ENCLOSURE 1

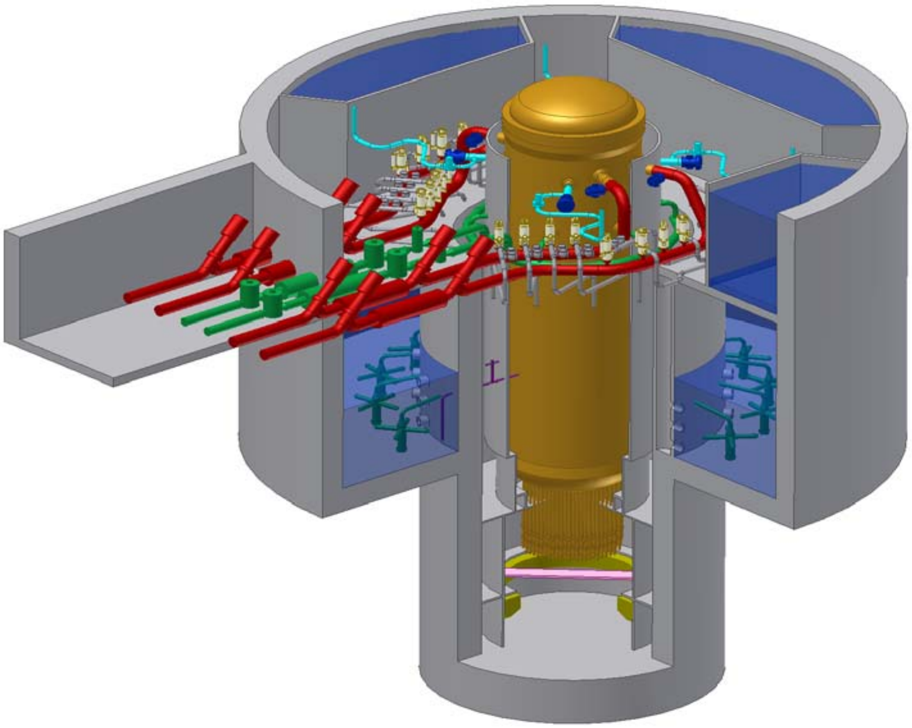
MFN 06-334

CD – Revision 1 to DCD Tier 2 –
ESBWR PRA and Severe Accidents –
Chapter 19 (26A6642BY, Rev. 01)

Item	**Location** Chapter 19 PRA and Severe Accidents	Description of Change
1	Entire Document	Chapter 19 was re-written entirely to conform to recently developed NRC guidelines in DG-1145. The re-write did not change PRA results.

GE Nuclear Energy

26A6642BY
Revision 1
September 2006



ESBWR Design Control Document

Tier 2

Chapter 19

Probabilistic Risk Assessment and Severe Accidents

Contents

List of Tables

List of Figures

Global Abbreviations And Acronyms List

10 CFR	Title 10, Code of Federal Regulations
AC	Alternating Current
ACF	Automatic Control Function
ACS	Atmospheric Control System
ADS	Automatic Depressurization System
ALWR	Advanced Light Water Reactor
AOO	Anticipated Operational Occurrence
ARI	Alternate Rod Insertion
ASME	American Society of Mechanical Engineers
ATWS	Anticipated Transients Without Scram
BiMAC	Basemat Internal Melt Arrest and Coolability
BMP	Basemat Melt Penetration
BWR	Boiling Water Reactor
CBP	Containment Bypass and Leakage
CCF	Common Cause Failure
CCFP	Conditional Containment Failure Probability
CCI	Corium-Concrete Interactions
CDF	Core Damage Frequency
CET	Containment Event Tree
CFR	Code of Federal Regulations
CIV	Combined Intermediate Valve
CLCH	Convection-Limited Containment Heating
COL	Combined Operating License
COP	Containment Over-Pressurization
COPS	Containment Over-pressure Protection System
CPET	Containment Phenomenological Event Tree
CRD	Control Rod Drive
CRDHS	Control Rod Drive Hydraulic System
CRDM	Control Rod Drive Mechanism
CRSS	Center for Risk Studies and Safety
CSET	Containment Systems Event Tree

CST	Condensate Storage Tank
CV	Containment Vessel
DC	Direct Current
DCH	Direct Containment Heating
DCS	Drywell Cooling System
DG	Diesel-Generator
dPT	Differential Pressure Transmitter
DPV	Depressurization Valve
DW	Drywell
EPRI	Electric Power Research Institute
EVE	Ex-Vessel Steam Explosion
FAPCS	Fuel and Auxiliary Pools Cooling System
FCI	Fuel-Coolant Interactions
FMCRD	Fine Motion Control Rod Drive
FPS	Fire Protection System
FV	Fussell-Vesely Importance
GDC	General Design Criteria
GDCS	Gravity-Driven Cooling System
GE	General Electric Company
GE-NE	GE Nuclear Energy
HCLPF	High Confidence Low Probability of Failure
HFE	Human Factors Engineering
HP	High Pressure
HPME	High Pressure Melt Ejection
HPNSS	High Pressure Nitrogen Supply System
HVAC	Heating, Ventilation and Air Conditioning
HX	Heat Exchanger
I&C	Instrumentation and Control
I/O	Input/Output
IAS	Instrument Air System
IC	Isolation Condenser
ICD	Interface Control Diagram

ICS	Isolation Condenser System
IEEE	Institute of Electrical and Electronics Engineers
IIS	Iron Injection System
IVR	In-Vessel Retention
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
MAAP	Modular Accident Analysis Program
MCCI	Molten Corium-Concrete Interactions
MCS	Minimal Cutset
MOV	Motor-Operated Valve
MSIV	Main Steam Isolation Valve
MSL	Main Steamline
NBS	Nuclear Boiler System
NRC	Nuclear Regulatory Commission
NSSS	Nuclear Steam Supply System
PCCS	Passive Containment Cooling System
PCS	Power Conversion System
PRA	Probabilistic Risk Assessment
PSA	Probabilistic Safety Assessment
PWR	Pressurized Water Reactor
RAM	Reliability, Availability and Maintainability
RAW	Risk Achievement Worth
RCCV	Reinforced Concrete Containment Vessel
RCCWS	Reactor Component Cooling Water System
RCPB	Reactor Coolant Pressure Boundary
REM	Radiation Dose Equivalence Measure
RG	Regulatory Guide
ROAAM	Risk-Oriented Accident Analysis Methodology

