered, with stable and improving conditions, beyond 72 hours. This function is met by the safety-related Isolation Condenser System (ICS) for scenarios with the RCS intact, and by the safety-related Gravity-Driven Cooling System (GDCS) injection function for scenarios with the RCS open to containment. As long as decay heat removal is ensured as described below, the GDCS provides a sustainable closed-loop method to keep the core covered.

There are no RTNSS systems associated with this safety function.

19A.3.1.2 *Decay Heat Removal*

The safety function is to remove reactor decay heat from the core, containment, and spent fuel pool. The passive systems that provide this function for the core and containment are the safety-related ICS and the safety-related Passive Containment Cooling System (PCCS). These systems are capable of removing decay heat for at least 72 hours without the need for active systems or operator actions. After 72 hours, makeup water is needed to replenish the boil-off from the upper containment and spent fuel pools. The ESBWR design includes permanently installed piping in the Fuel and Auxiliary Pools Cooling System (FAPCS) that connects directly to a diesel-driven makeup pump system. This connection enables the upper containment pools and spent fuel pools to be filled with water from the Fire Protection System (FPS), which provides on-site makeup water to extend the cooling period from 72 hours to 7 days. The dedicated FPS equipment for providing makeup water and the flow paths to the pools are classified as nonsafety-related. Some of the piping that interfaces between FPS, FAPCS, and the pools is safety-related, as described in Tier 2 Subsection 9.1.3. The spent fuel pool is normally cooled by FAPCS. However, on a complete loss of FAPCS cooling under the condition of maximum heat load, a sufficient quantity of water is available in the spent fuel pool to allow boiling for 72 hours and still provide acceptable fuel coverage in the pool. A dedicated external connection to the FAPCS line allows for manual hook-up of external water sources, if needed, at 7 days for either upper containment pool replenishment and for spent fuel pool makeup. These functions are manually actuated from the yard area and can be performed without any support systems.

The following components are within the scope of RTNSS, with the exception of those components described as safety-related in Tier 2 Subsection 9.1.3: the diesel-driven makeup pump system, FAPCS piping connecting to the diesel-driven makeup pump system, the external connection.

19A.3.1.3 *Control Room Habitability*

Safety-related portions of the Control Room Habitability Area Ventilation System maintain control room habitability. This function is operated on safety-related battery power for the first 72 hours following an event. For longer term operation, the system can be powered by a small, portable AC power generator that is kept on the plant site.

This generator is included within the scope of RTNSS.

19A.3.1.4 *Post-Accident Monitoring*

Operator actions are not required for successful operation of safety-related systems for the first 72 hours following an event. Beyond that, operator actions are necessary to support continued operation of decay heat removal and control room ventilation systems. These functions can be performed without any support systems or indications (other than local indications on the equipment to be operated).

However, the operators can use information on the condition of the plant to determine ways to augment the functions needed for beyond design basis response. This provides an additional flexibility (defense-in-depth) for the operators to respond in the post-72 hour time frame.

The Distributed Control and Instrumentation System (DCIS) that is powered by the safety-related power systems is used to perform this monitoring. In order to support monitoring beyond 72 hours, it is necessary to provide power for the Q-DCIS components. Two 6.9 kV Plant Investment Protection (PIP) nonsafety-related buses (PIP-A and PIP-B) provide power for the nonsafety-related PIP loads. PIP-A and PIP-B buses are each backed by a separate standby onsite AC power supply source. Cooling for the areas containing the DCIS components may also be required, depending on the outcome of the detailed building heatup analyses. These functions are provided by nonsafety-related SSCs that are candidates for RTNSS.

The standby diesel generators and the PIP buses provide power for Q-DCIS. Portions of the HVAC systems in the Reactor Building, Electrical Building, Fuel Building, Control Building, and some areas of the Turbine Building perform component and area cooling. In addition, support for these nonsafety-related functions is required from Reactor Component Cooling Water, Plant Service Water, and the Chilled Water System.

19A.3.2 Seismic Assessment

The seismic margins analysis described in section 19.2.3.5 assesses the seismic ruggedness of safety-related plant systems and the non-safety systems required for decay heat removal after 72 hours. No accident sequence has a High Confidence for Low Probability of Failure (HCLPF) ratio less than 1.67 times the peak ground acceleration magnitude of the safe shutdown earthquake (SSE).

Therefore, there are no additional RTNSS candidates due to seismic events.

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 for internal events, evaluations of external events, an assessment of the effects of nonsafety-related systems on initiating event frequencies, and an assessment of uncertainties in these analyses and uncertainties that may be introduced by first of a kind passive components.

19A.4.1 Focused PRA Sensitivity Study

A focused PRA sensitivity study evaluates whether passive 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 retains the same initiating event frequencies as the baseline PRA, and sets the status of nonsafety-related systems to failed, while safety-related systems remain unchanged in the model. The focused PRA model is evaluated using only the safety-related systems and RTNSS systems determined from criteria A or B. Additional nonsafety-related systems are included only if they are required to meet the CDF or LRF goals. The additional nonsafety-related systems required to meet the CDF and LRF goals are candidates for RTNSS.

The CDF and LRF goals will be met with the addition of portions of the Diverse Protection System (DPS) as RTNSS. This is needed to counter the effects of a dominant risk contribution due to common cause failures of actuation instrumentation and controls.

19A.4.2 Assessment of Non-Safety Systems on External Events

The effects of nonsafety-related systems relative to external events, at power and during shutdown, have a negligible effect on the CDF and LRF goals. The insights described in this subsection support this conclusion.

19A.4.2.1 *Fire*

The Fire PRA is a bounding analysis that incorporates several conservative assumptions. The fire analysis does not account for the amount of combustible material present, or for the distance between fire sources and targets. The analysis assumes that a fire ignition in any fire area grows into a fully developed fire. Therefore, fires are conservatively assumed to propagate unsuppressed in each fire area and damage all functions in the fire area.

The ESBWR probabilistic internal fire analysis highlights the following key insights regarding the fire mitigation capability of the ESBWR:

- The basic layout and safety design features of the ESBWR make it inherently capable of mitigating internal fires. Safety system redundancy and physical separation by fire barriers ensure that, in all cases, a single fire limits damage to a single safety system division. Fire propagation to neighboring areas presents a relatively minor risk contribution due to fire barriers.

- A fire in the control room is assumed to affect the execution of human actions. A fire in the control room does not affect the automatic actuations of the safety systems. Additionally, the existence of remote shutdown panels allows the detection of failed automatic actuations and the performance of compensatory manual actuations.

The separation and redundancy of safety systems coupled with the fire protection and suppression features built into the design result in CDF and LRF risks due to internal fires that are not significant. Nonsafety-related systems do not play a significant role in mitigation because fire separation results in one division of safety-related SSCs being damaged while the functions from the remaining three safety-related divisions are intact and capable of achieving safe shutdown conditions.

19A.4.2.2 *Flood*

Due to the inherent ESBWR flooding mitigation capability, some flooding specific design features are key in the mitigation of significant flood sources. Although not a significant contributor to CDF or LRF, the shutdown flooding analysis identified the need to close the Lower Drywell hatches following a flooding event.

Separation, barriers and redundancy features built into the ESBWR plant design ensure that the CDF and LRF risks due to internal floods are not significant. Nonsafety-related systems do not play a significant role in mitigation because separation features result in only one division of safety-related SSCs being damaged by an internal flood while the safety functions from the remaining three safety-related divisions are intact and capable of achieving safe shutdown conditions.

Although the lower drywell hatch is a part of the safety-related containment system, the control of those hatches during shutdown conditions (Modes 5 and 6) is an important function for controlling risk. Lower drywell hatch control is being treated using RTNSS availability controls.

19A.4.2.3 *Wind*

The conclusion from the ESBWR high wind risk analysis is that the risk from hurricane or tornado strikes on the plant is acceptably low. The effect of high winds on the Focused PRA results is similar to a loss of offsite power with the plant safety systems available, and the corresponding CDF and LRF values are very low.

19A.4.2.4 *Seismic*

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/PCC 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.4.3 Assessment of Uncertainties

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

Passive system T-H 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. Therefore, assessing the event tree success criteria in the PRA model identifies T-H uncertainties.

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 these uncertainties, the FAPCS system is added as a RTNSS candidate. This system has the capability to provide a core injection function and to provide a decay heat removal function. The support systems needed to use this system are RCCWS, diesel generators, PIP buses, Fuel Building HVAC, and PSWS. These are all considered to be covered by RTNSS for Criterion C.

The function of FAPCS is provided as a two train system. The 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.

The BiMAC device provides an engineered method to assure heat transfer between a core debris bed and cooling water in the lower drywell during some 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 a first of a kind design that is added to the ESBWR to reduce the uncertainties involved with severe accident phenomenology. As such, it is a candidate for RTNSS.

19A.4.4 PRA Initiating Events Assessment

The At-Power and Shutdown PRA models are reviewed to determine whether non-safety SSCs could have a significant effect on the estimated frequency of initiating events. 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.4.4.1 *At-Power Generic Transients*

Initiating events that are considered Generic Transients are described in subsection 19.2.3.1. Because several initiating events in this group are caused by the failures of non-safety-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 non-safety-related systems have a significant effect on risk, and there are no RTNSS candidates from this category.

19A.4.4.2 *At-Power Inadvertent Opening of a Relief Valve*

Safety/Relief Valves are safety-related. Therefore, they are not RTNSS candidates.

19A.4.4.3 *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, 2, and 3 are answered "Yes." The loss of feedwater is a significant contributor to CDF, so the feedwater and condensate systems are RTNSS candidates. However, 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 triplicate, 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.

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 considered a transient, which 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.4.4.4 *At-Power Loss of Preferred Power*

Loss of Preferred Power (LOPP) occurs as a result of severe weather, grid disturbances, transformer failures, or switchyard faults. Loss of preferred power 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 that comprise the onsite AC power distribution system are nonsafety-related, and thus, Questions 1, 2, and 3 are answered "Yes." The cumulative effects of Loss of preferred power are a significant contributor to CDF and LRF for at-power and shutdown risk. However, 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. Those components, controlled by the site organization, that prevent a loss of offsite power, such as substations, breakers, motor control centers, and protective relays, are much less risk-significant and below the threshold for RTNSS consideration. Therefore, the SSCs within the ESBWR design scope for preventing a loss of offsite power initiating event are not risk significant and do not warrant additional regulatory oversight.

Note that the onsite power generation does have RTNSS controls due to other criteria.

19A.4.4.5 *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.4.4.6 *Shutdown Loss of Preferred Power*

The causes and effects of loss of preferred (that is, offsite) power initiating event during shutdown are similar to at-power conditions, which were discussed previously.

19A.4.4.7 *Loss of Shutdown Cooling*

The decay heat removal function during shutdown modes of operation is provided by the Reactor Water Cleanup/Shutdown Cooling System (RWCU/SDCS) System operating in shutdown cooling mode. With the reactor well flooded, FAPCS may be used as an alternative.

If the reactor well is flooded, the risk associated with loss of decay heat removal is negligible because the large amount of water stored above the core assures long-term core cooling.

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 pump were to trip in this configuration, it would not initiate a loss of shutdown cooling event, and Questions 1, 2, and 3 are answered "No."

There are no RTNSS candidates for regulatory oversight.

19A.4.4.8 *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."

There are no RTNSS candidates from this category, although availability controls on the lower drywell hatches are provided.

19A.4.5 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 ECCS provides the level of protection necessary to meet both the CDF and LRF goals.

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 requirements for RTNSS.

In addition, the level 2 analysis includes assumptions on the design and performance of the BiMAC device, which is in the process of being analyzed and tested. Therefore, the BiMAC device is also a RTNSS candidate.

19A.5 CRITERION D: CONTAINMENT PERFORMANCE ASSESSMENT

The containment performance goal in SECY-93-087, Issue I.J is addressed in DCD Subsection 19.2.

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. Tier 2 Subsection 6.2.1.1.5 addresses the steam bypass of the suppression pool. Tier 2 Subsection 6.2.2.3 addresses the design of the Passive Containment Cooling Heat Exchanger tubes. The Criterion D safety concerns are addressed in the ESBWR design, and no RTNSS candidates are identified.

19A.6 CRITERION E: ASSESSMENT OF SIGNIFICANT ADVERSE INTERACTIONS

The concerns about adverse system interactions have been addressed for currently operating reactors as NRC Unresolved Safety Issue, Item A-17: SYSTEMS INTERACTIONS IN

NUCLEAR POWER PLANTS. Item A-17 acknowledges that systems interactions are usually well recognized and, therefore, are accounted for in the evaluation of plant safety by designers and in plant safety assessments. The concern is the potential for unrecognized subtle dependencies among SSCs to be unidentified and possibly lead to safety-significant events. The term used to describe these unrecognized, subtle dependencies is adverse systems interactions (ASIs). The NRC recommends that COL Holder not conduct broad searches specifically to identify all ASIs because such searches had not proved to be cost-effective in the past, and there was no guarantee after such studies that all ASIs had been uncovered.

19A.6.1 Systematic Approach

The purpose of the Criterion E analysis is to systematically evaluate adverse interactions between the active and passive systems. For the purpose of this analysis, an adverse systems interaction 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 ECCS passive safety 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 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 non-safety-related systems with a potential adverse effect are analyzed further as RTNSS candidates.

19A.6.1.1 *Gravity Driven Cooling System (GDCS)*

19A.6.1.1.1 Design Features

GDCS provides flow to the annulus region of the reactor through dedicated nozzles. 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

Containment, DC Power, Fuel and Auxiliary Pools Cooling System (FAPCS), Suppression Pool, Passive Containment Cooling System (PCCS)

19A.6.1.1.3 Analysis of Potential Adverse System Interactions

Squib valve and deluge valve initiation circuitry are powered by divisionally separated, safety-related, DC 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 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, and
- 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 safety-related, and are thus designed with adequate redundancy, as described in the DCD.

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. Failure of the HPNSS does not result in a loss of SRV function.

19A.6.1.2.2 System Interfaces

Main Steam, Containment, Suppression Pool, 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. The IC system 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 (IC/PCC) 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/PCC 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/PCC pool makeup clean water supply for replenishing level during normal plant operation is provided from FAPCS. A nonsafety-related independent FAPCS makeup line is provided to provide emergency makeup water into the IC/PCC 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 (IC system standby conditions), excess hydrogen from radiolytic decomposition or air entering into the reactor coolant from the feedwater does not accumulate in the IC steam supply line, thus assuring that the IC tubes are not blanketed with non-condensables when the system is first started.

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 IC reservoir and develops a level up to the steam distributor, above the upper headers. To start an IC 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 IC tube bundle moves downward below the lower headers to a point in the main condensate return line. The fail-open condensate return bypass valve opens if the DC power is lost.

19A.6.1.3.2 System Interfaces

Main Steam, Containment, Suppression Pool, FAPCS, DC Power, Process Radiation Monitoring

19A.6.1.3.3 Analysis of Potential Adverse System Interactions

The ICS and PCCS pools (IC/PCC) 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/PCC pools cooling and cleanup subsystem pump is automatically tripped on low water level in IC/PCC 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/PCC pools is maintained by automatic open/closure of the makeup water supply isolation valve.

Four radiation monitors are provided in the IC/PCC pool steam atmospheric exhaust passages for each IC train. They are shielded from all radiation sources other than the steam flow in the exhaust passages for a specific IC train. The radiation monitors are used to detect IC 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 IC 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 System (SLCS)*

19A.6.1.4.1 Design Features

SLCS 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 SLCS injection is required to be operable.

The design features of SLCS 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 Isolation Condenser/Passive Containment Cooling (IC/PCC) pool inventory not being replenished.

19A.6.1.5.2 System Interfaces

Containment, FAPCS, ICS, Suppression Pool

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.6.1.5.4 Monitoring Instrumentation

This is covered under the discussion above on actions required beyond 72 hours.

19A.7 SELECTION OF IMPORTANT NON-SAFETY SYSTEMS

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, D and E are based on deterministic analyses. RTNSS systems needed to meet Criterion C are based on PRA insights.

Systems identified as RTNSS are evaluated in the focused PRA sensitivity study to ensure that this combination of safety-related and non-safety related systems meets the safety goal guidelines. If the goals are met, PRA importance studies are then performed to determine the risk-significance of these systems. The risk significance is then used to determine the appropriate regulatory treatment for the system.

Results of the regulatory treatment assessment are summarized in Table 19A-2.

19A.8 PROPOSED REGULATORY OVERSIGHT

19A.8.1 Regulatory Oversight

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. 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 should be 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 Control Manual.

Support – These systems have low risk significance 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 Control Manual.

19A.8.2 Reliability Assurance

All RTNSS systems shall be in the scope of the Design Reliability Assurance Program, as directed by DCD Tier 2 Chapter 17, which will be incorporated into the Maintenance Rule program.

19A.8.3 Augmented Design Standards

Systems that meet RTNSS Criterion B (that is, for actions required beyond 72 hours) require augmented design standards to assure reliable performance in the event of hazards, such as seismic events, high winds, and flooding. These standards are applied to High and Low Regulatory Oversight systems that meet Criterion B.

A RTNSS system classified as B1 or B2 that is required to function following a seismic event requires an augmented seismic design criterion. For B1 SSCs, the design is performed in accordance with Seismic Category II. B2 SSCs are designed for seismic requirements consistent with the International Building Code (IBC) – 2003 by International Code Council, Inc. (300-214-4321). The building structures are classified as Category IV (Power Generating Stations) with an Occupancy Importance Factor of 1.5. Either of the methods permitted by the IBC, simplified analysis or dynamic analysis, is acceptable for determination of seismic loads on NS structures and equipment including those designated as RTNSS. 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.

In addition to seismic standards, all Criterion B systems must meet design standards to withstand winds and missiles generated from category 5 hurricanes. As with seismic, the systems do not need to perform their functions during the high wind event, but must be available following the event. Fire events are sufficiently addressed with the current regulatory standards, so no additional controls are applied.

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 SSC 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 SSC from the effects of the PMF and PMP.

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.

19A.8.4 Regulatory Treatment

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

19A.8.4.1 *Alternate Rod Insertion (ARI)*

This function is RTNSS based on the requirements of Criterion A relative to the ATWS Rule, 10 CFR 50.62. The ARI function does not have a high risk significance due to the redundancy and diversity of the reactor protection system. The proposed level of regulatory oversight for this function should be in the Availability Control Manual.

19A.8.4.2 *Standby Liquid Control System Actuation for ATWS*

This function is RTNSS based on requirements of Criterion A relative to the ATWS Rule, 10 CFR 50.62. The SLCS function does not have a high risk significance due to the redundancy and diversity of the reactor protection system. The proposed level of regulatory oversight for this function should be in the Availability Control Manual.

19A.8.4.3 *Feedwater Runback Logic*

This function is also RTNSS based on the requirements of Criterion A relative to the ATWS Rule, 10 CFR 50.62. The feedwater runback logic provides a quick power reduction in response to ATWS conditions. This function, however, does not have a high risk significance due to the redundancy and diversity of the reactor protection system. The proposed level of regulatory oversight for this function should be in the Availability Control Manual.

19A.8.4.4 *Diesel-Driven Makeup Pump and Dedicated Connection for FPS Makeup*

The diesel-driven makeup pump is considered for RTNSS in accordance with Criterion B1, long-term actions required beyond 72 hours to ensure safe shutdown conditions. The pump and the FPS piping and valves are classified as nonsafety-related but are designed so that 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 diesel-driven pump, the dedicated connection for FPS makeup includes 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 FAPCS. FPS makeup to the IC/PCC pools is a candidate for regulatory oversight in accordance with Criterion B1, actions that are required beyond 72 hours to ensure safe shutdown conditions. When consideration is given to all safety-related and RTNSS equipment, 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 Control Manual.

19A.8.4.5 *Diverse Protection System*

Certain functions of DPS are significant with respect to the focused PRA sensitivity study to meet the NRC safety goal guidelines. DPS will provide diverse actuation functions that will enhance the plant's ability to mitigate dominant accident sequences involving the common cause failure of actuation logic or controls. 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 capability to manually actuate ECCS and containment isolations are contained in Technical Specifications.