RPS	Reactor Protection System
RPV	Reactor Pressure Vessel
RSS	Remote Shutdown System
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
SAMS	Severe Accident Management Strategy
SAS	Service Air System
SAT	Severe Accident Treatment
SBWR	Simplified Boiling Water Reactor
SDC	Shutdown Cooling
SLCS	Standby Liquid Control System
SMA	Seismic Margins Analysis
SRP	Standard Review Plan
SRV	Safety Relief Valve
SRVDL	Safety Relief Valve Discharge Line
SSC	Structures, Systems, and Components
SSE	Safe Shutdown Earthquake
TAF	Top of Active Fuel
TDH	Torispherical Drywell Head
TMI	Three Mile Island
TRACG	Transient Reactor Analysis Code
TS	Technical Specification
TSL	Technical Specification Leakage
UCSB	University of California, Santa Barbara
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 purpose and objectives of the design-specific Probabilistic Risk Assessment (PRA) and severe accident evaluations. This section provides an introduction to the regulatory requirements and safety goals associated with the ESBWR PRA, and summarizes how the results of the PRA compare against these safety goals.

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 Revision 1, (Reference 19.1-1) which was docketed as part of the ESBWR DCD application.

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

(1) Demonstrate compliance with any technically relevant portions of the TMI requirements given in 10 CFR 50.34(f);

(2) 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

(3) 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 such that the following goals are achieved:

- Core damage frequency is less than 1 E-4 per year;
- Large release frequency is less than 1 E-6 per year with a Conditional Containment Failure Probability of 0.1 or less;
- Frequency of radiation dose of 0.25 Sv (25 Rem) at the site boundary is less than 1 E-6 per year;
- Overall risks lower than conventional BWRs;
- Identify non-safety functions requiring enhanced regulatory oversight; and
- Assess potential vulnerabilities to not meeting the first 3 goals.

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. More detailed information is provided in reference 19.1-1, to be used by the NRC to facilitate the review of these 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.

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.

Section 19.5 addresses commitments and COL action items as they pertain to the PRA and severe accident management.

The overall conclusions of the PRA and severe accident evaluations are presented in Section 19.6.

19.1.4 References

19.1-1 GE Energy, "ESBWR Design Certification Probabilistic Risk Assessment," NEDO-33201, Revision 1, September 2006.

Table 19.1-1
ESBWR Comparison To Safety Goals

SAFETY GOAL	ESBWR COMPARISON AGAINST GOAL
Core damage frequency (CDF) of $\leq 10^{-4}$ per year of reactor operation	ESBWR baseline PRA CDF is significantly less than 10^{-4} per year of reactor operation. This is true even if only safety-related and RTNSS equipment are credited, or if no operator action is assumed for 72 hours (with credit for non-safety equipment)
The expected mean frequency of occurrence of events that result in a large release of radioactivity shall be $\leq 10^{-6}$ per year of reactor operation considering both internal and external events.	ESBWR baseline PRA LRF is significantly less than 10^{-6} per year of reactor operation. This is true even if only safety-related and RTNSS equipment are credited, or if no operator action is assumed for 72 hours (with credit for non-safety equipment) Conservative analysis of external events resulted in an LRF that is much smaller than the internal events contribution
The containment conditional failure probability (CCFP) should not exceed 0.1 when weighted over credible core damage sequences	The ESBWR CCFP is significantly less than 0.1 when weighted over credible core damage sequences that occur when the containment is required to be operable.
The containment should maintain its role as a reliable, leak-tight barrier for approximately 24 hours following the onset of core damage under the more likely severe accident challenges and, following this period, the containment should continue to provide a barrier against the uncontrolled release of fission products	The ESBWR meets this containment performance goal with considerable margin. The more likely severe accident sequences do not result in containment failure for 72 hours or more. The low frequency severe accident sequences do not result in containment failure in less than 24 hours. Severe accidents that can cause containment failure in less than 24 hours have a frequency low enough to be considered remote and speculative.
The probability of exceeding a whole body dose of 0.25 sv (25 Rem) at a distance of 805 m (one half mile) from the reactor shall be less than one in a million (10^{-6}) per reactor year.	The probability of a release that would exceed a dose of 0.25 sv (25 Rem) at a distance of 0.5 miles from the plant is significantly less than 10^{-6} per reactor year.

Table 19.1-2
Systems and Functions Modeled

System	Functions Modeled
Reactor Depressurization System	Depressurization (SRV or DPV) Overpressure Protection Containment Isolation
Isolation Condenser System	Reactor Heat Removal Containment Isolation
Control Rod Drive System	RPV Injection at High Pressure
Standby Liquid Control System	Boron Injection
Instrument and Control System	Nonsafety-Related Multiplexing Nonsafety-Related Signals ADS Inhibit Feedwater Runback RPV Isolation Safety-Related Multiplexing Safety-Related Signals
Gravity Driven Cooling System	RPV Short/Long Term Low Pressure Injection Injection from Equalizing Lines
Fuel & Auxiliary Pool Cooling System	Suppression Pool Cooling Low Pressure Coolant Injection IC/PCC Pool Makeup from Fire Water RPV Injection from Fire Water
Reactor Water Cleanup & Shutdown System	Shutdown Cooling Containment Isolation
Feedwater and Condensate System	RPV Injection at High Pressure Containment Isolation BOP Heat Sink Component Cooling
Reactor Component Cooling Water System	Reactor Building Component Cooling
Plant Service Water System	Component Cooling Ultimate Heat Sink