19A.8.4.6 *Basemat-Internal Melt Arrest and Coolability System and GDCS Deluge Lines*

The BiMAC function has been developed to a conceptual level, with several design details that are not yet finalized. These details are needed to justify the target failure probability of less than 1.0 E-3. BiMAC plays an important role in mitigating core melt scenarios. Therefore, it is a candidate for RTNSS consideration. The BiMAC device functions during severe accidents, and thus has 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 line.

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 Control Manual.

19A.8.4.7 *Distributed Control and Instrumentation System*

The DCIS provides post-accident monitoring capability to give the operators more flexibility in responding to long term accident conditions. The monitoring is expected to be performed using the Q-DCIS system, so there would be no direct components covered by this category. Support systems needed to operate the Q-DCIS following depletion of the safety-related batteries are covered in this function. The proposed level of regulatory oversight for the RTNSS support of Q-DCIS is in the Availability Control Manual.

19A.8.4.8 *Fuel and Auxiliary Pool Cooling System*

Based on a review of the original PRA results, FAPCS can supply core cooling and containment heat removal in certain non-seismic PRA sequences in a backup capacity (that is, two 100% capacity trains.) Due to its expected importance in providing redundancy to core cooling and containment heat removal, 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 Control Manual.

19A.8.4.9 AC Power System

The Diesel Generators and PIP buses are required to provide power to support post-accident monitoring (Criterion B2), and for FAPCS in non-seismic PRA sequences (Criterion C.) The expected risk significance of the Diesel Generators and PIP buses in both applications does not challenge the CDF or LRF goals, and as such, the proposed level of regulatory oversight for this function is in the Availability Control Manual.

19A.8.4.10 *Component Cooling – HVAC, Cooling Water, Chilled Water, and Plant Service Water*

In order to support post-accident monitoring beyond 72 hours and FAPCS operation, it is necessary to provide component cooling to the DCIS and FAPCS components. Component cooling will be performed by the HVAC systems in the Reactor Building, Electrical Building, Fuel Building, Control Building, and parts of the Turbine Building. In addition, support for HVAC is required from AC power and cooling from Reactor Component Cooling Water, and Plant Service Water. 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 Control Manual addresses degraded or lost support systems in the context of the supported functions. No explicit availability controls are supplied for these support systems.

19A.8.4.11 *Long-Term Containment Integrity*

The basis of the severe accident analysis assumes that the containment is inerted. Maintaining containment oxygen concentration within the specified limit provides defense-in-depth for severe accidents that could result in combustible gas that could threaten containment integrity. This is not risk-significant and the proposed regulatory oversight is in the Availability Control Manual.

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 Control Manual.

19A.8.4.13 Control Room Habitability – Long-Term Ventilation

The portable AC generator that provides power to the Control Room Habitability Area ventilation is not risk-significant and the proposed regulatory oversight is in the Availability Control Manual.

19A.8.5 COL Information

None

19A.8.6 References

None

Table 19A-1
Initiating Events Assessment for RTNSS (Deleted)

Table 19A-2
RTNSS Systems

Table System	Function	RTNSS Criterion	Regulatory Treatment
ARI	Automatically depressurize scram header on ATWS signal.	A	LRO
BiMAC	Provide core debris cooling in LDW through deluge valves.	C	LRO
CB HVAC	Provide post 72-hour cooling for DCIS and Control Room habitability.	B2	Support
Chilled Water System	Provide post 72-hour cooling for HVAC. Provide cooling support for FAPCS.	B2 C	Support Support
Control Room Area Ventilation	Portable Generator for post 72-hour ventilation	B1	LRO
Diesel Fire Pump	Provide post 72-hour refill to PC/ICC and Spent Fuel pools.	B1	LRO
Diesel Generators	Provide power for post accident monitoring Provide power for FAPCS and support systems. (Non-seismic PRA sequences.)	B2 C	LRO LRO
DPS	Diverse actuation of ECCS functions.	C	HRO
Drywell Hatches	Provide boundary for recovering vessel level following a Shutdown LOCA below top of fuel event	C	LRO
EB HVAC	Provide post 72-hour cooling for DGs and 1E Electrical Distribution. Provide support for electrical power to FAPCS.	B2 C	Support Support
External Connection	Provide post 7-day refill to PC/ICC and Spent Fuel pools.	B1	LRO
FAPCS	Suppression pool cooling and low pressure coolant injection modes. (Non-seismic PRA sequences.)	C	LRO
FB HVAC	Provide cooling support for FAPCS.	C	Support
Feedwater Runback	Run FW demand to minimum on ATWS signal.	A	LRO
PAM Instruments (DCIS)	Provide post accident monitoring (use RG 1.97 to determine scope.)	B2	LRO

Table 19A-2
RTNSS Systems

Table System	Function	RTNSS Criterion	Regulatory Treatment
PIP Buses	Provides post 72-hour AC power from standby diesel generators to support Post-Accident Monitoring, and FAPCS.	B2 C	Support Support
PSW	Provide post 72-hour cooling for RCCWS. Provide cooling support for FAPCS.	B2 C	Support Support
RB HVAC	Provide post 72-hour cooling for DCIS.	B2	Support
RCCWS	Provide post 72-hour cooling for Chillers and DGs. Provide cooling support for FAPCS.	B2 C	Support Support
SLCS Actuation	Backup actuation logic to initiate SLCS and isolate RWCU/SDC.	A	LRO
TB HVAC	Provide post 72-hour cooling for DCIS in Turbine Building. Provide room cooling for RCCW pumps.	B2 C	Support Support

19ACM AVAILABILITY CONTROLS MANUAL

TABLE OF CONTENTS

19ACM AVAILABILITY CONTROLS MANUAL

TABLE OF CONTENTS

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; and

- NOTE -

ACLCO 3.0.3.b shall be completed if ACLCO 3.0.3 is entered.

b. 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;

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

ACLCO Applicability

ACLCO 3.0.4 (continued)

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 3.0.5 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) are 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, and b) 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.

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

BASES

ACLCO 3.0.4 (continued)

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. 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.

BASES

ACLCO 3.0.4 (continued)

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.

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 ACSR(s) 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.

Upon completion of maintenance, appropriate post maintenance testing is required to declare equipment AVAILABLE. This includes ensuring

BASES

ACSR 3.0.1 (continued)

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 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

BASES

ACSR 3.0.2 (continued)

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 ACSR(s) 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 ACSR(s) since the requirement for the ACSR(s) 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. ACRS 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 condition(s) 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 ARI function of the air header dump valves in the Control Rod Drive (CRD) System shall be AVAILABLE.

APPLICABILITY: MODES 1 and 2.

ACTIONS

CONDITION	REQUIRED ACTION		COMPLETION TIME
A. The ARI function of one or more CRD System air header dump valves unavailable.	A.1	Restore CRD System air header dump 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, "Nuclear Monitoring System (NMS) Instrumentation," Table 3.3.1.4-1, for Functions 1.a, 1.b, and 1.c are applicable.	In accordance with applicable SRs

SURVEILLANCE		FREQUENCY
ACSR 3.3.1.2	Verify each CRD System air header dump 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 for each required ARI Function automatic actuation division.	24 months on a STAGGERED TEST BASIS

ACM B 3.3.1 INSTRUMENTATION

AC B 3.3.1 Alternate Rod Insertion (ARI)

BASES

This Availability Control (AC) addresses AVAILABILITY of the Alternate Rod Insertion (ARI) function of the air header dump 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). The DPS generates the signal; to open the ARI (air header dump) valves in the CRD system on any of the following signals: 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.

Operability and surveillance testing of Reactor Protection System (RPS) and Nuclear Monitoring System (NMS) instrumentation providing signals to the ARI function are addressed in Technical Specifications (TS) Limiting Conditions for Operation (LCO) 3.3.1.1, "Reactor Protection System (RPS) Instrumentation," and LCO 3.3.1.4, "Nuclear Monitoring System (NMS) Instrumentation."

ACM 3.3 INSTRUMENTATION

AC 3.3.2 Anticipated Transient Without Scram (ATWS) / Standby Liquid Control (SLC) System Actuation

ACLCO 3.3.2 The SLC System actuation function of the ATWS/SLC logic shall be AVAILABLE.

APPLICABILITY: MODES 1 and 2.

ACTIONS

CONDITION	REQUIRED ACTION	COMPLETION TIME
A. SLC actuation function of the ATWS/SLC logic unavailable.	A.1 Restore SLC actuation function of the ATWS/SLC logic 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	Perform LOGIC SYSTEM FUNCTIONAL TEST for each required SLC actuation function of the ATWS/SLC automatic actuation division.	24 months on a STAGGERED TEST BASIS

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." Operability of the instrumentation sensors is addressed in TS 3.3.1.1, "Reactor Protection System (RPS) Instrumentation." This Availability Control addresses only the actuation logic associated with the ATWS/SLC actuation of SLC for diverse backup reactor shutdown, and includes isolation of RWCU/SDC on ATWS/SLC initiation.

There is an ATWS logic processor in each of four divisional Reactor Trip and Isolation Function (RTIF) cabinets. The ATWS logic processors are separate and diverse from RPS circuitry. Each ATWS 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.

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.

The ATWS/SLC logic also provides a feedwater run-back signal to attenuate power excursions. This function is addressed in Availability Control 3.3.3, "Feedwater Runback (FWRB)."

The ATWS/SLC actuation 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 3.3.3 Feedwater Runback (FWRB)

ACLCO 3.3.3 The FWRB function shall be AVAILABLE.

APPLICABILITY: MODE 1

ACTIONS

CONDITION	REQUIRED ACTION	COMPLETION TIME
A. FWRB function unavailable.	A.1 Restore FWRB 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 FWRB function actuation on receipt of an actual or simulated actuation signal.	24 months
ACSR 3.3.3.2	Perform LOGIC SYSTEM FUNCTIONAL TEST for each required FWRB function automatic actuation division.	24 months on a STAGGERED TEST BASIS

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. The Feedwater Control System (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 upon receipt of an ATWS trip signal from the Anticipated Transient Without Scram/Standby Liquid Control (ATWS/SLC) logic. Operability of the instrumentation sensors is addressed in TS 3.3.1.1, "Reactor Protection System (RPS) Instrumentation." This Availability Control addresses the ATWS/SLC actuation logic and FWCS components associated with the FWRB function.

There is an ATWS logic processor in each of four divisional Reactor Trip and isolation Function (RTIF) cabinets. The ATWS logic processors are separate and diverse from Reactor Protection System (RPS) circuitry. Each ATWS 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 feedwater runback.

Automatic initiation of the FWRB occurs on persistent high power with a Selected Control Rod Run-In (SCRRI) command issued, persistent high power following an RPS scram demand, or High RPV dome pressure with a Startup Range Neutron Monitor (SRNM) ATWS permissive.

The ATWS/SLC logic also provides actuation of the Standby Liquid Control (SLC) System for diverse backup reactor shutdown. This function is addressed in Availability Control 3.3.2, " Anticipated Transient Without Scram (ATWS)/Standby Liquid Control (SLC) System Actuation."

The FWRB 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 3.3.4 Post Accident Monitoring (PAM) Instrumentation

ACLCO 3.3.4 Two PAM instrumentation channels for each critical safety function required by FSAR Section 7.5.1 shall be AVAILABLE.

APPLICABILITY: MODES 1 and 2.

ACTIONS

- NOTE -

Separate Condition entry is allowed for each critical safety function.

CONDITION	REQUIRED ACTION	COMPLETION TIME
A. One or more critical safety functions with one required channel unavailable.	A.1 Restore required channel to AVAILABLE status.	30 days
B. One or more critical safety functions with two required channels unavailable.	B.1 Restore one required channel to AVAILABLE status.	7 days
C. Required Action and associated Completion Time not met.	C.1 Enter ACLCO 3.0.3.	Immediately

SURVEILLANCE REQUIREMENTS

SURVEILLANCE		FREQUENCY
ACSR 3.3.4.1	Perform CHANNEL CHECK on each required channel.	31 days
ACSR 3.3.4.2	Perform CHANNEL CALIBRATION on each required channel.	24 months

ACM B 3.3 INSTRUMENTATION

AC B 3.3.4 Post-Accident Monitoring (PAM) Instrumentation

BASES

The PAM Variable List is prepared as a separate document utilizing inputs from the design process, licensing design basis, and HFE process; including the development of the Emergency Procedure Guidelines (EPGs) and/or Plant Specific Emergency Operating Procedures (EOPs) and Abnormal Operating Procedures (AOPs). The PAM variable list document provides summary information for each PAM variable as applicable (Reference FSAR Section 7.5.1).

For accident monitoring instrumentation associated with critical safety functions and powered from the safety-related sources, the safety-related Distributed Control and Information System (Q-DCIS) provides the required signal path to process this information. This information is then displayed on Q-DCIS divisional safety-related displays. The safety-related information can also be transmitted via isolated safety-related gateways to the nonsafety-related Distributed Control and Information System (N-DCIS) for input to nonsafety-related displays, plant computer functions and the Alarm Management System. Type A, Type B, and Type C variables are powered from safety-related sources.

The PAM instrumentation 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 3.3.5 Automatic Depressurization System (ADS) Inhibit

ACLCO 3.3.5 The ADS Inhibit function shall be AVAILABLE.

APPLICABILITY: MODES 1 and 2

ACTIONS

CONDITION	REQUIRED ACTION	COMPLETION TIME
A. ADS Inhibit function unavailable.	A.1 Restore ADS Inhibit 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 3.3.5.1	Verify ADS Inhibit function actuation on receipt of an actual or simulated actuation signal.	24 months
ACSR 3.3.5.2	Perform LOGIC SYSTEM FUNCTIONAL TEST for each required ADS Inhibit function automatic actuation division.	24 months on a STAGGERED TEST BASIS

ACM 3.3 INSTRUMENTATION

AC B 3.3.5 Automatic Depressurization System (ADS) Inhibit

BASES

For Anticipated Transient Without Scram (ATWS) mitigation, the ADS, which is part of the Nuclear Boiler System (NBS), is inhibited automatically. Automatic initiation of ADS is inhibited 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).

- A coincident high RPV pressure and APRM ATWS permissive signal that persists for 60 seconds.

MCR switches manually inhibit the ADS under ATWS conditions.

There is an ATWS logic processor in each of four divisional Reactor Trip and isolation Function (RTIF) cabinets. The ATWS logic processors are separate and diverse from Reactor Protection System (RPS) circuitry. Each ATWS 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 ADS inhibit.

The ADS Inhibit supports proper operation of the Standby Liquid Control (SLC) System for diverse backup reactor shutdown. This function is addressed in Availability Control 3.3.2, " Anticipated Transient Without Scram (ATWS)/Standby Liquid Control (SLC) System Actuation."

The ADS Inhibit function is a nonsafety-related function supporting the assumed performance of SLCS which 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.

ACLCO 3.5.1 Two 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	---------- **- 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
ACSR 3.5.1.2	---------- **- NOTE -** Squib actuation may be excluded. ---------- Verify required deluge valves actuate on an actual or simulated automatic initiation signal.	24 months

SURVEILLANCE		FREQUENCY
ACSR 3.5.1.3	Perform LOGIC SYSTEM FUNCTIONAL TEST for each required Deluge automatic actuation division.	24 months on a STAGGERED TEST BASIS
ACSR 3.5.1.4	-- **- NOTE -** Squib actuation may be excluded. -- Verify the flow path for each deluge line is not obstructed.	10 years

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 provide 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 two 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."

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.

ACM 3.6 CONTAINMENT SYSTEMS

AC 3.6.1 Containment Oxygen

ACLCO 3.6.1 Containment oxygen concentration shall be < 4.0 volume percent.

APPLICABILITY: MODE 1.

ACTIONS

- NOTE -

ACLCO 3.0.4.c is applicable.

CONDITION	REQUIRED ACTION	COMPLETION TIME
A. Containment oxygen concentration ≥ 4 volume percent.	A.1 Restore containment oxygen concentration to < 4 volume percent.	24 hours
B. Required Action and associated Completion Time not met.	B.1 Enter ACLCO 3.0.3.	Immediately

SURVEILLANCE REQUIREMENTS

SURVEILLANCE	FREQUENCY
ACSR 3.6.1.1 Verify containment oxygen concentration is < 4 volume percent.	7 days

ACM B 3.6 CONTAINMENT SYSTEMS

AC B 3.6.1 Containment Oxygen

BASES

For the Design Basis Accident (DBA), the generation of post accident oxygen would not result in a combustible gas condition and a design basis Loss-of-Coolant Accident (LOCA) does not have to be considered in this regard. However, the basis of the severe accident analysis assumes that the containment is inert. Maintaining containment oxygen within the specified limit provides defense-in-depth for beyond design basis events that could result in combustible gas mixtures that could threaten containment integrity and lead to offsite radiological releases.[CWS113]

Intentional Entry into Condition A and the associated Required Action is permitted during the reactor startup and shutdown process.[CWS114]

The Containment Oxygen function is a nonsafety-related function that supports the containment inerting assumption of the severe accident analysis, and therefore enhanced 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 Lower Drywell Hatches

ACLCO 3.6.2 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 3.6.2.1	Verify lower drywell hatch administrative closure plan is in place.	12 hours
ACSR 3.6.2.2	Verify lower drywell equipment hatch can be secured closed.	30 days
ACSR 3.6.2.3	Verify lower drywell personnel airlock can be secured closed.	30 days

ACM B 3.6 CONTAINMENT SYSTEMS

AC B 3.6.2 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 and instrument lines and 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 3.6.3 Passive Autocatalytic Recombiners (PARs)

ACLCO 3.6.3 {Two} PARs shall be AVAILABLE.

APPLICABILITY: {MODE 1.}

ACTIONS

CONDITION	REQUIRED ACTION		COMPLETION TIME
A. {One} PAR unavailable.	A.1	Restore PAR to AVAILABLE status.	{30 days}
{B. Two or more PARs unavailable.	B.1	Verify by administrative means that the hydrogen control function is maintained.	1 hour AND Once per 12 hours thereafter
	AND		
	B.2	Restore one PAR 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	Visually examine each PAR and verify there is no evidence of abnormal conditions.	24 months

ACM B 3.6 CONTAINMENT SYSTEMS

AC B 3.6.3 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 sever 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 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 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.	A.1	Restore required diesel-driven firewater pump to AVAILABLE status.	7 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.	 31 days
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 (1.03×10^6 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 (IC/PCC) Pools Makeup Water – Emergency Makeup	1,2
2. Spent Fuel Pool (SFP) - Emergency Makeup Water	When spent fuel assemblies are stored in the SFP
3. Low Pressure Coolant Injection (LPCI) - Emergency Makeup	6[(a)]

(a) With the new fuel pool gate removed and water level ≥ 7.01 meters (23.0 feet) over the top of the reactor pressure vessel flange.

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 (IC/PCC) 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 and to offsite water sources. The required volume from 72 hours through 7 days is approximately 3,900 m^3 (138,000 ft^3), and the maximum required delivery rate is approximately 46 m^3/hr (200 gpm) at 72 hours.

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. The required volume from 72 hours through 7 days is approximately 1921 m^3 (67,840 ft^3).

In conjunction with the diesel-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 firewater pump in the FPE to the desired flow path. The two firewater storage tanks are required to contain a total volume of ≥ 3900 m^3 (1.03×10^6 gallons) of water to ensure a sufficient quantity of emergency makeup is available.

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 One Fuel and Auxiliary Pools Cooling System (FAPCS) train shall be AVAILABLE.

APPLICABILITY: MODES 1, 2, 3, and 4.

ACTIONS

CONDITION	REQUIRED ACTION	COMPLETION TIME
A. Required FAPCS train unavailable.	A.1 Restore required FAPCS train 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 3.7.2.1	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.	7 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
	<u>AND</u>	
	C.1 Initiate action to suspend operations with a potential for draining the reactor vessel (OPDRVs).	Immediately
	<u>AND</u>	
	C.2 Initiate action to restore Reactor Building to OPERABLE status.	Immediately

ACM 3.7 PLANT SYSTEMS

AC 3.7.3 Fuel and Auxiliary Pools Cooling System (FAPCS) - Shutdown

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 AC 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 B and then Feedwater loop A. 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 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 3.7.4 Spent Fuel Pool (SFP) Water Level

ACLCO 3.7.4 The SFP water level shall be ≥ 8.5 m (27.9 ft) over the top of irradiated fuel assemblies seated in the spent fuel storage pool.