Table 19.1-2
Systems and Functions Modeled

System	Functions Modeled
Instrument Air System (IAS) Service Air System (SAS)	Valve Motive Power Valve Motive Power
High Pressure Nitrogen Supply System	Valve Motive Power
AC Power Distribution System Uninterruptible AC Power System 250 VDC Power System	AC Power Onsite AC Power Uninterruptible AC Power DC Power
Containment System	Containment Vent Containment Isolation
Passive Containment Cooling System	Containment Ultimate Heat Sink

Table 19.1-3
Importance Analysis Results

SSC	BASIS	COMMENTS
B21 Nuclear Boiler System		
SQUIB VALVE F004A,B,C,D,E,F,G,H	RAW, FV, CCF	The Depressurization Valves (DPVs) automatically actuate to reduce reactor vessel pressure so that passive Gravity Driven Cooling injection may be used to maintain reactor vessel level.
CHECK VALVE F102A,B CHECK VALVE F103A,B	FV, RAW FV, RAW	Check Valves in Feedwater lines prevent backflow during loss of Feedwater scenarios.
C12 Control Rod Drive System		
CRD PUMP 1A,B	FV, RAW	Control Rod Drive Pumps provide high pressure makeup to the reactor vessel.
MOV F014A,B MOV F020A,B	FV, RAW FV, RAW	MOVs provide flow control to allow CRD injection into the reactor vessel.
C51 Neutron Monitoring		
APRM	CCF	For ATWS mitigation, ADS has an automatic inhibit of the automatic ADS initiation. Automatic initiation of ADS is inhibited after there is a coincident low reactor water level signal and an average power range monitors (APRMs) ATWS permissive signal (i.e., APRM signal above a specified setpoint.) The same inhibit condition applies to GDCS function.
C62, C74 Instrumentation, Logic and Control		
Voter Logic Unit Train A,B	RAW, CCF	The Voter Logic trains in each division are redundant but not independent modules. Each of the redundant pairs of VLUs receives the trip status from the Digital Trip Modules in all four divisions and performs 2-out-of-4 and 3-out-of-4 logic to determine the actuation status for each system function.
E50 Gravity Driven Cooling System		
SQUIB VALVE F002A,B,C,D,E,F,G,H	FV, RAW, CCF	Injection mode squib valves automatically actuate on ECCS signals.
CHECK VALVE F003A,B,C,D,E,F,G,H	FV, RAW, CCF	Check valves in the injection lines prevent backflow from the reactor vessel into the GDCS pools during the time when GDCS injection squib valves have actuated on low reactor vessel level and reactor vessel is depressurizing, but pressure is higher that drywell pressure.

Table 19.1-3
Importance Analysis Results

SSC	BASIS	COMMENTS
G21 Fuel and Auxiliary Pool Cooling System		
AOV F332 CHECK VALVE F331, F333	FV, RAW FV, RAW	A FAPCS line discharges water to RWCU/SDC which sends it to the feedwater system to be injected into the RPV when the FAPCS operates in the LPCI mode. This line is provided with an air-operated gate valve, F332, and an air-operated testable check valve, F333, downstream of it.
H23 Remote Multiplexing Units		
RMUs	FV, RAW, CCF	The RMUs in each division are redundant but not independent modules.
N21 Condensate and Feedwater System		
AOV F018 AOV F023, F026	FV, RAW FV, RAW	Condensate discharge valve and Hotwell makeup valves are necessary for condensate and feedwater operation.
P21 Reactor Component Cooling Water System		
AOV F022A,B AOV F025A,B	RAW RAW	The flow rate for each heat exchanger train is regulated by the bypass valves (P21-F022A/B) and the exchanger discharge valves (P21-F025A/B). Both valves are pneumatic. The flow through these valves regulates the temperature of the cold leg water supply temperature.
P41 Service Water System		
PUMPS	CCF	Service Water Pumps supply cooling water to RCCW and TCCW.
FANS	CCF	Cooling Tower Fans provide heat removal for service water.
R10 500 kV		
Transmission Line	RAW	Loss of incoming transmission lines results in loss of preferred power scenario.
R11 Transformers		
Breakers for Transformers	FV, RAW	The 13.8kV and 6.9kV power distribution system receives power from the unit auxiliary transformers. During normal power operation, the unit auxiliary switchgear buses receive power from the main generator through the generator breaker and the unit auxiliary transformers. If the main generator trips, the low voltage generator breaker opens and power to the unit auxiliary transformers is backfed from the normal preferred power (utility power grid).

Table 19.1-3
Importance Analysis Results

SSC	BASIS	COMMENTS
R13 Uninterruptible AC Power Supply System		
Buses Breakers	RAW RAW	The safety-related Uninterruptible Power Supply consists of four divisions. Division 1 and 2 include two separate units. One unit supplies 120 V single-phase power and the other unit supplies 480 V AC three-phase power. Divisions 3 and 4 supply 480 V AC three-phase power. Each unit has two power supplies. The main source is from 250 VDC. The auxiliary source is through a voltage regulatory transformer supplied by 480 VAC.
R16 DC POWER		
Batteries	FV, RAW	The safety-related DC distribution system is arranged in four divisional class 1E 250V DC power supplies. Each DC train consists of a battery, battery charger, and DC distribution panels. Divisions 1 and 2 have two separate DC systems. One of the systems has a battery sized to provide power for a 24-hour period. The other system has a battery sized to provide power for a 72-hour period.
R21 Diesel Generator		
Diesel Generators	RAW, FV, CCF	Alternate AC power supply for loss of preferred power scenarios.
R22		
Breakers	RAW, FV	480 V AC circuit breaker protection.

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 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-S-2002 capability category 3 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.