APPLICABILITY: When spent fuel assemblies are stored in the SFP.

ACTIONS

CONDITION	REQUIRED ACTION	COMPLETION TIME
A. SFP water level not within limit.	A.1 Restore SFP water level to within limit.	24 hours
B. Required Action and associated Completion Time not met.	B.1 Enter ACLCO 3.0.3.	Immediately

SURVEILLANCE REQUIREMENTS

SURVEILLANCE	FREQUENCY
ACSR 3.7.4.1 Verify SFP water level within limits.	31 days

ACM B 3.7 PLANT SYSTEMS

AC B 3.7.4 Spent Fuel Pool (SFP) Water Level

BASES

The SFP is designed to dissipate fuel decay heat through heat up and boiling of the pool water during a loss of the Fuel and Auxiliary Pools Cooling System (FAPCS) trains. Steam generated by boiling of the SFP is released to the atmosphere through a relief panel in the Fuel Building. Water inventory in the SFP is adequate to keep the fuel covered through 72 hours, thereby avoiding heat up of the fuel and the potential for fission product release.

Sufficient reserve capacity is maintained on-site 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 and to offsite water sources.

This function is a nonsafety-related function that provides a significant passive heat sink in the loss of SFP cooling analysis satisfies the significance criteria for Regulatory Treatment of Non-Safety Systems, and therefore requires 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 3.8 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 ≥ {[ ] l ([ ] gal}.	31 days
ACSR 3.8.1.2	Verify that the required standby diesel generator starts and operates at ≥ [4000] kw for ≥ 1 hour.	92 days

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. <u>AND</u> C.1 Initiate action to suspend operations with a potential for draining the reactor vessel (OPDRVs). <u>AND</u> C.2 Initiate action to restore Reactor Building to OPERABLE status.	Immediately Immediately Immediately

SURVEILLANCE REQUIREMENTS

SURVEILLANCE		FREQUENCY
ACSR 3.8.2.1	Verify that the fuel oil volume in the required standby diesel generator fuel tank is ≥ {[ ] l ([ ] gal}.	31 days
ACSR 3.8.2.2	Verify that the required standby diesel generator starts and operates at ≥ [1000] kw for ≥ 1 hour.	92 days

ACM B 3.8 ELECTRICAL POWER SYSTEMS

AC B 3.8.1 / B 3.8.2 Standby Diesel Generators

BASES

The Diesel Generators (DGs) are required to provide power for recharging batteries to support post-accident monitoring (i.e., [RTNSS] Criterion B), and for Fuel and Auxiliary Pools Cooling System (FAPCS) in non-seismic PRA sequences (i.e., [RTNSS] Criterion C). No DG-derived AC power is required for 72 hours after an abnormal event. In addition, the DGs 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 DG 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 DG is required to be AVAILABLE during MODES 1, 2, 3, and 4 to support FAPCS and the ability to recharge batteries to support post-accident monitoring.} Two DGs 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 DGs 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.

DG starts required by ACSR 3.8.1.2 and ACSR 3.8.2.2 may be preceded by an engine prelube period to minimize wear and tear on the DGs during testing. For the purpose of this testing, the DGs 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 3.8.1.2 and ACSR 3.8.2.2 also demonstrates OPERABILITY of the associated fuel oil transfer pump and necessary DG support system function(s).

ACM 3.8 ELECTRICAL POWER SYSTEMS

AC 3.8.3 Control Room Habitability Area (CRHA) Heating, Ventilation, and Air Conditioning (HVAC) Subsystem (CRHAVS) Portable Generator

ACLCO 3.8.3 The CRHAVS portable generator shall be AVAILABLE.

APPLICABILITY: MODES 1, 2, 3, 4, 5, and 6.

ACTIONS

CONDITION	REQUIRED ACTION	COMPLETION TIME
A. CRHAVS portable generator unavailable.	A.1 Restore CRHAVS portable generator 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 3.8.3.1	Verify that the fuel volume of ≥ {[ ] m^3 ([ ] gal} is AVAILABLE for the required RCHAVS portable generator.	31 days
ACSR 3.8.3.2	Verify that the required CRHAVS portable generator starts and operates at ≥ {[2] kw} for ≥ 1 hour.	92 days

ACM B 3.8 ELECTRICAL POWER SYSTEM

AC B 3.8.3 Control Room Habitability Area (CRHA) Heating, Ventilation, and Air Conditioning (HVAC) Subsystem (CRHAVS) Portable Generator

BASES

The CRHAVS design maintains a habitable control room under accident conditions by providing adequate radiation protection and breathing air. Upon a loss of power, the remaining nonsafety-related heat loads are dissipated for 2 hours using battery power, and the remaining safety-related heat loads are passively dissipated by the walls, floor, ceiling and interior walls for the remainder of the 72 hour passive duration. The CRHAVS portable generator is required to support operation of the Control Room Emergency Filtration Unit (EFU) fans beyond 72 hours through 7 days.

The CRHAVS portable 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.

{CRHAVS portable generator starts required by ACSR 3.8.3.2 may be preceded by an engine prelube period to minimize wear and tear on the generator 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 Sacrificial Refractory Layer

The BiMAC is designed and shall be maintained with a refractory 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 plate 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 at approximately 10° from horizontal to permit natural circulation flow.

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); and
- 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 0.987 MPaG (143 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.

19B.2 RCCV AND LINERS

19B.2.1 Analysis Methods

A deterministic analysis is performed to demonstrate Level C pressure capability of the RCCV (Reinforced Concrete Containment Vessel) 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 MPa (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 MPa (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 0.987 MPaG (143 psig) or 3.18 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

The analysis is completed to a load factor of 3.5 times design pressure or an equivalent internal pressure of 1.085 MPaG (157.5 psig). 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 4 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 where the temperature is at ambient levels. 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. 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. Figure 19B-5 plots the maximum principal strain versus pressure at representative elements for these critical locations, identified as points A, B and C in the figure. 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. This plot shows that the liner at the connection with the suppression pool slab (Point B) meets the ASME factored load limit of 0.3% membrane strain at 0.987 MPaG (143 psig) pressure corresponding to 100% fuel clad-coolant reaction. Point C is a representative typical location for the liner at the connection with the top slab, and Point A is at a local concentration that develops at the locations where the upper pool girders connect to the top slab. Figure 19B-6 plots the maximum principal (EP2) and plastic (PEEQ) strains at this local concentration in the RCCV wall liner at the top slab connection. Yielding of the liner at this local concentration just starts at the 0.62 MpaG (90 psig) pressure level. At an internal pressure of 0.987 MpaG (143 psig) or 3.18 P_d, the plastic strain in the liner for this location reaches 0.72%. While this exceeds the ASME factored load limit, this value is still on the shoulder of the stress-strain curve, as illustrated in Figure 19B-7. This level of plastic strain is well below the ductility limit, even considering substantial strain concentration factors, and, in addition, this strain is due to a localized effect.

Furthermore, because the liner will undergo compression when exposed to the temperatures that accompany this accident pressure, the level of membrane tension strain will be reduced. When thermal-induced stresses are also included, the maximum liner strain at this location reduces to 0.25% at 0.987 MpaG(143 psig), as illustrated in Figure 19B-8. Thus, if the thermal stress is included, then the liner strain is within the factored load limit even at the local concentration for the 100% fuel clad-coolant reaction pressure. Thus, it is demonstrated through the nonlinear analysis that the liner remains a leak tight barrier for 0.987 MPaG(143 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 0.39%, 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 0.987 MPaG (143 psig) pressure. The liner strains including thermal effects are within the factored load allowable at 0.987 MPaG (143 psig). Some slight yielding of rebar develops at the 0.987 MPaG (143 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 can be determined from the fragility analysis described in Appendix 19C, which includes the thermal stress for the 260°C (500°F) steady state thermal condition. Using $\beta = -2.33$, a 99% confidence level for the pressure capacity for the RCCV and liner system is determined to be 1.185 MPaG (172 psig). It is also noted that the fragility analysis determined that the 99% confidence level for leakage at the bolted flange connection of the drywell head is a pressure level of 1.097 MPaG (159 psig).

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:

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

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 severest 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 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 finite element model for the torispherical head including the top flange is shown in Figure 19B-9. This analysis was conducted before the latest revision to strengthen the bolted flange connection using thicker flanges and the tapered shell sections connecting to the flanges. However, this change will have very little affect on the buckling analysis because the buckling analysis assumes that the top flange is fixed. The critical areas are in the knuckle region above the tapered shell section and in the apex of the dome region where the shell thickness is unchanged at 40 mm.

The first step in the analysis is to confirm and demonstrate that the torishperical 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 thickness of the shell elements in the analysis model was reduced so that the 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-10 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-11 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. The analysis uses the lower bound or design values for the steel properties, namely yield strength = 262 MPa (38 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 an ambient temperature of 15.5°C (60°F) and includes the external hydrostatic pressure of the water on the top of the head. Figure 19B-12 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 using the BOSOR 5 computer program 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 axisymmtric 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-13 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 14, the ductility limit of 8% strain is reached and rupture of the dome will occur.

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 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 1 or 2 locations around the shell surface, as found in Reference 19B-6, a cosine type shape with 6 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. In addition, an analysis was also performed using the perfect geometry but considering a temperature of 171°C (340°F) to evaluate the effect of elevated temperature on the pressure capacity. This analysis assumed that the drywell head is free to expand with temperature and that the elevated temperature is uniform across the thickness. Thus, no thermal induced stress is present, and any effect on the pressure capacity is caused by reduction in the material properties.

Figure 19B-14 plots the mid-thickness plastic strain in the crown with increasing pressure for these three analysis cases, namely, perfect geometry at ambient temperature, imperfect geometry at ambient temperature, and perfect geometry at elevated temperature. The ductility limit for strain that will cause tearing of the head is also shown on the figure. The failure pressure for perfect geometry at ambient temperature is seen to be a load factor of 13.9 on the design pressure with a reduction to 13.2 P_d for the imposed imperfections. Note that the imposed imperfections did not trigger buckling response in the knuckle. For the perfect geometry at elevated temperature, a pressure of 12.4 P_d would cause tensile failure in the dome. 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 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 at temperature of 260 C (500 F) of the most critical component in the PCCS heat exchangers is 1.33 MPaG (193 psig).

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 1.033 MPaG (150 psig) associated with the lower flange plate of the drywell head anchorage. It is higher than 0.987 MPaG (143 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. 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 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

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			
.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
SA540-B24 Class 3 Bolting			
Yield Stress (MPa)	896.6	868.8	813.4
Tensile Strength (MPa)	1000.0	963.8	901.5
Elongation (%)	12.0	15.0	15.5

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

Table 19B-5
Summary of Thermal Material Properties

Material	Weight Density (MN/m^3)	Specific Heat (kcal/kg-°C)	Conductivity (kcal/hr-m-°C)
Concrete	0.0235	0.21	1.4
Carbon Steel Liner	0.0770	0.11	46.0
Stainless Steel Liner	0.0770	0.118	14.0
Structural Steel	0.0770	0.11	46.0

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

Location	Maximum Rebar Tension		Maximum Rebar Compression		Maximum Concrete Compression	
	Stress (MPa)	[1]Ratio to Allowable	Stress (MPa)	[1]Ratio to Allowable	Stress (MPa)	[2]Ratio to Allowable
Top Slab					-8.71	0.34
X-Bar Top	57.89	0.16	-20.84	0.06	On top surface under pool girder at RCCV wall	
X-Bar Bot	139.38	0.47	-53.08	0.18		
Y-Bar Top	75.05	0.20	-30.03	0.08		
Y-Bar Bot	157.25	0.53	-52.34	0.18		
RCCV Wall					-9.82	0.38
Vert In	186.54	0.63	-21.74	0.07	At bottom connection with SP slab	
Vert Out	40.35	0.11	-16.38	0.04		
Hoop In	23.98	0.08	-14.25	0.05		
Hoop Out	22.84	0.06	-6.44	0.02		
SP Slab					-7.00	0.27
Hoop Top	7.09	0.02	-3.84	0.01	On bottom surface at RCCV wall	
Hoop Bot	13.15	0.04	-			
Rad Top	29.12	0.10	-20.41	0.07		
Rad Bot	87.45	0.23	-33.6	0.09		
Pedestal Wall					-12.51	0.48
Vert In	6.66	0.02	-47.16	0.16	Outside surface at connection with basemat	
Vert Out	0.12	0.00	-64.61	0.17		
Hoop In	27.39	0.09	-10.88	0.04		
Hoop Out	22.52	0.06	-9.17	0.02		
Basemat					-5.88	0.28
Top Layers	13.07	0.04	-17.71	0.06	Top surface at pedestal wall, [27.6 MPa, (4 ksi) concrete]	
X-Bar Bot	120.56	0.32	-20.77	0.06		
Y-Bar Bot	117.15	0.31	-21.99	0.06		

[1]allowable is 90% of yield; for inner bars, yield = 327.5 MPa; for outer bars, yield = 413.8 MPa

[2]allowable is 75% of fc'; for inner surface, fc' = 25.91 MPa; for outer surface, fc' = 34.48 MPa

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

Location	Maximum Rebar Tension		Maximum Rebar Compression		Maximum Concrete Compression	
	Stress (MPa)	[1]Ratio to Allowable	Stress (MPa)	[1]Ratio to Allowable	Stress (MPa)	[2]Ratio to Allowable
Top Slab					-22.65	0.88
X-Bar Top	179.99	0.48	-42.15	0.11	.015% peak plastic strain in horizontal bars at connection with top slab at pool girders	
X-Bar Bot	344.54	1.17	-155.4	0.53		
Y-Bar Top	251.35	0.67	-37.12	0.10		
Y-Bar Bot	339.89	1.15	-160.91	0.55		
RCCV Wall					-24.39	0.94
Vert In	351.41	1.19	-33.02	0.11	.39% peak plastic strain in vertical bars at top slab under pool girder locations	
Vert Out	223.34	0.60	-33.72	0.09		
Hoop In	140.71	0.48	-29.74	0.10		
Hoop Out	168.86	0.45	-7.25	0.02		
SP Slab					-13.02	0.50
Hoop Top	4.85	0.02	-14.51	0.05		
Hoop Bot	79.69	0.21	-2.46	0.01		
Rad Top	142.82	0.48	-41.35	0.14		
Rad Bot	159.42	0.43	-53.74	0.14		
Pedestal Wall					-23.59	0.91
Vert In	72.63	0.25	-72.96	0.25		
Vert Out	5.97	0.02	-121.88	0.33		
Hoop In	77.34	0.26	-20.51	0.07		
Hoop Out	68.26	0.18	-21.27	0.06		
Basemat					-11.91	0.58
Top Layers	133.46	0.45	-41.46	0.14		
X-Bar Bot	283.92	0.76	-34.52	0.09		
Y-Bar Bot	297.3	0.80	-39.2	0.11		
[1]allowable is 90% of yield; for inner bars, yield = 327.5 MPa; for outer bars, yield = 413.8 MPa						
[2]allowable is 75% of fc'; for inner surface, fc' = 25.91 MPa; for outer surface, fc' = 34.48 MPa						

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)	344	344
Buckling Pressure (MPa)	0.731	0.738

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

Part		**Calculated Pressure Capability (MPaG)**
Sleeve		2.036
Torispherical head		1.369
Bolted Flange	Hub/Flange	1.204
	Flange Bolt	2.550
Anchor Structure	Inside Flange Plate	1.033
	Inside Gusset Plate	1.194
	Concrete	1.224

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

Component	Part		Calculated Pressure Capability (MPaG)
Equipment Hatch	Sleeve		2.817
	Head		3.544
	Bolted Flange	Flange	1.190
		Bracket	1.722
		Flange Bolt	2.556
	Anchor Structure	Inside Flange Plate	1.768
		Inside Gusset Plate	1.047
		Concrete	3.383
Personnel Airlock	Sleeve		2.817
	Sidewall		1.078
	Anchor Structure	Inside Flange Plate	1.768
		Inside Gusset Plate	1.570
		Concrete	3.383
Wetwell Hatch	Sleeve		3.375
	Head		4.251
	Bolted Flange	Flange	1.333
		Bracket	1.411
		Flange Bolt	2.821
	Anchor Structure	Inside Flange Plate	2.140
		Inside Gusset Plate	1.499
		Concrete	3.924

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

Component	Pressure (MPa), gauge
RCCV and Liners	1.185
Drywell Head	1.033
Hatches and Airlocks	1.047
Penetrations	3.38
PCCS Heat Exchangers	1.33