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, Large Release Frequency, and importance measures such as F-V and RAW for major component functions. In particular, the ESBWR design certification PRA shows that the design meets the following goals:

- Core damage frequency is less than 1 E-4 per year;
- Large release frequency is less than 1 E-6 per year with a Conditional Containment Failure Probability of 0.1 or less;
- Frequency of radiation dose of 0.25 Sv (25 Rem) at the site boundary is less than 1 E-6 per year;
- Overall risks lower than conventional BWRs;
- Identify non-safety functions requiring enhanced regulatory oversight; and
- Assess PRA potential vulnerabilities to not meeting the first 3 goals.

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 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 major risk insights that have been applied to the conceptual design of the ESBWR.

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:

(1) Identify the systems that should have enhanced regulatory oversight (Reference: DCD Tier 2 Appendix 19B);

(2) Provide an independent assessment of the set of surveillance intervals and allowed outage times in the technical specifications (Reference: DCD Tier 2 Chapter 16);

(3) Identify the most important operator action categories in support of the man-machine interface (Reference: DCD Tier 2 Chapter 18); and

(4) 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.

19.2.2.2 COL Application Phase

19.2.2.2.1 Use of PRA in Support of Licensee Programs

The PRA in the COL phase is used in support of licensee 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 Licensee Programs

The PRA in the Construction phase is used in support of licensee 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 Licensee Programs

The PRA in the Operational phase is used in support of licensee 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 the licensee.

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 section is to provide the insights of the plant specific PRA for full power operations for internal and external events.

19.2.3.1 Risk from Internal Events

Identification of Internal Initiating Events

Internal initiating events are those events that occur either as a direct result of equipment failure, or as the result of errors while performing maintenance, testing, or other operator actions. These events occur during normal power operations. Initiating events are based on NUREG/CR-5750 (Reference 19.2-1). These frequencies are considered 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. These features are listed in Table 19.1-2.

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

- Transients
  - Generic Transient (Turbine trip or spurious reactor trip)
  - Transient with power conversion system unavailable
  - Loss of feedwater transient
  - Loss of the plant service water system (including the loss of the Reactor Component Cooling Water system)
  - Inadvertent opening of an SRV
  - Loss of Preferred Power.
- 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
  - Breaks in pipes connected to the vessel below the top of fuel.

  The size 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 those that are larger than CRD capacity.

- Anticipated Transients Without Scram (ATWS)

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

- Breaks Outside Containment

Acceptance Criteria for Internal Events

The acceptance criteria for the critical safety functions that are required for 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.

Event Tree Development of Internal Events

The event tree methodology is used to represent the possible sequences of events following any one of the initiating event groups defined above. Each event tree sequence depicts a possible combination of system and operator action successes or failures leading to either a successful cooling of the core or to core damage according to the acceptance and success criteria. This method provides a time-independent representation of each accident sequence[1].

The event trees developed in the ESBWR PRA are:

- General Transient
- Transient with PCS Unavailable
- Loss of Feedwater Transient

1 Historically it has been used to represent sequences that occur within a 24 hour period, thus the time independence is a reasonable simplification. In the ESBWR PRA, certain sensitivity analyses are performed for longer time periods. These sensitivities must be viewed in light of the limitations of the simplifications employed in the methodology.

- Loss of Service Water System
- Loss of Preferred Power Transient
- Inadvertent Opening of a Relief Valve
- ATWS from Generic Transient or LOPP
- ATWS from Transient Loss of PCS
- ATWS from Transient with Loss of Feedwater System
- ATWS from Transient with Loss of Service Water System
- ATWS from Inadvertent Opening of a Relief Valve
- Large steam breaks other than Feedwater lines
- Large steam breaks on Feedwater (A) line
- Large steam breaks on Feedwater (B) line
- Small steam breaks
- Medium liquid breaks other than RWCU/SDC lines
- Medium liquid breaks in RWCU/SDC lines
- Small liquid LOCA other than RWCU/SDC lines
- Small liquid LOCA in RWCU/SDC lines
- Reactor Vessel Rupture (as an extension of other event trees)
- Steam break outside containment on Main Steam lines
- Steam break outside containment on Feedwater A lines
- Steam break outside containment on Feedwater B lines
- Large steam break outside containment on IC lines
- Large liquid break outside containment on RWCU/SDC lines.

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 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 19.1-2 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

Two accident sequences are important for internal events. They are initiated by either a Loss of Preferred Power, or a Loss of Feedwater[2]. The only credible way to have a total loss of feedwater event is to lose power to the feedwater control system. A LOPP is also assumed to cause an immediate loss of Feedwater, so the plant response is similar in both sequences. Following the initiating event, a plant scram occurs because of the loss of power to the feedwater controllers. The level in the downcomer (thus the measured level in the reactor) quickly drops to below level 1½. This begins a timer as input to the ECCS logic system such that if the water level is not recovered above level 1½ within 15 minutes ADS is initiated. It takes 2 CRD pumps running in high pressure injection mode to recover level within the time allotted. In these sequences, this CRD function has failed, so the blowdown occurs as designed. As a result of the depressurization, ICS is considered unavailable and cannot provide continuous decay heat removal. Core level could be maintained by a single CRD pump, but in these sequences, both CRD trains have failed to provide injection flow. Low pressure injection is required. The sequence includes failure of the passive GDCS due to hardware failures and failure of the active low pressure injection systems due to either operator error or hardware failures. Core damage is assumed to occur with the reactor vessel at low pressure.

There is only one important post-initiator operator action in the internal events full power PRA. This is failure to recognize the need for low-pressure makeup following a failure of the passive GDCS. The only recovery action that is modeled in the design PRA is the recovery of offsite power. The values for these actions are derived from industry data and are assumed to be applicable to the ESBWR design configuration.

In the ESBWR design PRA, the CDF is dominated by common cause failures of equipment. This is because of the extensive redundancy and diversity inherent in the design. The important common cause terms are the failure of ECCS squib valves. The important individual component random failures in the internal events PRA are feedwater line check valves fail to open and CRD injection line check valve fails to open.

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.

---

2 In the ESBWR, only a total loss of feedwater is explicitly modeled. A partial loss would behave similar to a general transient if there were any affect on plant operation at all.