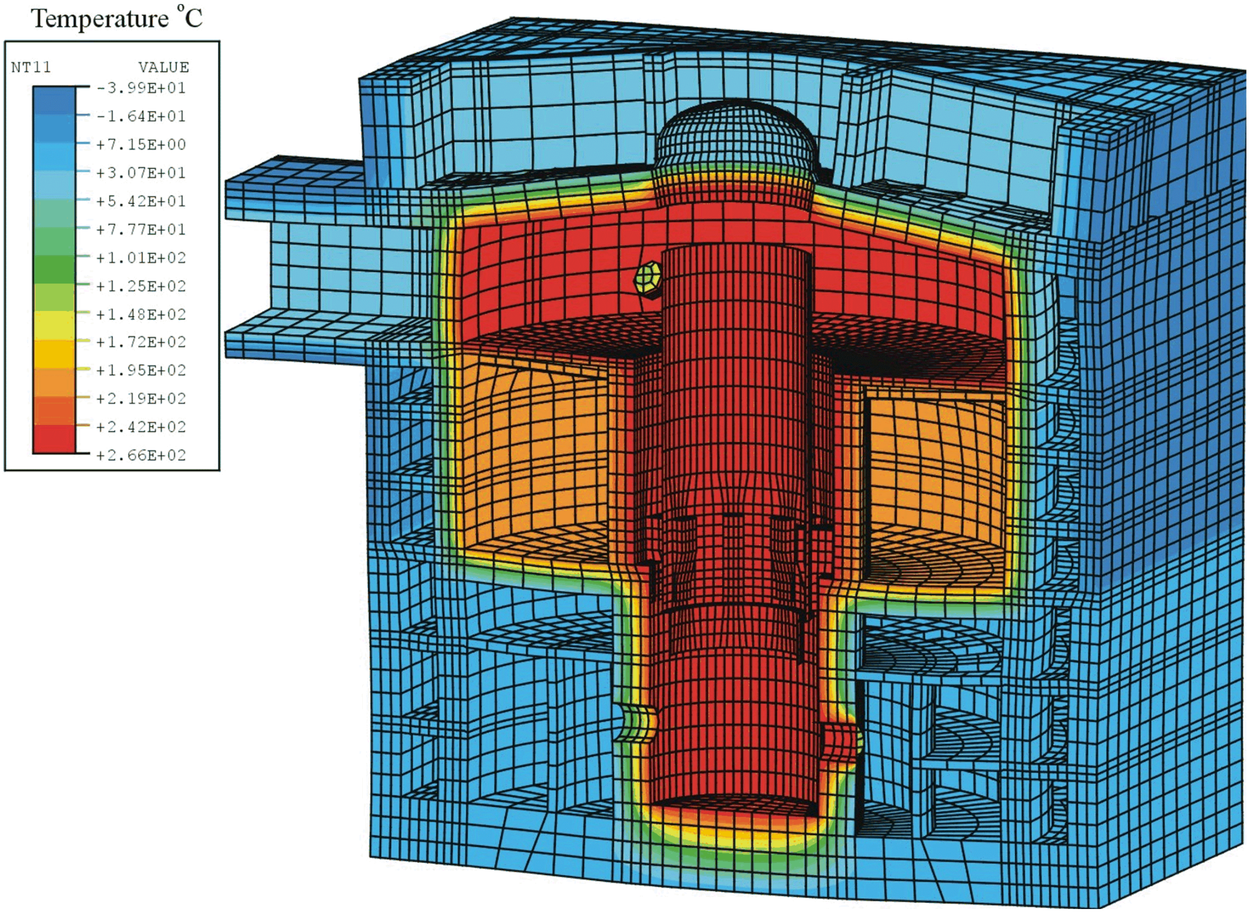


Figure 19B-1. Finite Element Model Showing Steady State Thermal Condition

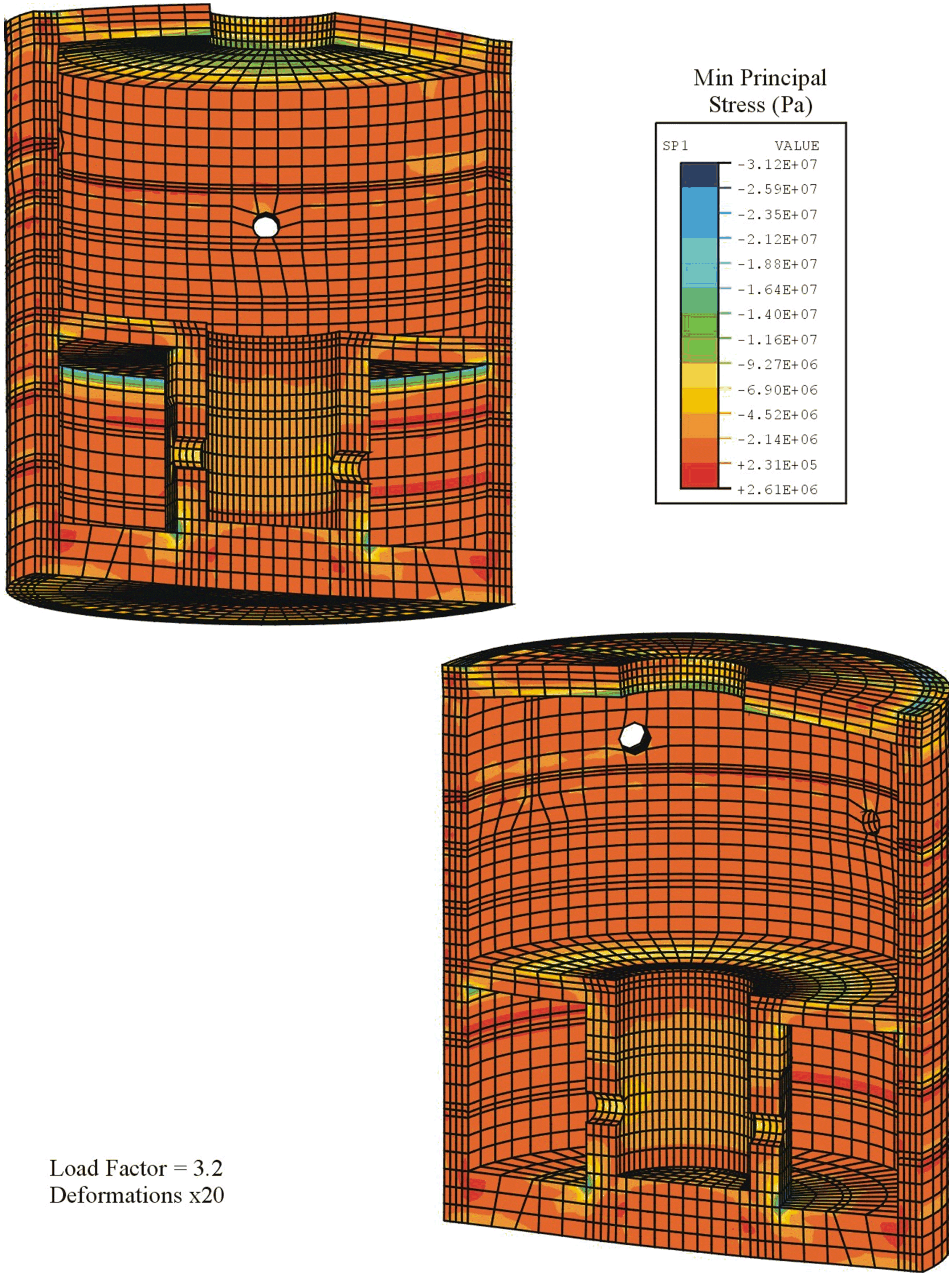


Figure 19B-2. Concrete Compressive Stress, Level C Analysis, 0.992 MPaG (144 psig) Pressure

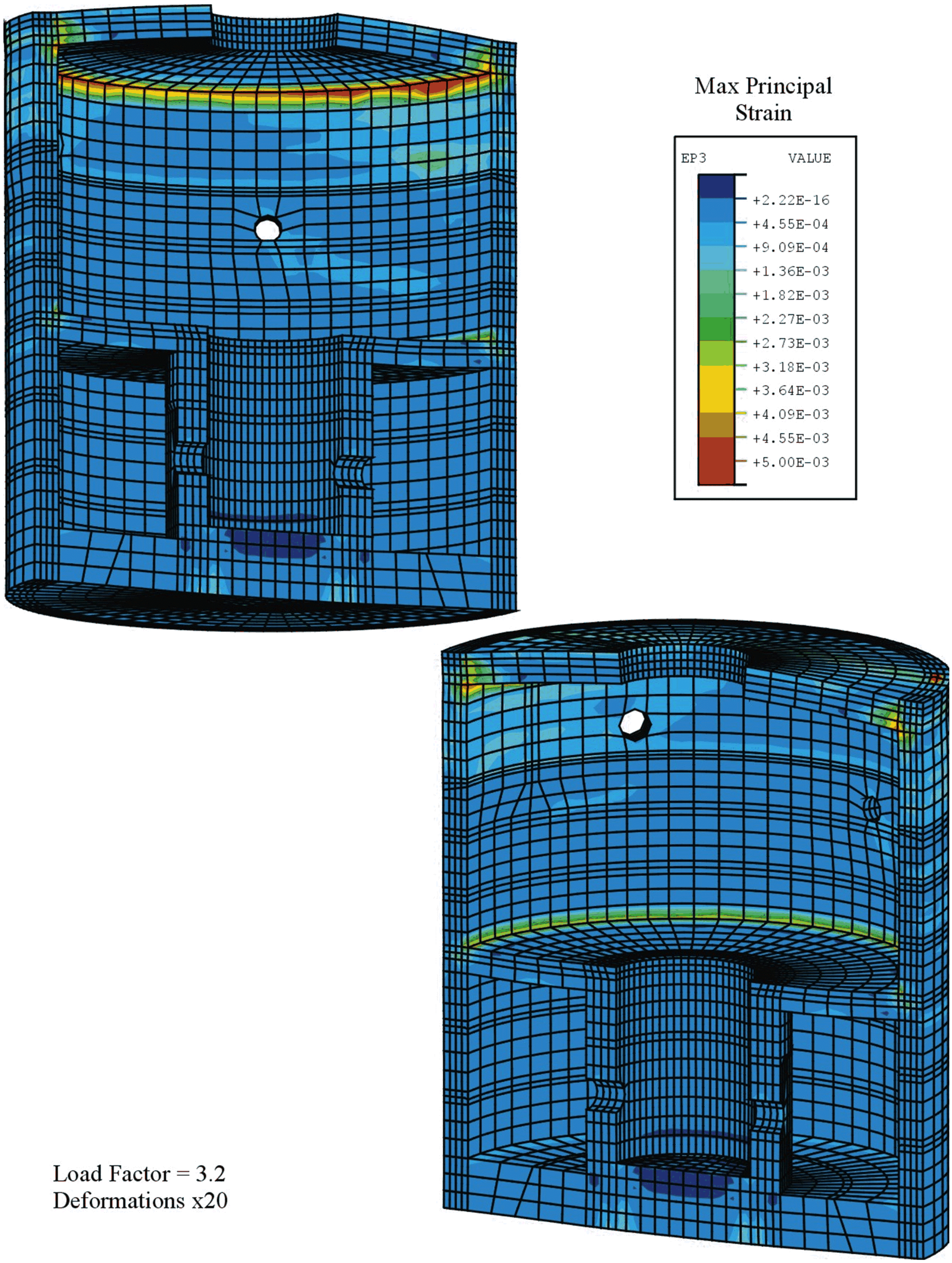


Figure 19B-3. Concrete Cracking Strain, Level C Analysis, 0.992 MPaG (144 psig) Pressure

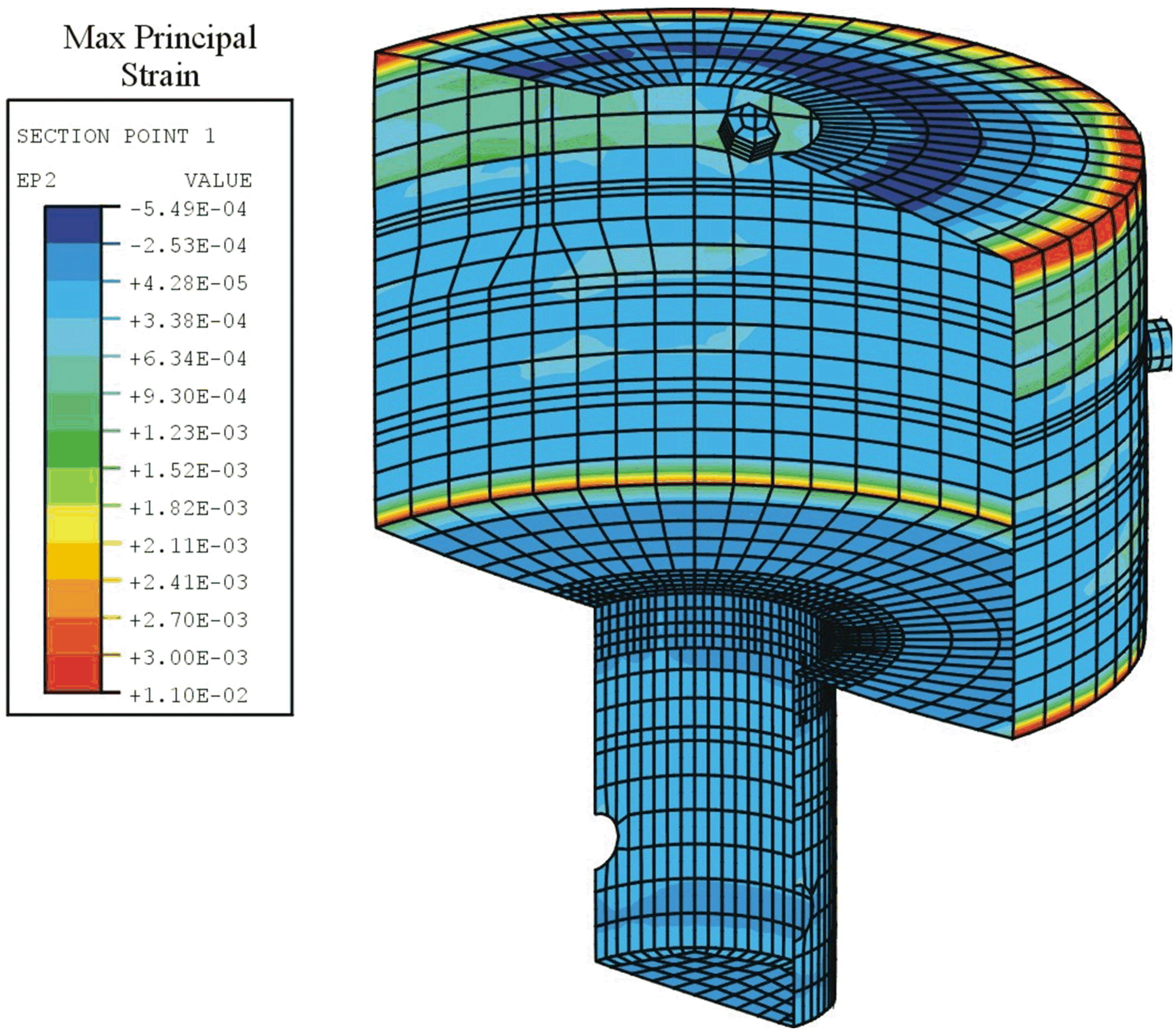


Figure 19B-4. Liner Maximum Principal Strain, Level C Analysis, 0.992 MPaG (144 psig) Pressure

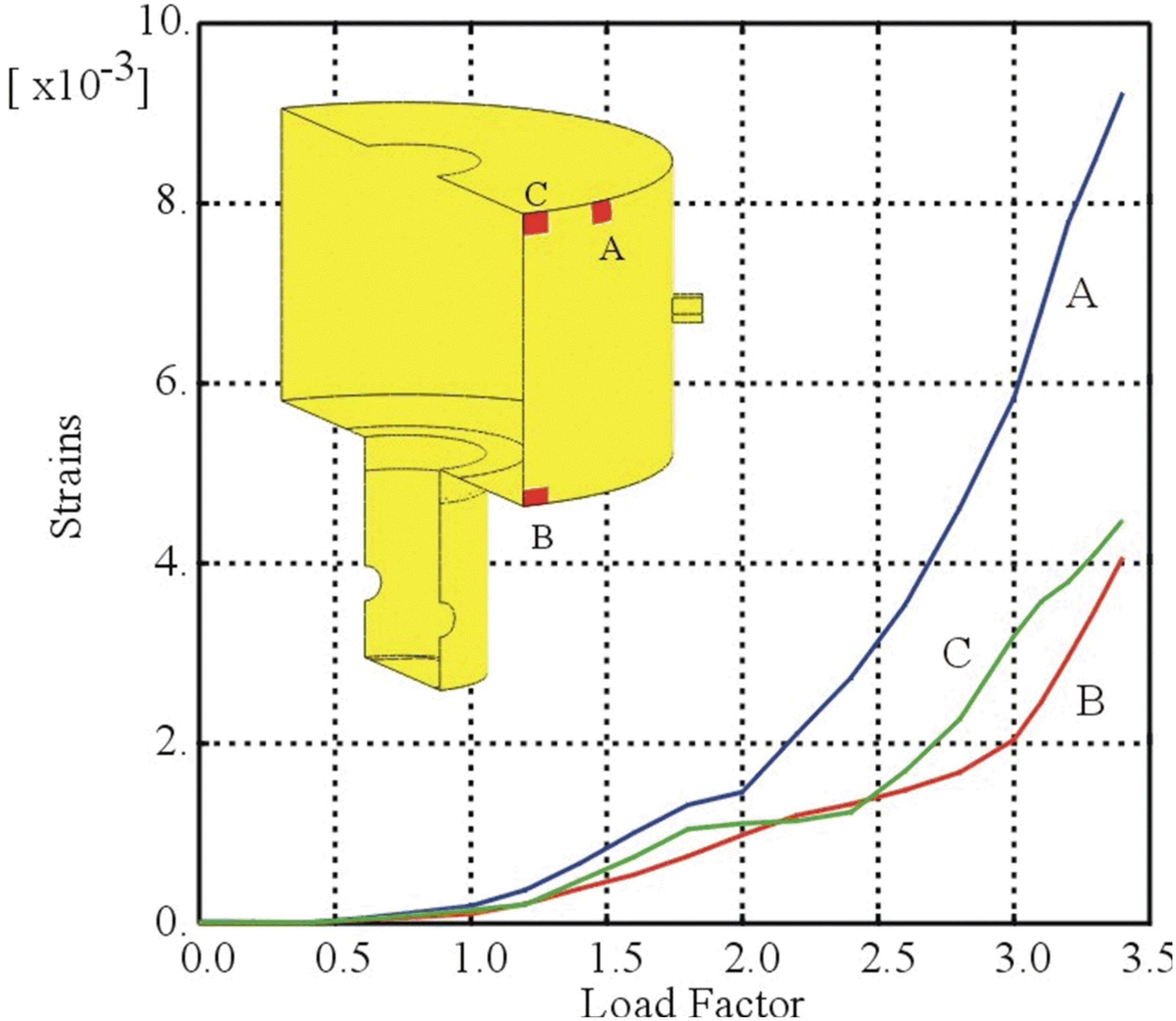


Figure 19B-5. Maximum Principal Strains in Liner at Critical Locations, Level C Analysis