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 the passive vapor suppression function. The depressurization functions are successful, but 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 19.3.2.2.

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, 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 important sequence for over pressurization starts with a LOPP, followed by a common cause failure of the safety-related batteries. This prevents depressurization and CRD high-pressure injection. The isolation condensers are designed to initiate on a loss of DC power, but there is only water on the shell side for 24 hours of decay heat removal. The loss of DC power prevents the supplemental water from the dryer / separator pit from being available to the ICS. In this sequence the operators fail to provide supplemental post-24 hour water using the fire water system. 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 (Subsection 19.3.2.3), but the containment heat removal functions are required for long term cooling. For the same reasons that prevent ICS from providing long-term heat removal, the PCCS also does not function. The loss of DC power prevents the active Fuel and Auxiliary Pool Cooling system performing the backup function. The containment ultimately fails or is vented when the containment pressure exceeds the ultimate strength (Subsection 19.3.2.4). In either case, a large release is assumed to occur at approximately 32 hours following the LOPP event.

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 the goal of 1E-6/yr.

19.2.3.1.4 Summary of Important Results and Insights of Internal Events

Table 19.2-3 summarizes the important initiating events, operator actions, common cause failures, SSCs, assumptions, and insights from importance, sensitivity, and uncertainty analyses.

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. 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, i.e., any fire in any fire area will cause the worst damage; a fire ignition in any fire area continues to grow unchecked into a fully-developed fire without credit for fire suppression; and the analysis does not take credit for the distance between fire sources and targets. The purpose of the analysis is to show that core damage frequency due to fire is a non-significant 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 (as described above) 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.

19.2.3.2.2 Significant Core Damage Sequences of External Event Fire

The important accident sequences involve a fire in the Turbine Building. The fire analysis conservatively assumes that a Turbine building fire fails the feedwater and condensate systems, thus constituting a Loss of Feedwater initiating event with a loss of the service air system. Following the fire, a plant scram occurs because of the loss of power to the feedwater controllers. The level in the downcomer (thus the measured level in the reactor) quickly drops to below level 1½. This begins a timer as input to the ECCS logic system such that if the water level is not recovered above level 1½ within 15 minutes ADS is initiated. It takes 2 CRD pumps running in high pressure injection mode to recover level within the time allotted. In these sequences, this CRD function has failed, so the blowdown occurs as designed. As a result of the depressurization, ICS is considered unavailable and cannot provide continuous decay heat removal. Core level could be maintained by a single CRD pump, but in these sequences, both CRD trains have failed to provide injection flow. Low pressure injection is required. The sequence includes failure of the passive GDCS due to hardware failures and failure of the active low pressure injection systems due to either operator error or hardware failures. Core damage is assumed to occur with the reactor vessel at low pressure.

Important operator actions in the full power internal fires PRA are:

- Failure to recognize the need for low-pressure makeup; and
- Failure to recognize the need for RPV depressurization.

The bounding fire analysis only adds one important component failure mode to the ESBWR risk profile. This is the failure of a Reactor Building fire barrier failure.

Important assumptions from the fire analysis are as follows:

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.

19.2.3.2.3 Significant Large Release Sequences of External Event Fire

Due to the bounding method that is used to calculate the fire core damage frequency, it is considered to be unnecessary to extrapolate large release frequency calculations. The important fire sequences do not challenge any of the passive containment cooling systems or the BiMAC. There is also no potential for EVE sequences initiated by a fire event. Therefore the internal events containment performance insights can be directly used for fire sequences.

19.2.3.2.4 Significant Offsite Consequences of External Event Fire

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

19.2.3.2.5 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 core damage frequency 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.

Table 19.2-3 summarizes the important initiating events, operator actions, common cause failures, SSCs, assumptions, and insights from importance, sensitivity, and uncertainty analyses.

19.2.3.3 Evaluation of External Event Flood

19.2.3.3.1 Introduction to Evaluation of External Event Flood

The objective of the ESBWR internal probabilistic flood analysis is to identify and provide a quantitative assessment of the core damage frequency 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 spraying or dripping of water from pipe breaks or fire protection equipment onto equipment is also considered in the analysis assuming the loss of all the components that can be affected by the water and are located in the sprayed zone.

This analysis is a bounding approach that begins by assigning a flood initiation frequency to every flood scenario in a building that is equal to the entire flood initiation frequency for that building. Following the accident sequence quantification, the flood scenario with the highest CDF in each building is used to represent the flood CDF for that building. The total flood risk is the sum of the CDFs of the bounding flood scenario for each building.

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.

19.2.3.3.2 Significant Core Damage Sequences of External Event Flood

The important flood initiating event in the full power internal flooding PRA is a Circulating Water System pipe break in the Turbine Building. The flood is assumed to cause an immediate Loss of Feedwater initiating event and the failure of the RCCWS. A plant scram occurs because of the loss of the feedwater controllers. The level in the downcomer (thus the measured level in the reactor) quickly drops to below level 1½. This begins a timer as input to the ECCS logic system such that if the water level is not recovered above level 1½ within 15 minutes ADS is initiated. It takes 2 CRD pumps running in high pressure injection mode to recover level within the time allotted. In these sequences, this CRD function has failed, so the blowdown occurs as designed. As a result of the depressurization, ICS is considered unavailable and cannot provide continuous decay heat removal. Core level could be maintained by a single CRD pump, but in these sequences, both CRD trains have failed to provide injection flow. Low pressure injection is required. The sequence includes failure of the passive GDCS due to hardware failures and failure of the active low pressure injection systems due to either operator error or hardware failures. Core damage is assumed to occur with the reactor vessel at low pressure.

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

Similar to the internal events analysis, the important SSC random failures in the external flooding PRA are feedwater line check valves failing to open and CRD check valve F022 fails to open.

During the initial phase of the ESBWR design, a significant flood risk in the Control Building due to a break in Fire Protection System pipes was identified. Based on this PRA insight, the design specifications now require that the FPS pipes and fire hose stations are located in the stairwells. This feature eliminates nearly all risk due to such flood sources.