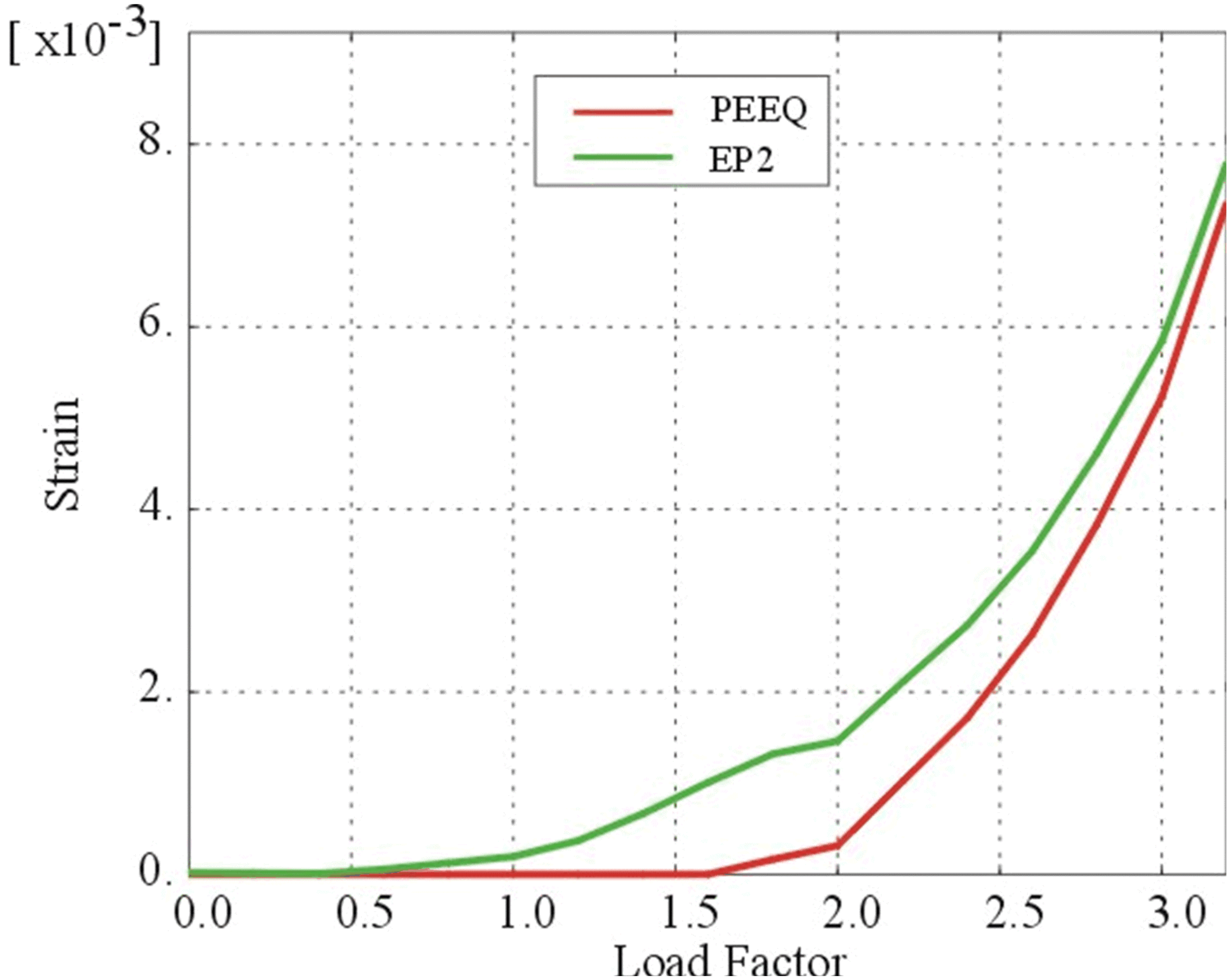


Figure 19B-6. Liner Membrane Strain at Top Slab Connection, Level C Analysis

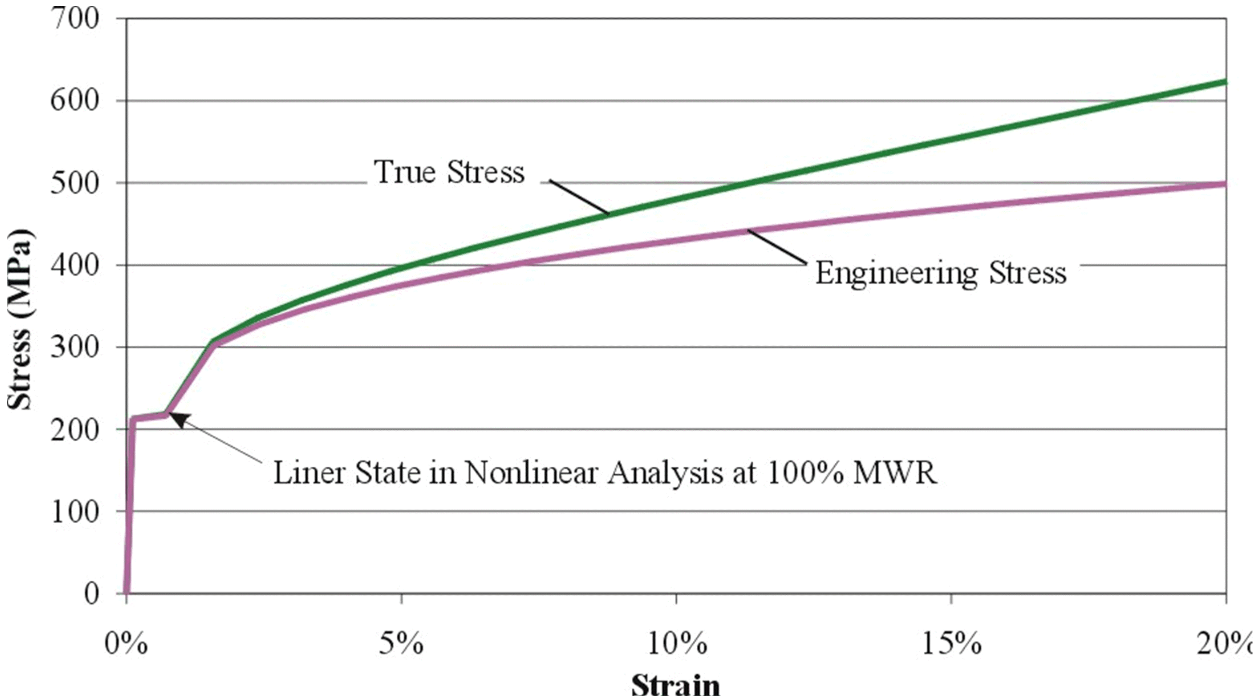


Figure 19B-7. State of Liner at Top Slab Connection at 100% MWR Pressure

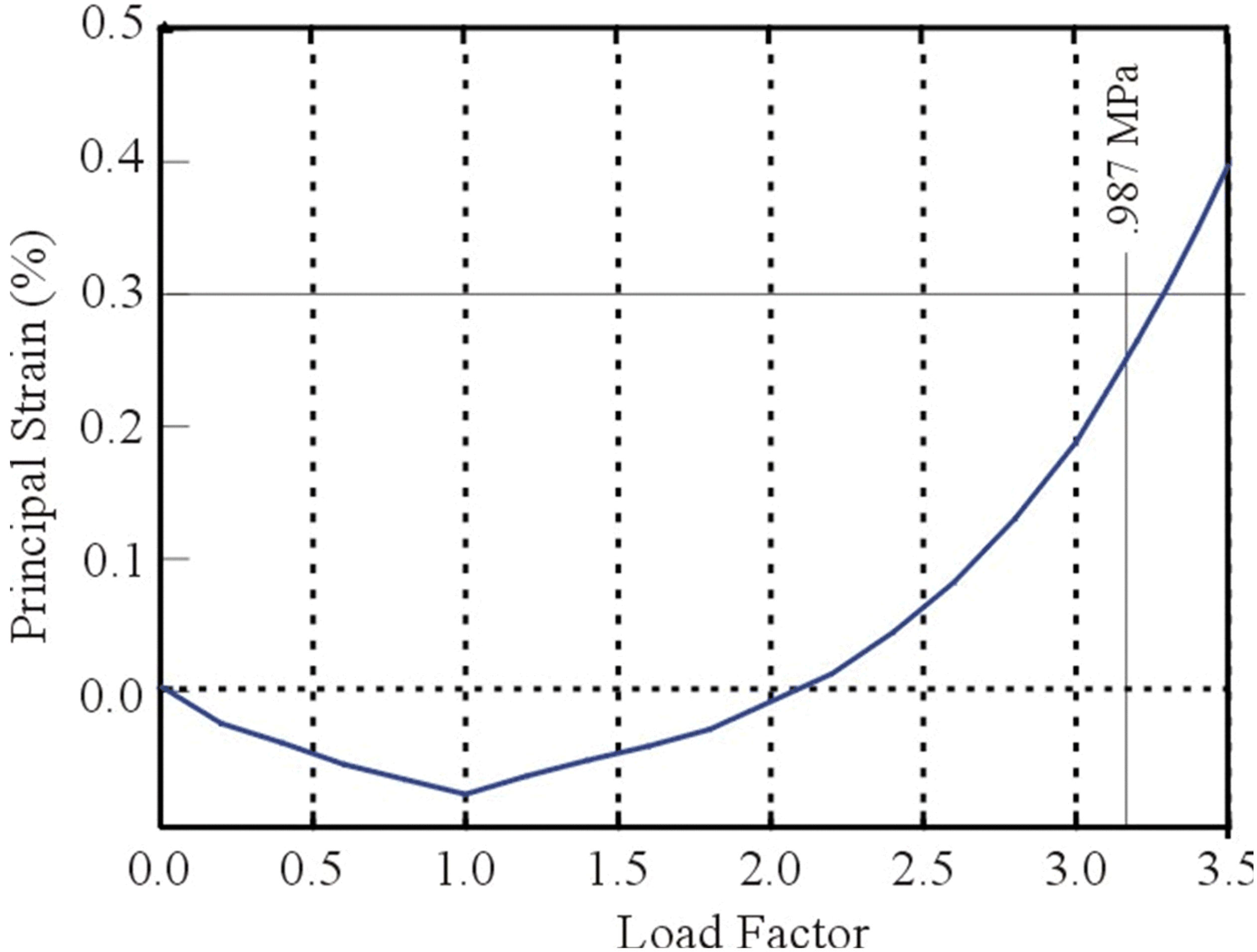


Figure 19B-8. Liner Membrane Strain at Top Slab Connection, Level C Analysis with Thermal Stress