19.2.3.3.3 Significant Large Release Sequences of External Event Flood

Due to the bounding method that is used to calculate the fire core damage frequency, it is considered to be unnecessary to extrapolate large release frequency calculations. The important fire sequences do not challenge any of the passive containment cooling systems or the BiMAC. There is also no potential for EVE sequences initiated by a fire event. Therefore the internal events containment performance insights can be directly used for fire sequences.

19.2.3.3.4 Significant Offsite Consequences of External Event Flood

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

19.2.3.3.5 Summary of Important Results and Insight of External Event Flood

Table 19.2-3 summarizes the important initiating events, operator actions, common cause failures, SSCs, assumptions, and insights from importance, sensitivity, and uncertainty analyses.

19.2.3.4 Evaluation of External Event High Wind

19.2.3.4.1 Introduction to Evaluation of External Event High Wind

The ESBWR high wind analysis explicitly quantifies accident sequences initiated by tornado winds. Straight winds are lesser velocity winds that pose minimal challenges to the plant design. Hurricane winds are very site specific and therefore are not this analysis. Due to the strength of construction of the ESBWR Category I buildings, the effects of a tornado strike are limited to Loss of Preferred Power events with a potential loss of the Condensate Storage Tank. Overall risk from tornados and 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 24-hour operational life.

19.2.3.4.2 Significant Core Damage Sequences of External Event High Wind

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

19.2.3.4.3 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.

19.2.3.4.4 Significant Offsite Consequences of External Event Flood

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

19.2.3.4.5 Summary of Important Results and Insights of External Event High Wind

Table 19.2-3 summarizes the important initiating events, operator actions, common cause failures, SSCs, assumptions, and insights from importance, sensitivity, and uncertainty analyses.

19.2.3.5 Evaluation of External Event Seismic

19.2.3.5.1 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 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 strong magnitude earthquakes.

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

19.2.3.5.2 Significant Core Damage Sequences of External Event Seismic

A Seismic Margins Analysis is used to derive seismic vulnerability insights. Therefore, there are no CDF calculations performed. The Seismic Margins Analysis concludes that the most significant HCLPF sequences are seismic-induced loss of preferred 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.

19.2.3.5.3 Significant Large Release Sequences of External Event Seismic

A Seismic Margins Approach is used to derive seismic vulnerability insights. Therefore, there are no LRF calculations performed.

19.2.3.5.4 Significant Offsite Consequences of External Event Seismic

A Seismic Margins Approach 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.

19.2.3.5.5 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:

(1) The ESBWR is inherently capable of safe shutdown in response to strong magnitude earthquakes.

(2) 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 section 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 (i.e., Power Operations, Startup, Hot Shutdown, Stable Shutdown). The shutdown model covers Modes 5 and 6 (i.e., Cold Shutdown and Refueling). A detailed PRA has been performed to determine the core damage frequency 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 of 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;
- RWCU/SDC Drain Line Break Below TAF – Mode 6, Flooded;
- Instrument Line Break Below TAF – Mode 6, Unflooded; and
- LOPP – Mode 6, Unflooded.

Three of the ensuing 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 Reactor Building Division I and Division II Zones during Mode 5. The analysis conservatively assumes that a fire in these zones could cause the inadvertent opening of an SRV. 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 recognize the need for RPV depressurization, and failure to start a condensate pump.

The important individual SSC failure for fire scenarios is Reactor Building fire barrier failure.

19.2.4.1.3 Flooding During Shutdown

The important flood initiating event in the shutdown internal flooding PRA is 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. The important common cause failure in the shutdown tornado PRA is CCF of all batteries. 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

The Seismic Margins Analysis for shutdown concludes that the most significant HCLPF sequences are seismic-induced loss of preferred power.

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.

19.2.4.1.6 Shutdown PRA Assumptions

Important design assumptions in the shutdown analysis are as follows:

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 back-seating of the control rod drive mechanism (CRDM) is the same as the one used in the BWRs and 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, i.e., Refueling Mode. The dominant initiating events are line breaks from lines penetrating the reactor vessel, and loss of preferred power. In these 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:

(1) All 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.

(2) 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

Table 19.2-3 summarizes the important initiating events, operator actions, common cause failures, SSCs, assumptions, and insights from importance, sensitivity, and uncertainty analyses. The greatest contribution to shutdown risk comes from breaks in lines connected to the vessel below TAF that occur in Mode 6. In this mode, 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).

In order to minimize the risk from these scenarios during refueling outages procedures shall require personnel to be available and in close proximity to the hatches, with the purpose of providing fast closure of the containment in the event of a water leak. Other measures can be taken, including temporary installation of equipment to aid in closing the hatch or to minimize the flooding rate in the lower drywell.

The next largest contribution to shutdown risk is due to LOPP scenarios. The contribution from LOPP initiated scenarios is due in part to the need for electric power for alignment of FPS injection to the RPV. Electric power is required to reposition a valve in the injection piping.

However, LOPP scenarios are slowly developing events because of the mass of water that must boil away prior to core uncovery and damage. Thermal-hydraulic calculations show that the core will not begin to uncover before approximately 23 hours following the loss of power, allowing significant time for recovery of offsite power that will enable the operators to provide injection to reflood the core.

The main conclusion that can be drawn from the ESBWR shutdown risk analysis is that the ESBWR containment and reactor systems provide a robust, passive means for preventing shutdown core damage events. The key risk insight is that the shutdown process should provide assurance that the equipment and personnel hatches in the lower drywell can be isolated in the event of a leak.

19.2.5 Summary of Overall Plant Risk Results and Insights

This section provides the overall results and insights from the plant specific PRA. In particular, it identifies the plant features, including nonsafety-related systems, and operator actions that are important to reducing risk and confirm that the expectation stated in 10 CFR 52.79(a)(2) is met. This section description includes a PRA-based insights table that identifies the PRA-based insights that ensure the assumptions and plant operational features addressed in the PRA will remain valid in the as-built, as-to-be-operated plant.