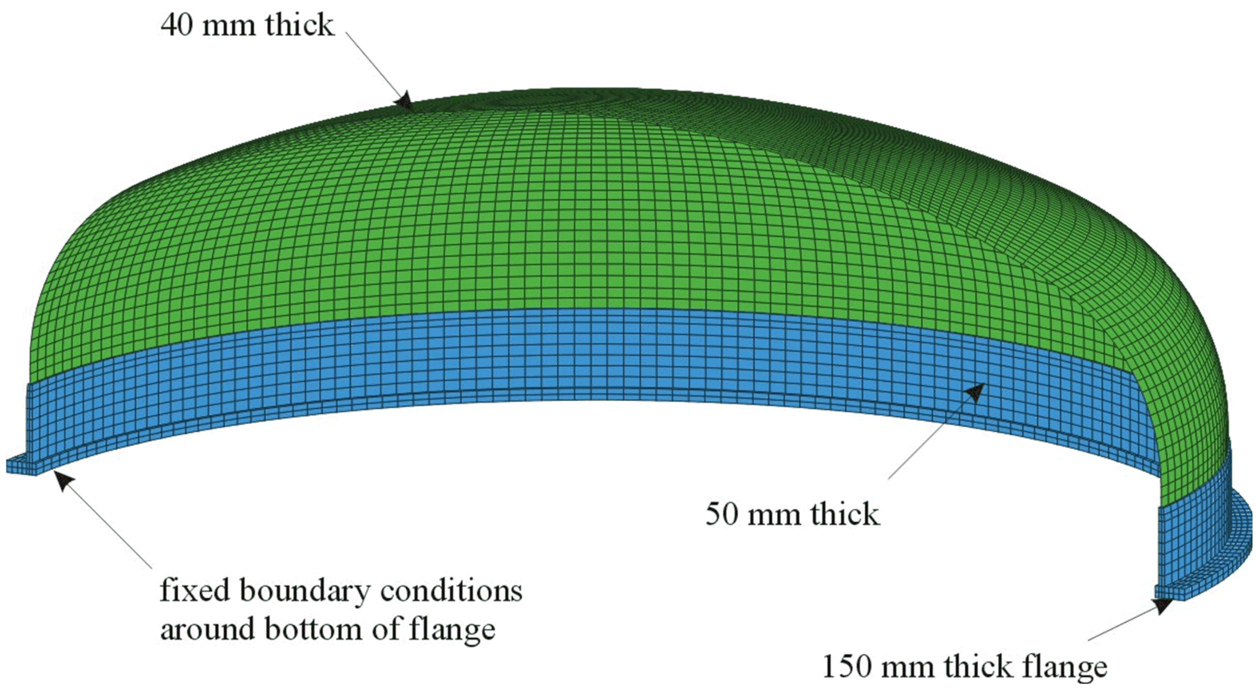


Figure 19B-9. Finite Element Model for Drywell Head Capacity Study

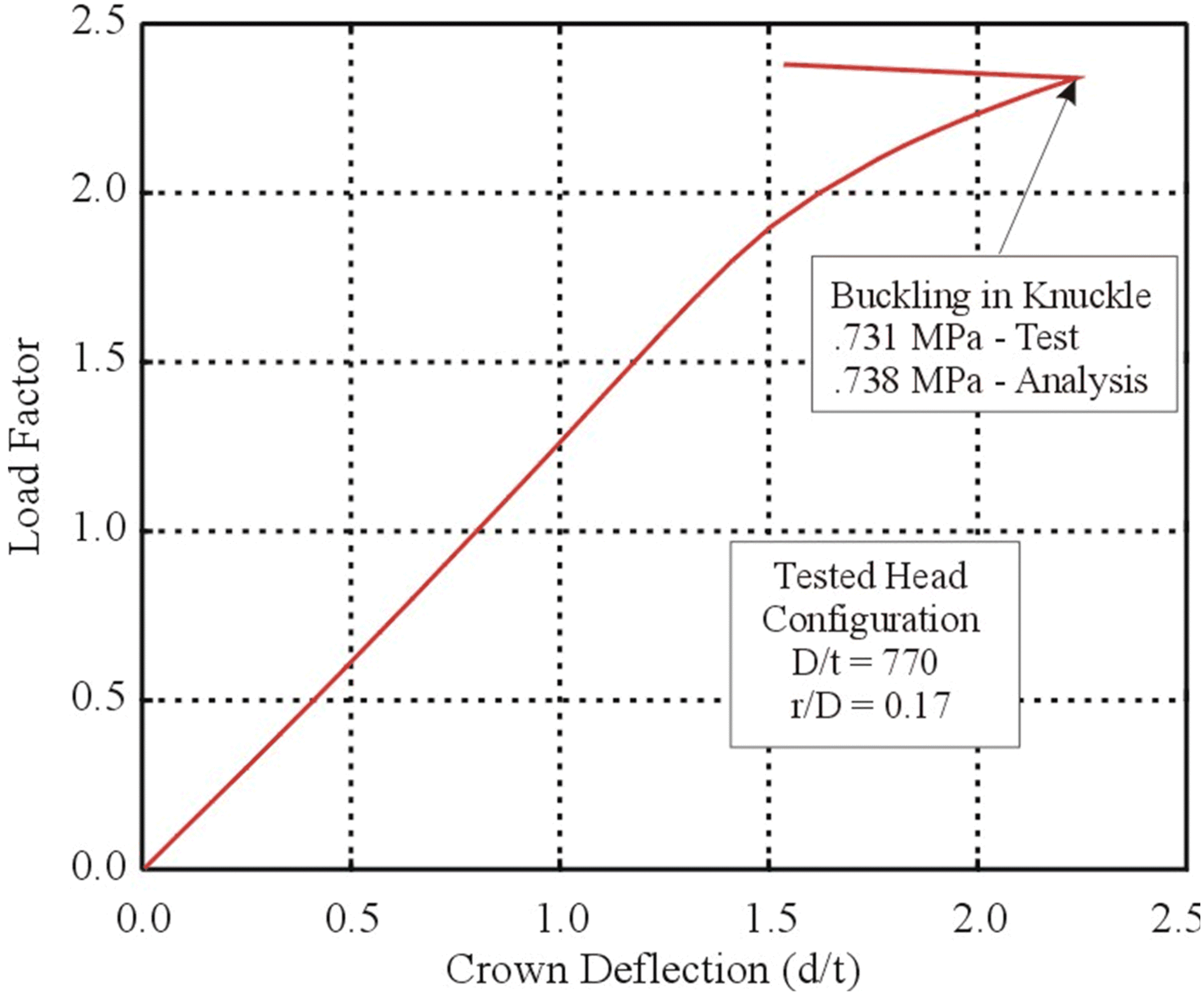


Figure 19B-10. Displacement at Crown in Buckling Test Analysis

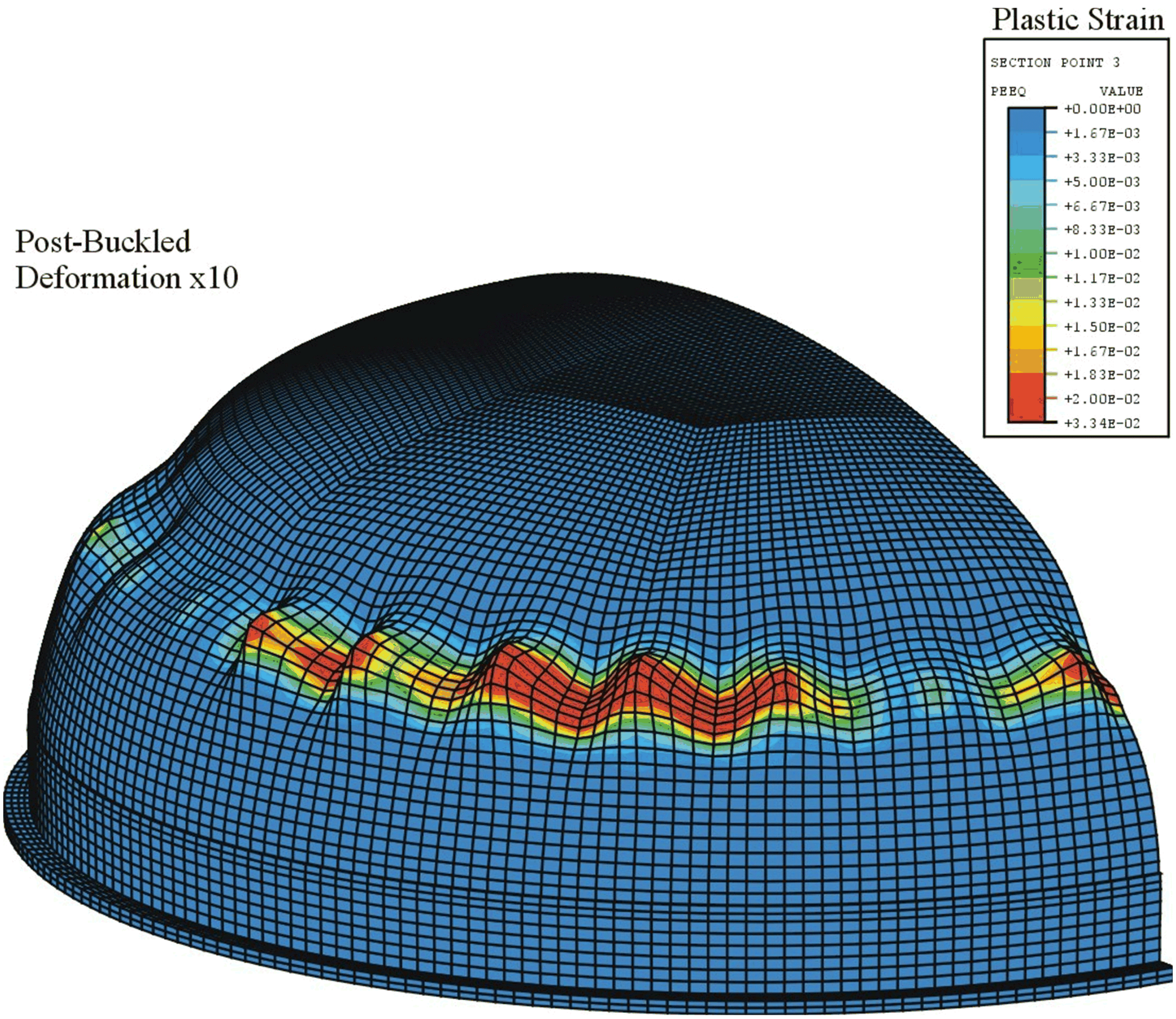


Figure 19B-11. Post Buckled Shape of Test Analysis Model

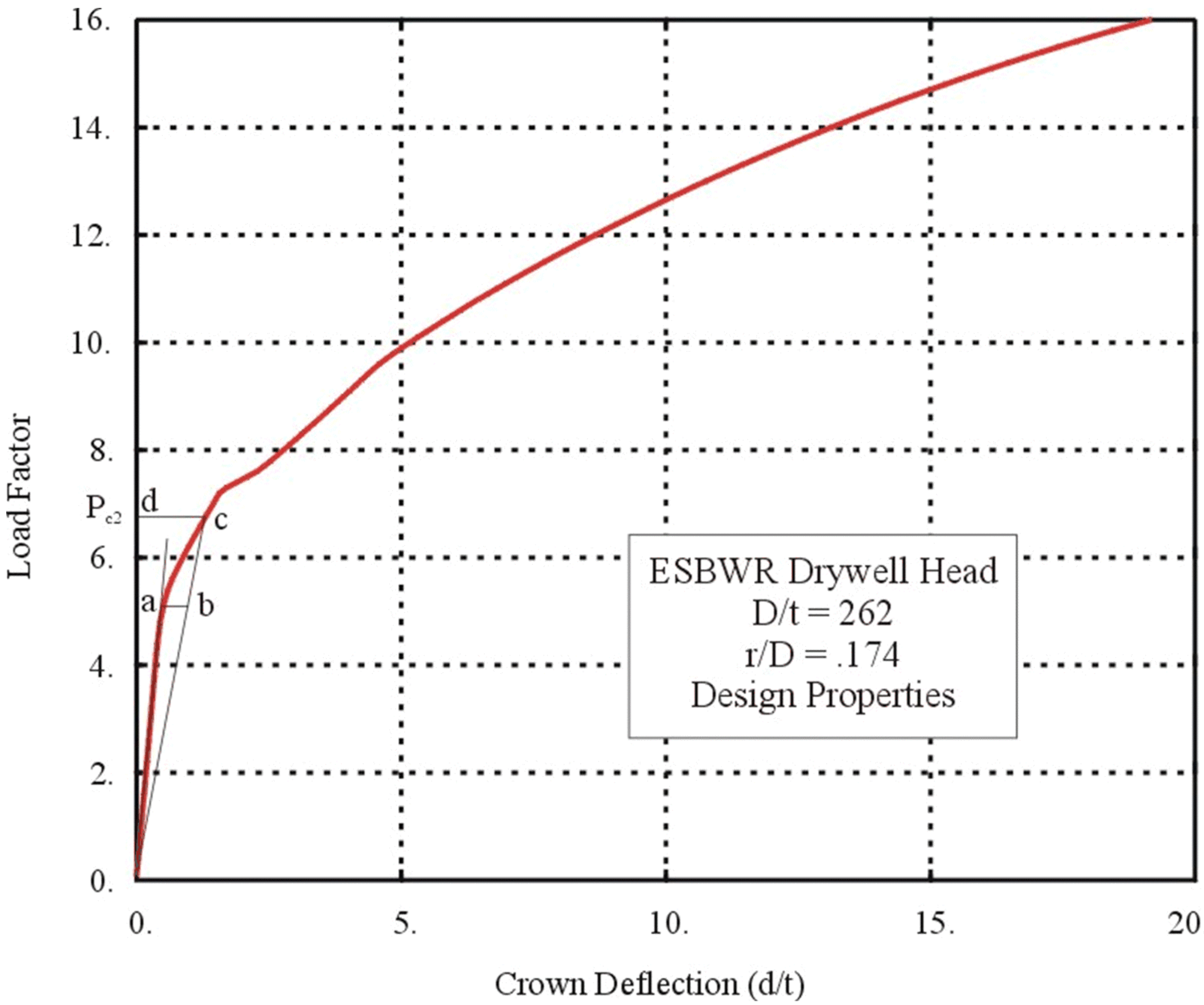


Figure 19B-12. Performance of ESBWR Drywell Head Under Internal Pressure

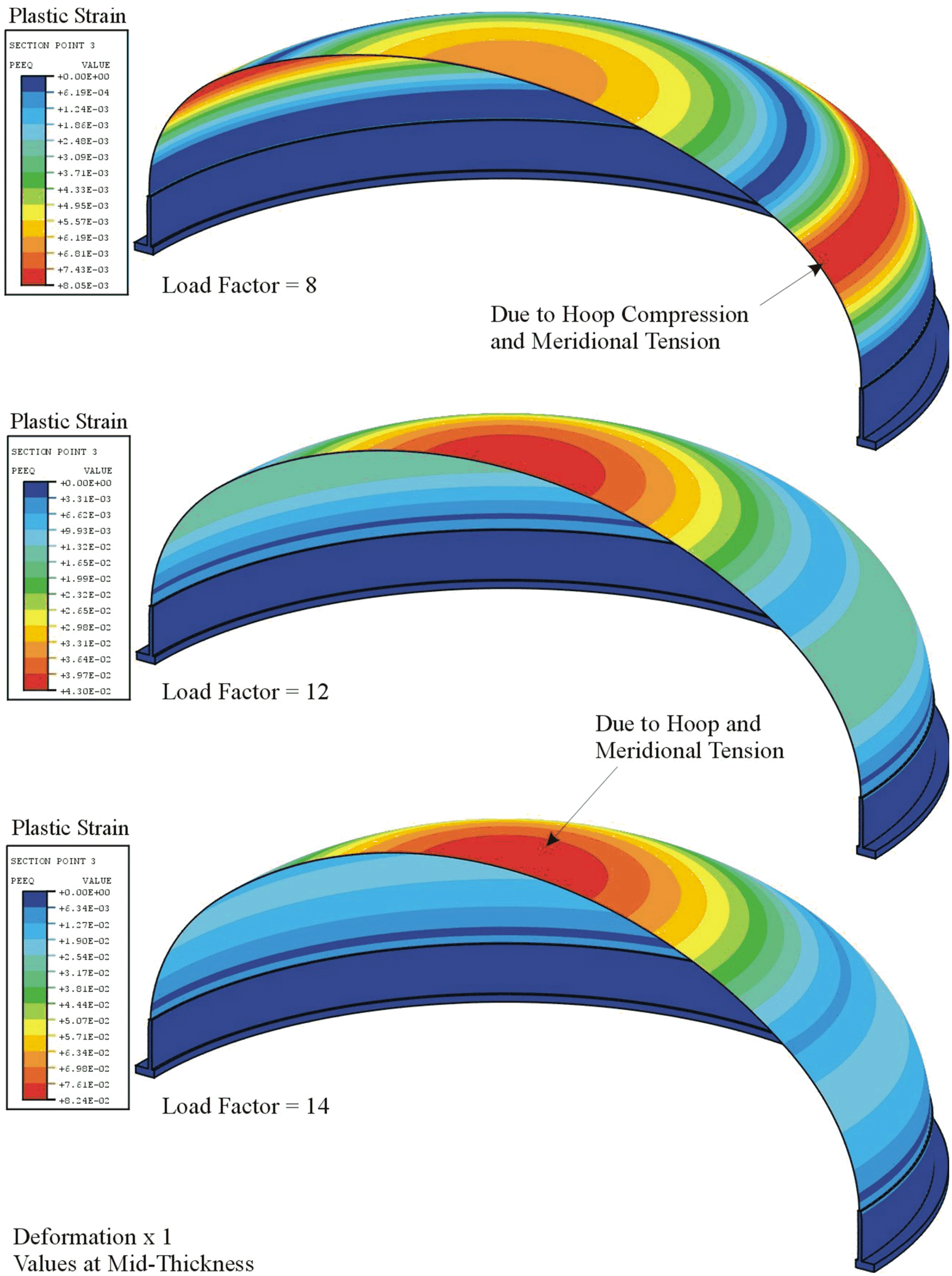


Figure 19B-13. Plastic Strains, Nominal Geometry, Ambient Temperature

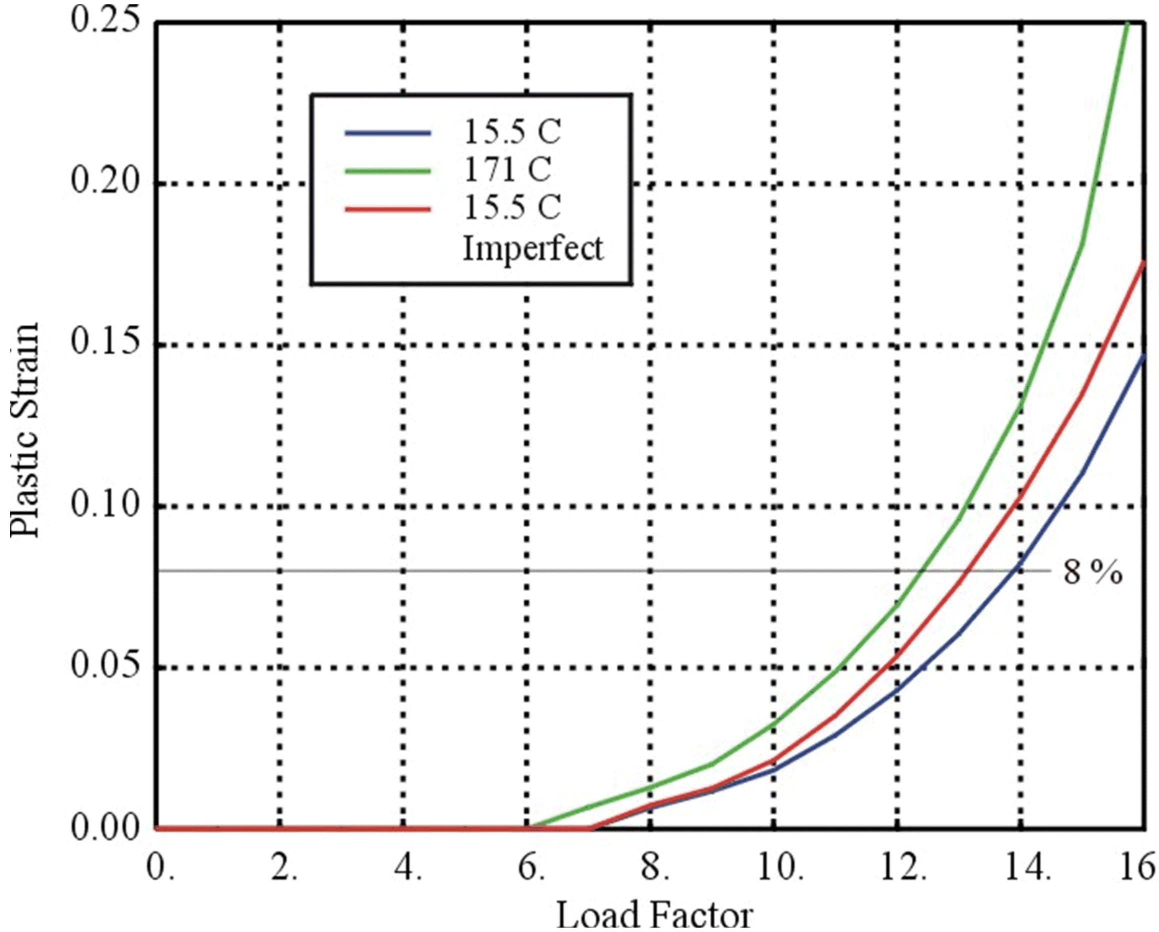


Figure 19B-14. Mid-Thickness Plastic Strain at Crown Under Increasing Pressure

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.

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

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

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

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

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 3 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 3 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 ½ 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 2 parameters defining the lognormal 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 $\beta = 0.06$ 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 with deformations magnified by 10. 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 4 times design pressure. This figure also shows the deformed shapes magnified by 10 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 1.913 MPaG (277 psig) or a load factor of 6.17 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, 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 1.708 MPaG (248 psig) or a load factor of 5.51 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.

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 11% from ambient conditions to elevated temperature conditions. In addition, there is very little difference between the capacity at 260°C steady state conditions and the 538°C transient conditions mainly because the upper pool girder controls this failure mode. 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 with 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 insure 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 is 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 seals in the flanges.

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 of this prying action that 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 1.587 MPaG (230 psig) or 5.12 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.

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. An extreme case with the inside of the drywell head held at 260°C (500°F) was also considered. This case also improved the pressure capacity due to bolt yielding. Here the elevated temperature on the inside of the head acts to keep the inner surface of the flanges together because the hot inner surface must expand. This thermal demand also resists the flange separation. Because there is very little effect on ultimate strength or ductility for this material up to 260°C (500°F), the mode of failure also does not change.

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 function, 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 with 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 develops 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 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 levels of strain 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 affect 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 thermal 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 for an accident. 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. 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) leakage at the bolted flange connection of the equipment hatch type penetrations due to flange separation, and 3) 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. 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 thermal induced stress at this bolted connection. Note that the drywell head is protected from these extreme temperatures because of insulation around the RPV and restricted flow paths from the drywell space into the area beneath the drywell head. The pool of water on top of the drywell head also keeps the flanges and closure bolts at moderate temperatures.

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 (MN/m^3)	Specific Heat (kcal/kg-°C)	Conductivity (kcal/hr-m-°C)
Concrete	0.0235	0.21	1.4
Carbon Steel Liner	0.0770	0.11	46.0
Stainless Steel Liner	0.0770	0.118	14.0
Structural Steel	0.0770	0.11	46.0

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

	Ambient Conditions		260°C Conditions		538°C 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

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

	Ambient Conditions		260°C Conditions		538°C 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						
.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
SA540-B24 Class 3 Bolting						
Yield Stress (MPa)	941.9	896.6	813.4	763.4	626.9	572.4
Tensile Strength (MPa)	1045.4	1000.0	901.5	851.5	692.9	638.5
Elongation (%)	14.5	12.0	15.5	13.0	16.5	14.0

Table 19C-4
Summary of Concrete Material Properties

Material/Property	Ambient Conditions		260°C Conditions		538°C 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

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

Criteria	Ambient Conditions		260°C Conditions		538°C 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

Table 19C-6
Summary of Variance for Modeling Uncertainty

Analysis Type	Lognormal Standard Deviations		
	Ambient Conditions	500°F Conditions	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 (LF on P_d)	β	Pressure MPaG (LF on P_d)	β
Median Failure Pressure	Median Values	1.913 (6.17)	--	1.708 (5.51)	--
Concrete Strength (MPa)	Material Property	1.624 (5.24)	0.0993	1.590 (5.13)	0.0434
Rebar Yield Stress (MPa)	Material Property	1.907 (6.15)	0.002	1.640 (5.29)	0.0248
Section Shear Strain Limit (%)	Failure Criterion	1.615 (5.21)	0.1028	N/A	--
Rebar Rupture Strain (%)	Failure Criterion	N/A	--	N/A	--
Liner Tearing Strain (%)	Failure Criterion	N/A	--	1.587 (5.12)	0.0446
Modeling Uncertainty (Section 4.6)	Modeling Methods	--	0.1355	--	0.1355
Composite Lognormal Standard Deviation	Composite	--	0.1970	--	0.1512

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

Failure Mode and Thermal Condition	PDF Lognormal Distribution		Failure Pressure, MPaG (Load Factor on P_d)	
	μ	β	Median Value	95% Value
RCCV Capacity due to Shear Failure in Pool Main Girder				
260 °C Steady State	1.800	0.1970	1.913 (6.17)	1.357 (4.38)
Ambient Steady State	1.911	0.1887	2.133 (6.88)	1.536 (4.95)
538 °C Transient	1.807	0.2056	1.928 (6.22)	1.346 (4.34)
Liner Tear at RCCV Wall Connection with Top Slab				
260 °C Steady State	1.695	0.1512	1.708 (5.51)	1.317 (4.25)
Ambient Steady State	1.648	0.1403	1.628 (5.25)	1.280 (4.13)
538 °C Transient	1.752	0.1623	1.810 (5.84)	1.368 (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 (LF on P_d)	β	Pressure MPaG (LF on P_d)	β
Median Failure Pressure	Median Values	1.587 (5.12)	--	2.015 (6.50)	--
Steel Yield Stress (MPa)	Material Property	1.652 (5.33)	-0.0244	2.114 (6.82)	-0.0292
Steel Rupture Strain (%)	Failure Criterion	N/A	--	1.705 (5.50)	0.1016
Drywell Head Temperature	Loading Condition	1.587 (5.12)	0.00	--	--
Bolt Prestress (MPa)	Loading Condition	1.587 (5.12)	0.00	1.975 (6.37)	0.0123
Bolt Yield Stress (MPa)	Failure Criterion	1.507 (4.86)	0.0317		--
Modeling Uncertainty (Section 4.6)	Modeling Methods	--	0.1482		0.1482
Composite Lognormal Standard Deviation	Composite	--	0.1535		0.1824

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

Failure Mode and Thermal Condition	PDF Lognormal Distribution		Failure Pressure, MPaG (Load Factor on P_d)	
	μ	β	Median Value	95% Value
Leakage Due to Bolt Yielding				
260 °C Steady State	1.621	0.1535	1.587 (5.12)	1.219 (3.93)
Ambient Steady State	1.846	0.1428	1.983 (6.40)	1.552 (5.01)
538 °C Transient	1.760	0.1645	1.826 (5.89)	1.374 (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 (LF on P_d)	β	Pressure MPaG (LF on P_d)	β
Median Failure Pressure	Median Values	2.635 (8.50)	--	1.882 (6.07)	--
Steel Yield Stress (MPa)	Material Property	N/A	--	1.866 (6.02)	0.0050
Bolt Prestress (MPa)	Loading Condition	2.635 (8.50)	0.000	1.776 (5.73)	0.0350
Bolt Yield Stress (MPa)	Failure Criterion	2.542 (8.20)	0.0218	1.882 (6.07)	0.00
Flange Separation (mm)	Failure Criterion	N/A	--	1.810 (5.84)	0.0235
Modeling Uncertainty (Section 4.6)	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 (Load Factor on P_d)	
	μ	β	Median Value	95% Value
Leakage at Bolted Flanges due to Flange Separation				
260 °C Steady State	1.791	0.1542	1.882 (6.07)	1.443 (4.65)
Ambient Steady State	1.860	0.1435	2.012 (6.49)	1.573 (5.07)
538 °C Transient	1.324	0.1651	1.181 (3.81)	0.888 (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)					
	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	5.12	3.93	5.89	4.43
	1.983	1.552	1.587	1.219	1.826	1.374
Liner Tearing RCCV Wall at Top Slab	5.25	4.13	5.51	4.25	5.84	4.41
	1.628	1.280	1.708	1.317	1.810	1.368
EQ Hatch Leakage - Flange Separation	6.49	5.07	6.07	4.65	3.81	2.86
	2.012	1.573	1.882	1.443	1.181	0.888
RCCV Wall at Top Slab Connection	6.88	4.95	6.17	4.38	6.22	4.34
	2.133	1.536	1.913	1.357	1.928	1.346

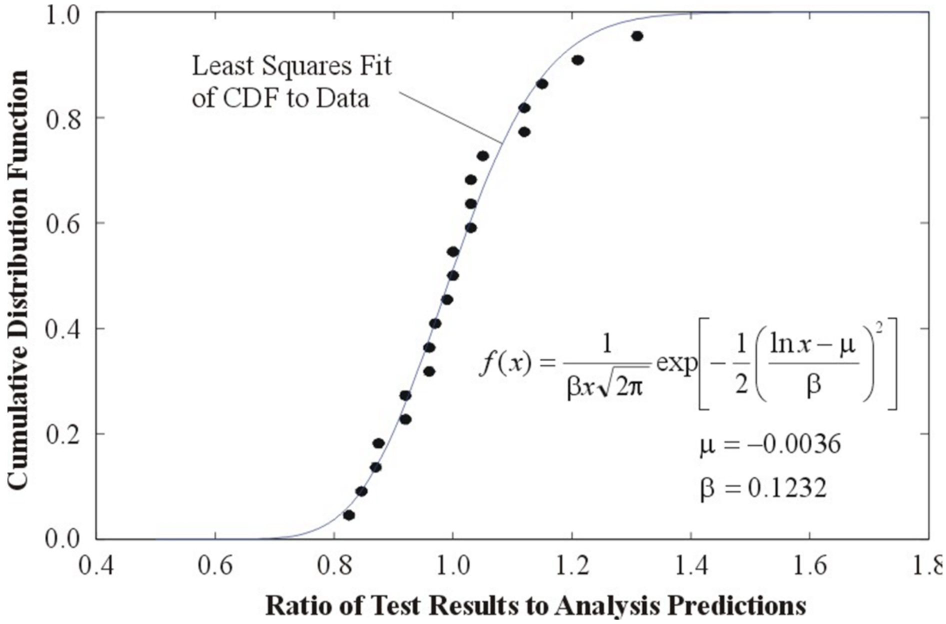


Figure 19C-1. Calculation of Variance due to Modeling Uncertainty

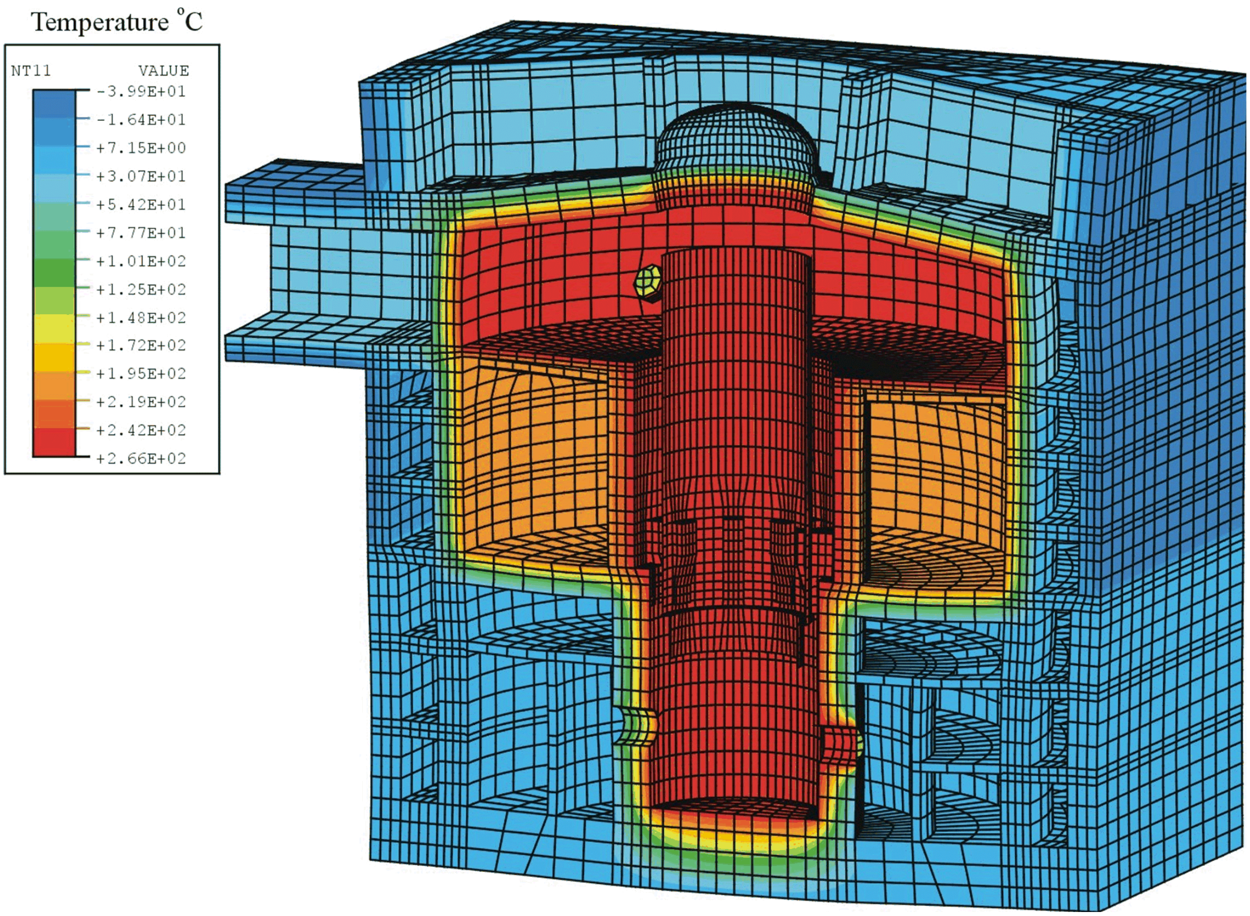


Figure 19C-2. Finite Element Model Showing the 260°C (500°F) Steady State Thermal Condition

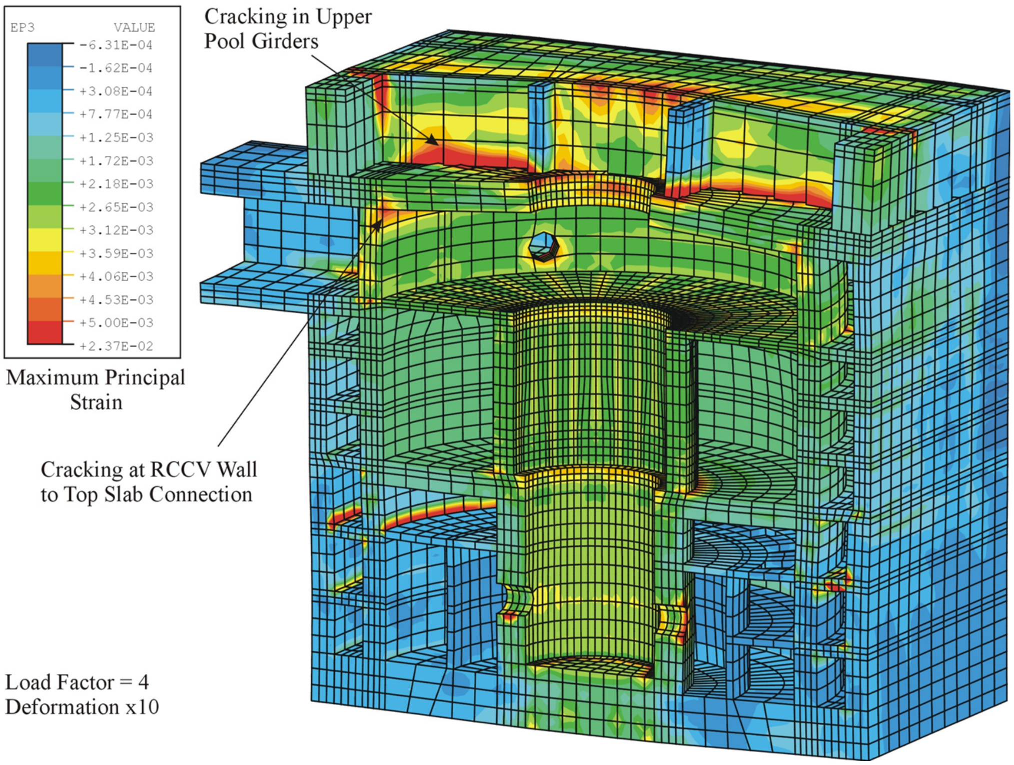


Figure 19C-3. Structural Response of RCCV at 1.24 MPaG (180 psig) Pressure

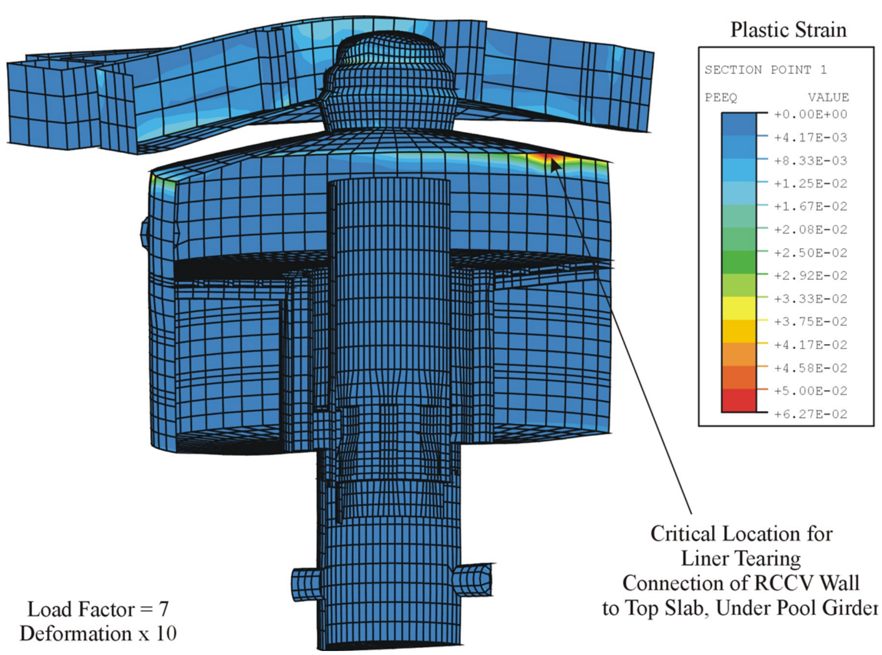


Figure 19C-4. Critical Location for Liner Tearing in RCCV

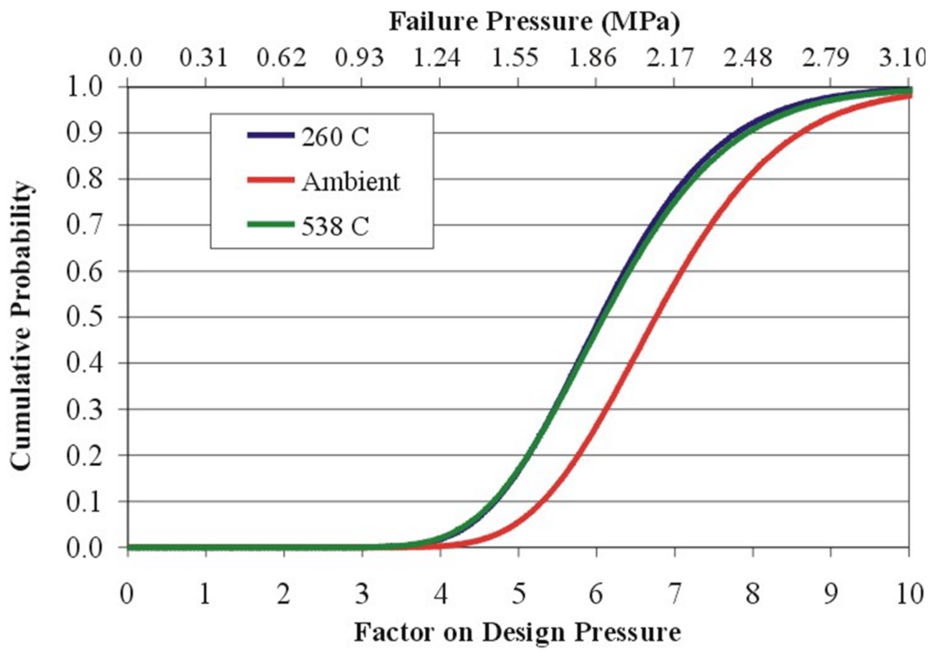


Figure 19C-5. Pressure Fragility for RCCV Wall Capacity with Temperature

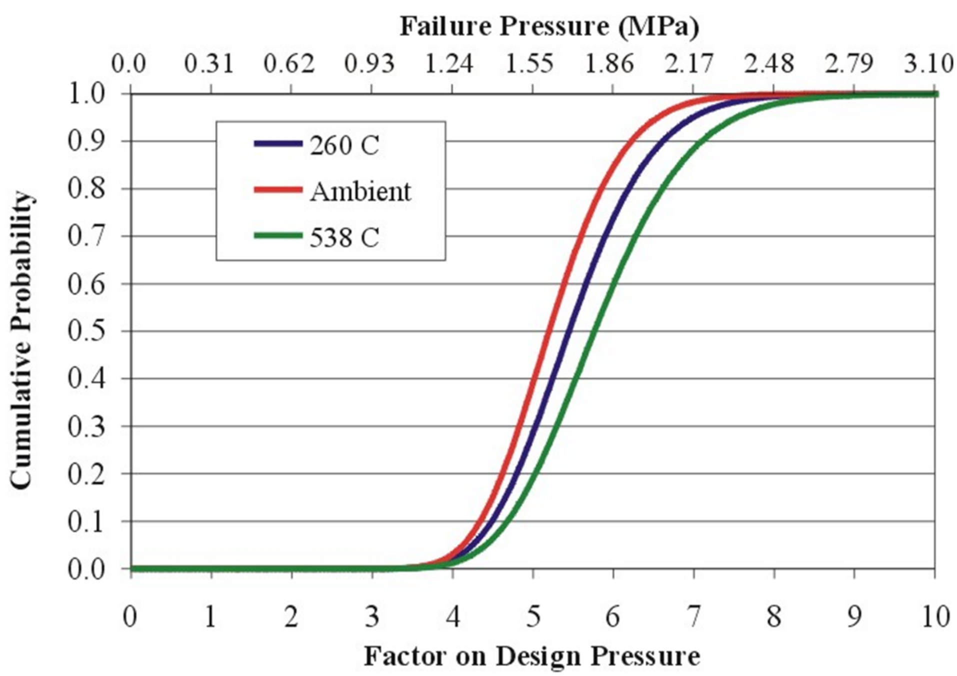


Figure 19C-6. Pressure Fragility for RCCV Liner Tearing with Temperature

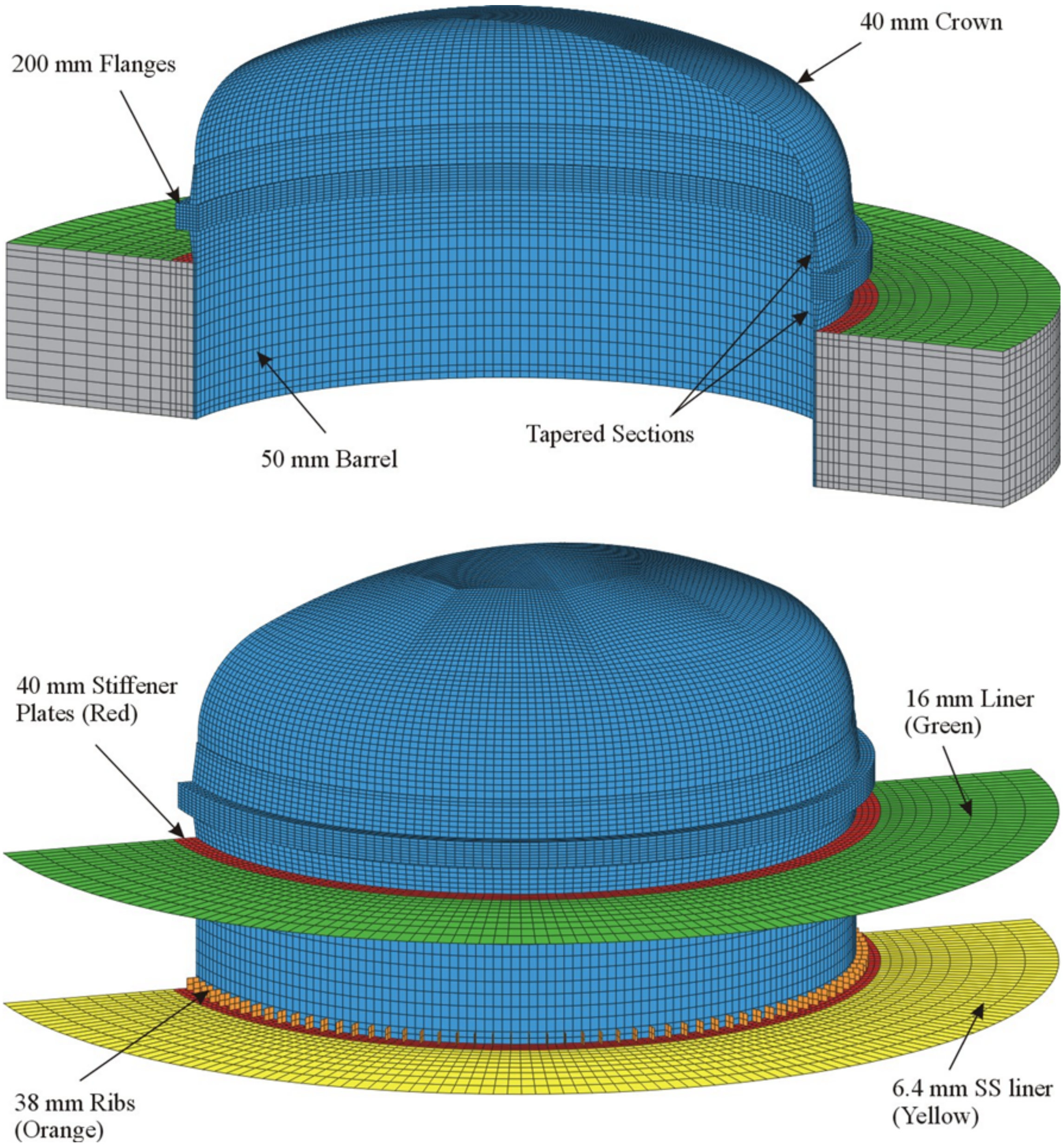


Figure 19C-7. Local Finite Element Model for Drywell Head

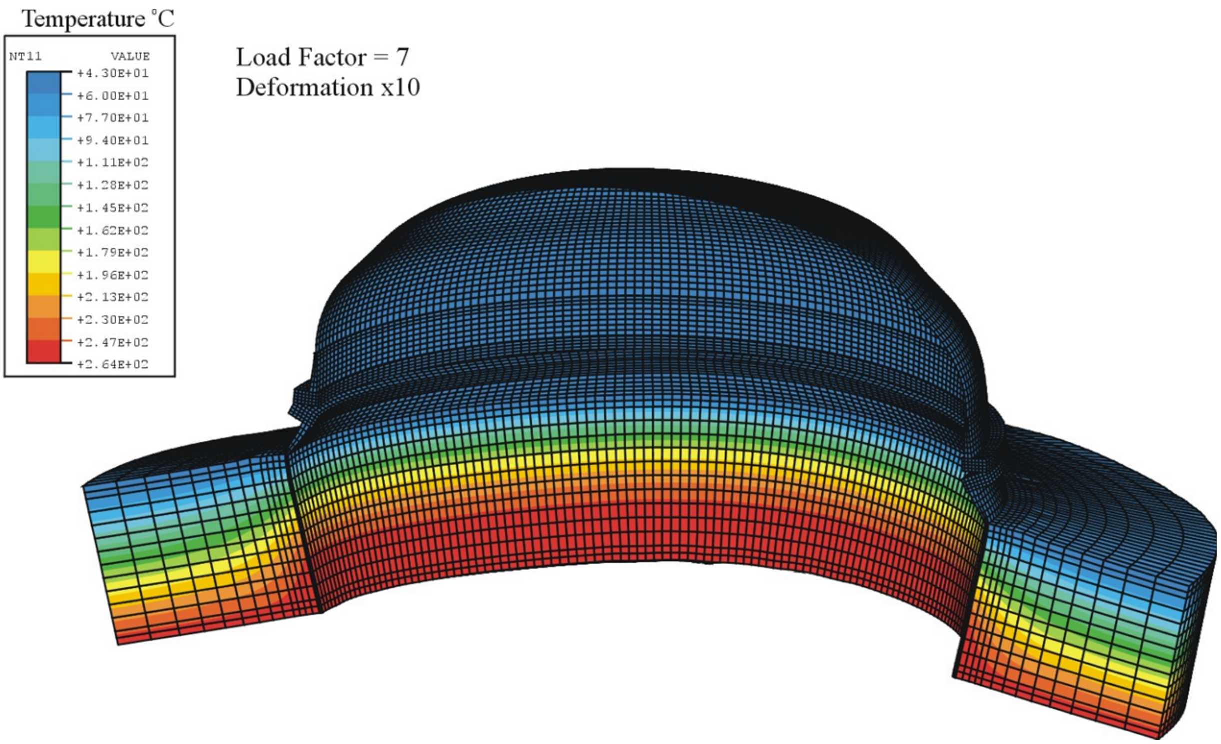


Figure 19C-8. Thermal Contours and Deformation for 260°C (500°F) Thermal Condition

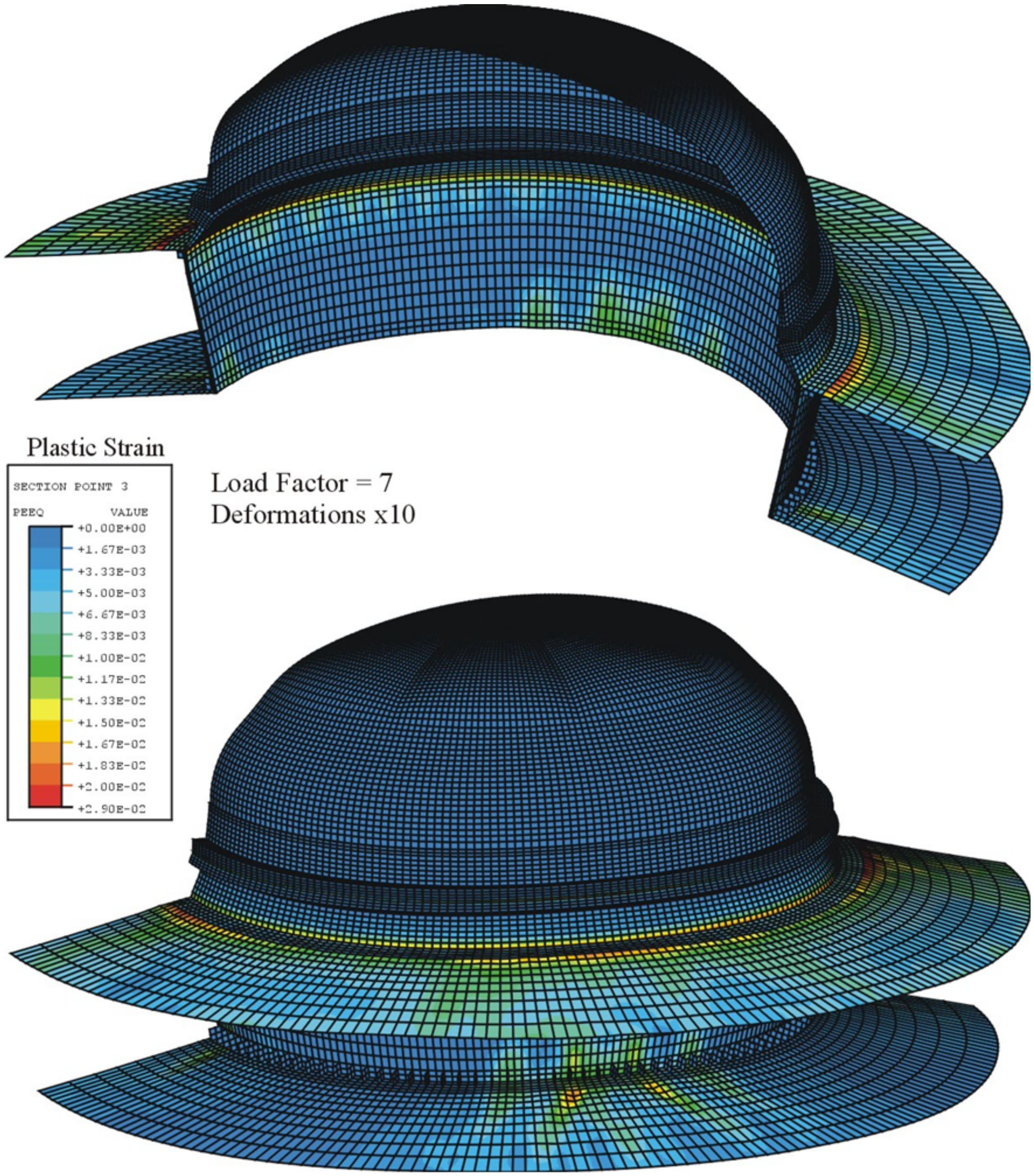


Figure 19C-9. Equivalent Plastic Strains in Steel Components at 2.17 MPaG (315 psig)