19.2.6 References

19.2-1 NUREG/CR-5750, Rates of Initiating Events at U.S. Nuclear Power Plants: 1987 - 1995, December 1998.

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).	ESBWR front-line safety functions have significantly less reliance on supporting systems and are not sensitive to variations in supporting system reliability.
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.	
AOOs (transients)	
Important contributor for most plants because of reliance on support systems; failure of such systems can defeat redundancy in front-line systems.	ESBWR passive features have significantly less reliance on supporting systems.
Noted variability in the probability that an operator will fail to depressurize the vessel for low pressure injection in BWRs	ESBWR does not require operator actions for successful event mitigation until 72 hours, thus there is significantly less reliance on successful operator actions.
Susceptibility to harsh environment affecting the availability of coolant injection capability following loss of decay heat removal.	Harsh environment primarily affects motors and pump seals in BWRs and is not important to ESBWR risk.
Ability to cross-tie systems to provide additional redundancy.	In ESBWR, the cross-tie potential has been identified at the design stage and is an integral part of the design.

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 24 and 72-hour batteries. 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 cornpartmentalization 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.
<u>LOCAs</u> BWRs generally have lower LOCA CDFs than PWRs for the following reasons: • BWRs have more injection systems • 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.

Table 19.2-1
Comparison of ESBWR Features With Existing BWRs

NUREG-1560 IPE Key Observations	ESBWR Features
ISLOCA Small contributor to plant CDF for BWRs and PWRs because of the low frequency of initiator.	 Also a small contributor to ESBWR CDF. The design of the ESBWR reduces the possibility of a LOCA outside the containment by designing to the extent practical all piping systems, major system components (pumps and valves), and subsystems connected to the reactor coolant pressure boundary (RCPB) to an ultimate rupture strength at least equal to the full RCPB pressure.
Early Containment Failure Overpressure failures (primarily from ATWS), fuel coolant interaction, and direct impingement of core debris on the containment boundary are important contributors to early failure for BWR containments. The higher early structural failures of BWR Mark I containments versus the later BWR containments are driven to a large extent by drywell shell melt-through.	 The ESBWR is designed to minimize the effects of direct containment heat, ex-vessel steam explosions, and core-concrete interaction.
Containment Bypass Bypass is generally not important for BWRs.	 Bypass is not important for ESBWRs due to the containment isolation functions, and no reliance on venting for containment heat removal.

Table 19.2-1
Comparison of ESBWR Features With Existing BWRs

NUREG-1560 IPE Key Observations	ESBWR Features
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.

Table 19.2-1
Comparison of ESBWR Features With Existing BWRs

NUREG-1560 IPE Key Observations	ESBWR Features
Station Blackout	
With the SBO rule implemented, the average SBO CDF is approximately 9E-6/yr. Although the majority of the plants that implemented the SBO rule have achieved the goal of limiting the average SBO contribution to core damage to about 1E-5/yr, a few plants are slightly above the goal.	Implementing the design requirements in the 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 pump headers minimizes Large LOCA potential • Smaller diameter piping connected to vessel below core elevation
Isolation Condenser System • Redundant and Diverse active components • Cooling Pools vs. shell-side heat exchangers • No operator actions required for first 72 hours • Independent of AC and DC Power to operate
Gravity Driven Cooling System Eliminate reliance on pumps and motor-operated valves
Passive Containment Cooling System • No active components • No operator actions required for first 72 hours • 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
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
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

Item	Insight/Assumption	Comment	Disposition
1. Core Damage Prevention			
1a	Loss of Preferred Power is an important initiating event.	Reliability of offsite power sources cannot be completely controlled by the plant. However, to assure that plant equipment does not contribute to power losses, inspection of equipment that connects the plant to the switchyard should be performed periodically in accordance with the RAP.	RAP
1b	Total Loss of Feedwater is an important initiating event.	The design of the feedwater system precludes any single failure from causing this initiator. The digital feedwater control system is a key ingredient to keeping this initiator low. It should be monitored in accordance with the RAP.	RAP
1c	Failure to Recognize Need for Low Pressure Makeup is an important post-initiator operator action.	This insight is covered in operator training and operating procedures.	Procedures Training
1d	Failure to Recover Offsite Power is an important recovery factor.	This insight is covered in operator training and operating procedures.	Procedures Training
1e	The GDCS pools and the suppression pool are instrumented and alarmed such that inadvertent draining of a pool would be immediately obvious to the crew and pool level would be restored.	This is an important indicator for prompt operator recovery action. Should be covered in operator training and operating procedures.	Procedures Training
1f	Important common cause failures are CCF of squib valves in GDCS lines.	The GDCS squib valve pyrotechnic charges shall be replaced during refueling in accordance with the RAP.	RAP
1g	An alarm located within the control room alerts the operator if the battery connection switch is inadvertently left open after test or maintenance.	This insight is covered in operator training and operating procedures.	Procedures Training
1h	Condensate pump discharge header valve F018 and Condensate pump discharge header bypass valve F016 are assumed to be air operated valves that fail to remain open on a loss of air supply.	Design requirement to support condensate system operation.	Design
1i	The opening of SRVs alone is sufficient for reactor depressurization to allow low pressure injection.	It is a design requirement for this function to be able to be accomplished, including margin.	Design