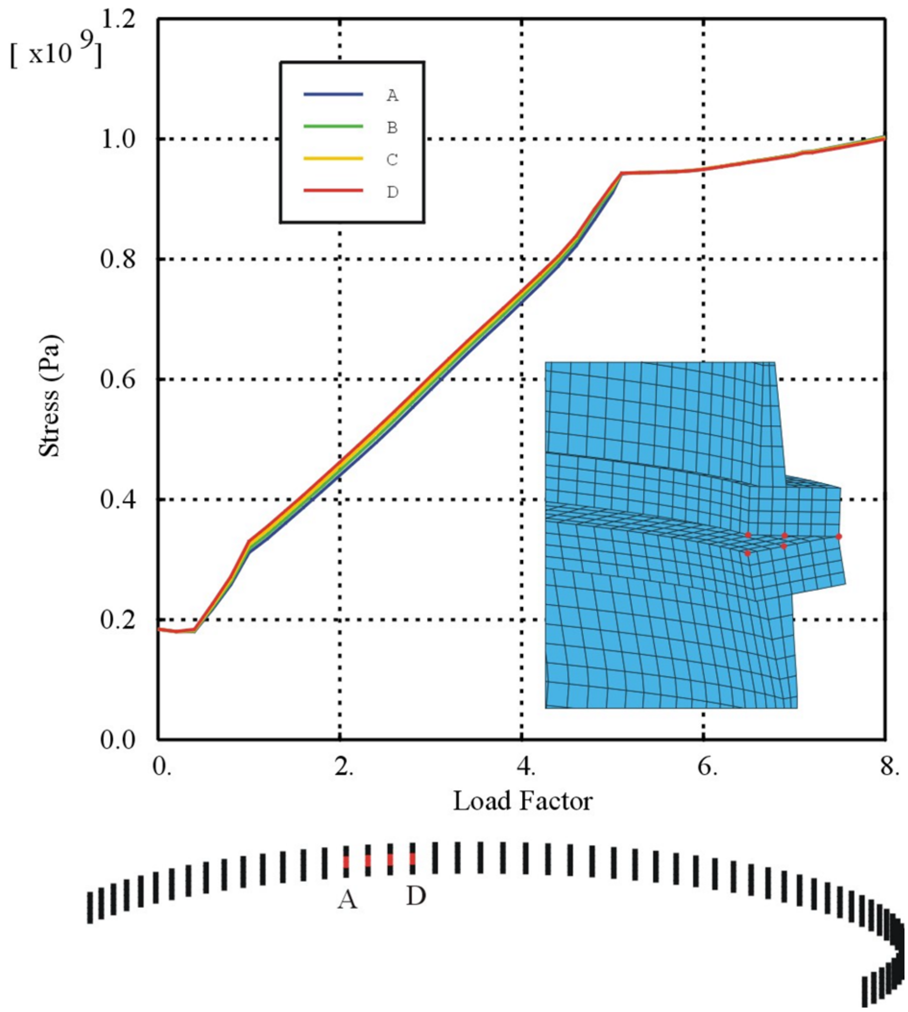


Figure 19C-10. Bolt Stresses in Drywell Head for 260°C (500°F) Thermal Condition

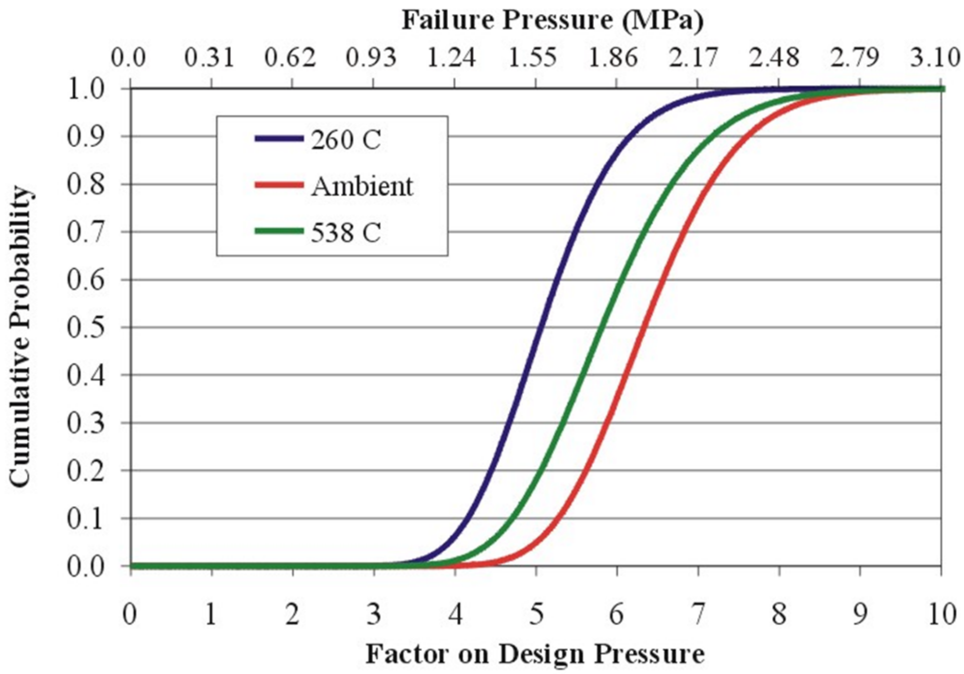


Figure 19C-11. Pressure Fragility with Temperature for Leakage at Drywell Head

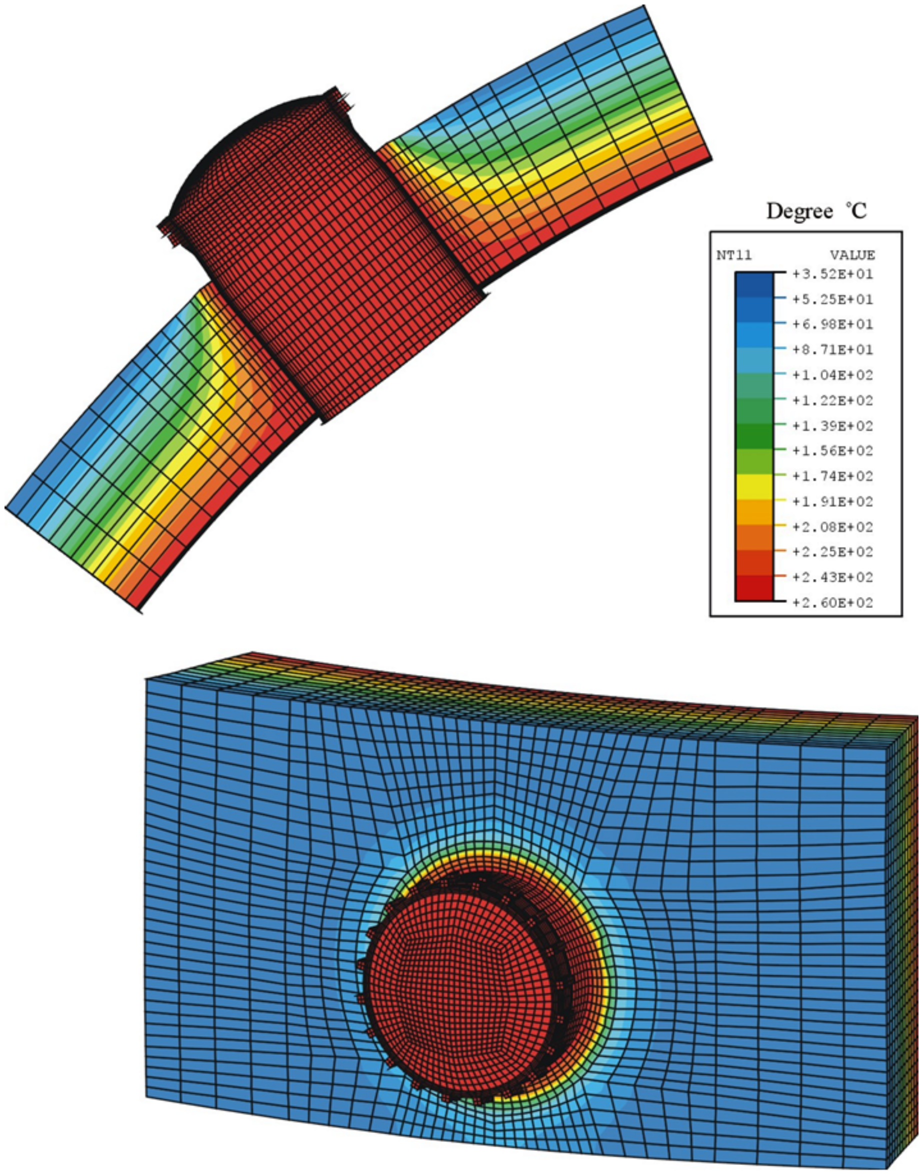


Figure 19C-12. Local Model of Drywell Equipment Hatch

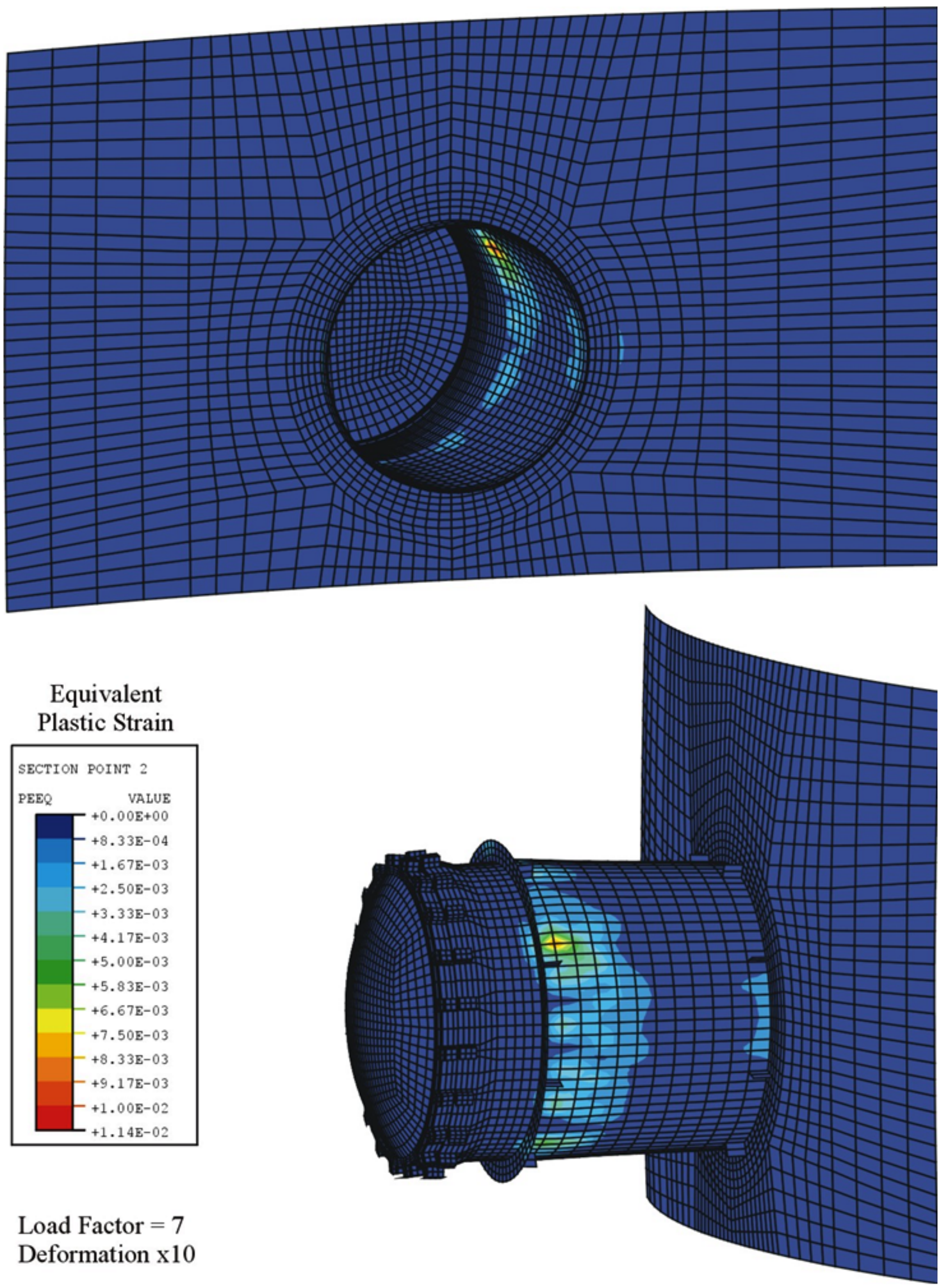


Figure 19C-13. Plastic Strains in EQ Hatch Steel Components, 260°C (500°F) Conditions

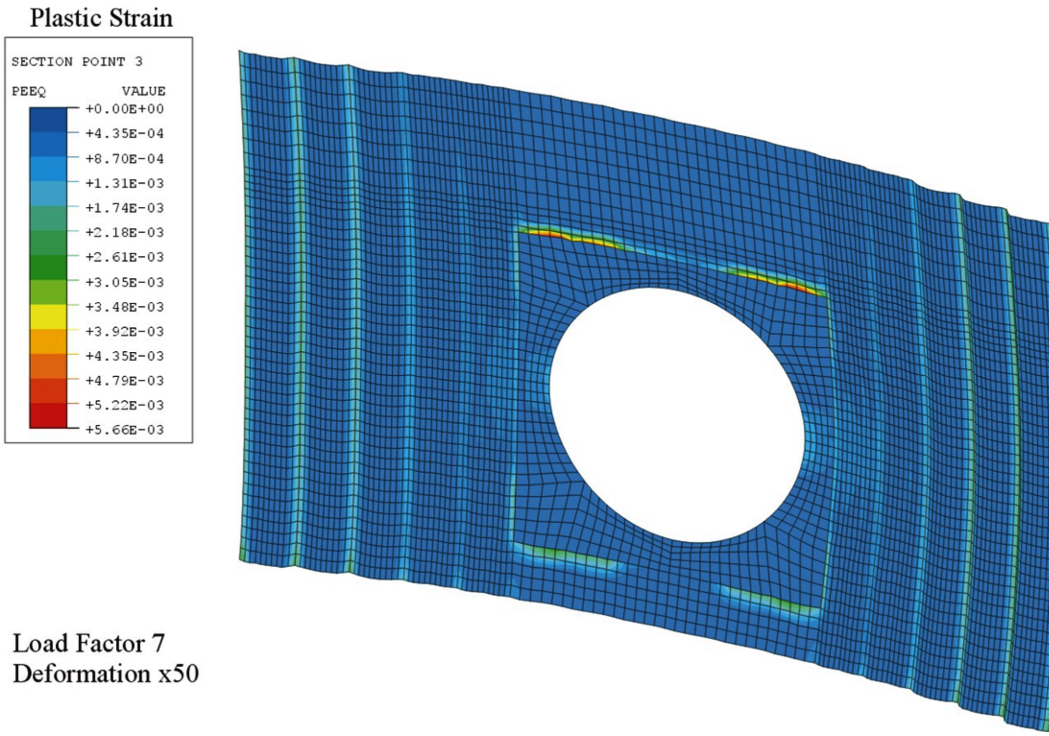


Figure 19C-14. Plastic Strains in Liner for Local Effects Slice Model

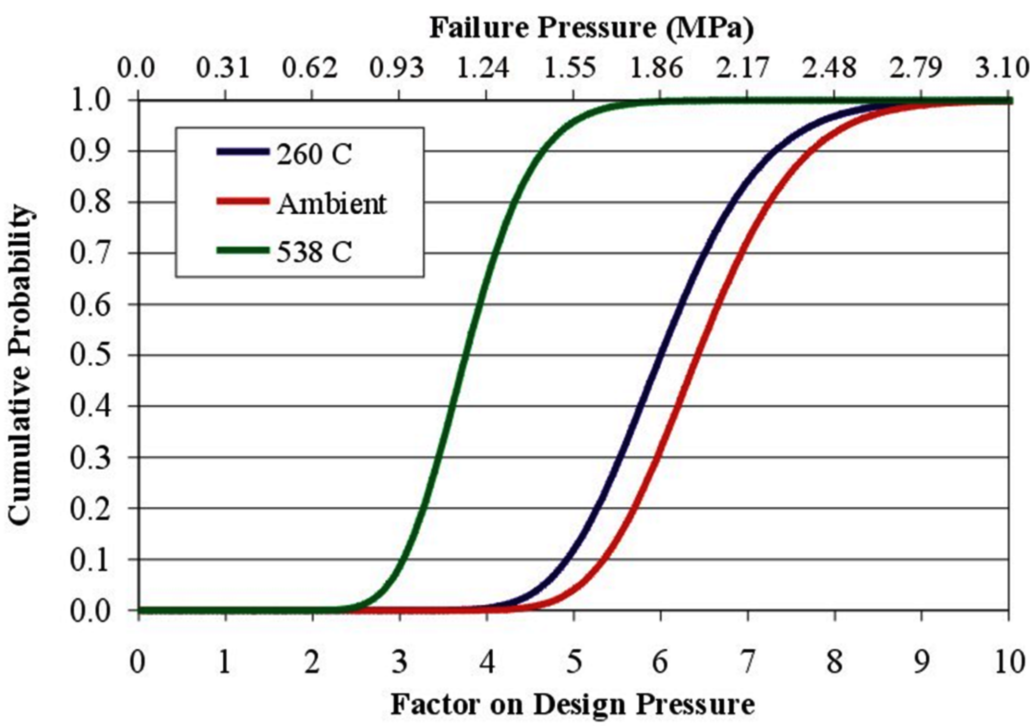


Figure 19C-15. Pressure Fragility with Temperature for Leakage at Equipment Hatch

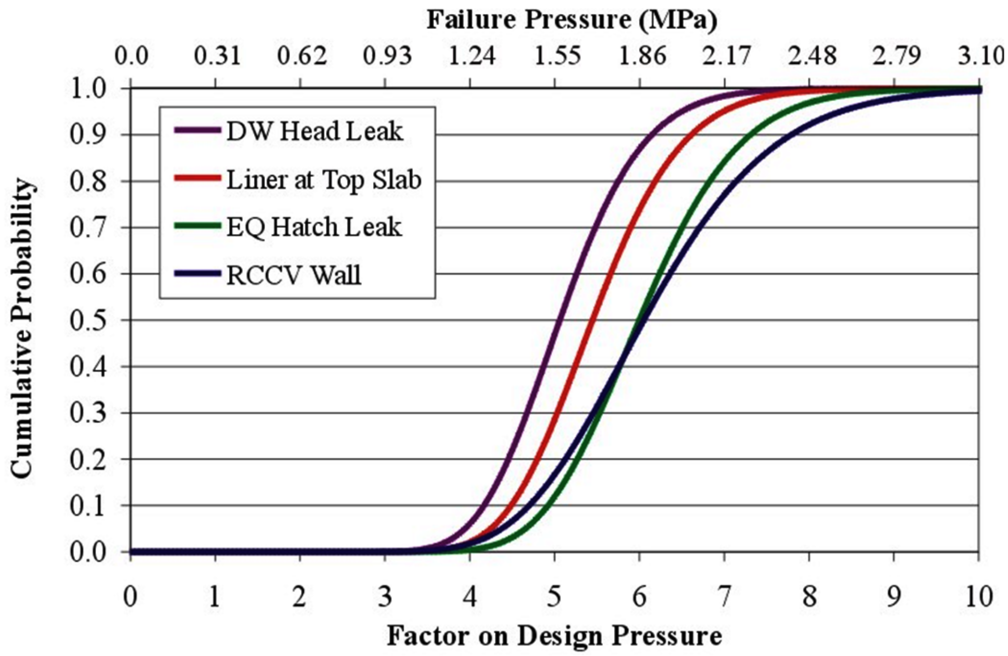


Figure 19C-16. Pressure Fragility at 260°C (500°F) Steady State Thermal Conditions