Table 19.2-3
Risk Insights and Assumptions

Item	Insight/Assumption	Comment	Disposition
1j	RCCW heat exchanger discharge valves open, heat exchanger bypass valves close, and cross connection valves fail as is, given a loss of pneumatic supply.	Design requirement to support PRA success criteria for RCCW.	Design
2. Important Functions Core Damage Mitigation And Severe Accident Response			
2a	Use of AC independent components of the fire water system to provide long term cooling.	The fire water system is capable of providing long term cooling water to the ICS, PCCS, and spent fuel pools that is independent of the safety-related systems and the onsite AC power system. Operator alignment of these systems should be covered in training and emergency response procedures. Flow and flow monitoring instrumentation from the fire protection system to these pools should be monitored and tested according to the RAP. All piping that provides this function of the FPS should be monitored and tested in the RAP.	Design Procedures Training RAP
2c	The nitrogen supply and battery capacity are sufficient to allow vessel depressurization after potential ICS failures.	Insights that are covered in operator training and operating procedures.	Procedures Training
2d	An inerted containment prevents hydrogen-oxygen concentrations from reaching combustible levels.	Design Requirement	Design
2e	Containment isolation prevents or mitigates releases.	Tested in accordance with Tech Spec Surveillance Requirements	Design RAP
2f	Upgraded low pressure piping for reactor coolant pressure boundary prevents interfacing systems LOCAs.	Design Requirement	Design
2g	Drywell-Wetwell Vacuum Breakers ensure containment integrity and sufficient pressure differential to drive PCCS.	The failures of these vacuum breakers to close can be kept to an acceptably low probability if they are incorporated into the RAP.	RAP
2h	The failure rate of the GDCS deluge system is not to exceed 1E-3 per demand. It is assumed that the system will be sufficiently independent from any core damage prevention systems to maintain this level of reliability.	Design requirement to support the mitigation effectiveness of GDCS/BiMAC.	Design
2i	Basemat Internal Melt Arrest and Coolability Device (BiMAC) mitigates vessel melt-through scenarios.	Inspection of the BiMAC device should be in the RAP.	RAP

Table 19.2-3
Risk Insights and Assumptions

Item	Insight/Assumption	Comment	Disposition
2b	Logic to Prevent Spurious Actuation of GDCS Deluge Subsystem.	In order to ensure a dry cavity at the time of vessel failure, it is important to prevent premature or spurious actuation of the passive deluge valves. Reliability of the Deluge Squib valves and actuation logic are in the RAP.	Design RAP
2j	For ATWS mitigation, Automatic initiation of ADS is inhibited after there is a coincident low reactor water level signal and an average power range monitor (APRM) ATWS permissive signal (i.e., APRM signal above a specified setpoint.) The same inhibit condition applies to GDCS function.	Logic functional testing to be in accordance with technical specifications.	RAP
2k	Check valves in the GDCS injection lines prevent backflow from the reactor vessel into the GDCS pools during the time when injection squib valves have actuated on low reactor vessel level and reactor vessel is depressurizing, but pressure is higher than drywell pressure.	The testable GDCS check valves shall be tested periodically to ensure the disk readiness to function, both to open, if required, and to close in case of spurious opening of the squib valves. During refueling, an inspection of the strainers of the GDCS equalizing lines connected to the suppression pool shall be performed to prevent potential undetected obstructions.	RAP
2l	The flow rate for each RCCW heat exchanger train is regulated by the bypass valves and the exchanger discharge valves. Both valves are pneumatic.	Risk significant These valves should be tested in accordance with the RAP.	Design RAP
2m	Service Water Pumps supply cooling water to RCCW and TCCW. Cooling Tower Fans provide heat removal for service water.	Risk significant These pumps and fans should be tested in accordance with the RAP.	RAP
2n	Loss of incoming transmission lines results in loss of preferred power scenario. If the main generator trips, the low voltage generator breaker opens and power to the unit auxiliary transformers is backfed from the normal preferred power (utility power grid).	Risk significant Reliability of offsite power sources cannot be completely controlled by the plant. However, to assure that plant equipment does not contribute to power losses, inspection of switchyard equipment should be performed periodically in accordance with the RAP.	RAP

Table 19.2-3
Risk Insights and Assumptions

Item	Insight/Assumption	Comment	Disposition
2p	The safety-related DC distribution system is arranged in four divisional class 1E 250V DC power supplies.	Risk significant Station emergency batteries receive periodic checks in accordance with plant Technical Specifications. These checks are adequate to ensure that the batteries will have the reliability assumed in safety analyses and that the possibility of common cause failures is minimized.	RAP
2q	Diesel Generators provide backup source of AC power for loss of preferred power events.	Risk significant Maintenance for the emergency diesel generators is expected to be performed in accordance with site procedures and the manufacturer's recommendations. Surveillance testing is required in accordance with manufacturer recommendations and best industry practices.	RAP
2r	Redundant motor operated valves interconnecting reactor well pool with IC/PCC pools to extend water inventory from 24 to 72 hours have been identified as important components.	These valves should be tested in accordance with the RAP.	RAP
2s	A high DW temperature could be caused by accidents such as LOCAs, inadvertent opening of one DPV, or loss of the drywell cooling system. The instrumentation is assumed to be designed for the maximum temperature attainable in the DW.	Design requirement that level sensors are designed for the maximum temperature attainable in the drywell.	Design
2t	An FPS pump is assumed to have the same head and flow capacity as an FAPCS pump.	This supports the assumption that FPS can provide makeup injection to the vessel in some low pressure sequences.	Design
2u	One FAPCS system train can also accomplish the long-term heat removal.	FAPCS suppression pool cooling provides long-term decay heat removal in certain sequences.	Design
2v	The FAPCS and FPS injection capability provides adequate core cooling for transients given successful DPV or ADS valve operation, even if containment pressure is at the ultimate containment pressure.	This assures that injection from FAPCS and FPS is available in sequences with high containment pressure.	Design
2w	Room cooling is not required for first 24 hours of the accident.	Design requirement to support PRA success criteria for RCCW.	Design
2x	All loads needed for the PRA are specified/required to be cooled with at least n+1 redundancy.	General design requirement to support PRA success criteria for cooling functions.	Design

Table 19.2-3
Risk Insights and Assumptions

Item	Insight/Assumption	Comment	Disposition
2y	Specific guidance for the use of the suppression pool vent has not been developed, thus, venting is assumed to occur when the containment pressure reaches 90% of the ultimate containment strength.	Design requirement to support successful containment venting.	Design Procedures Training
2z	Vent operation is modeled using the operator action for venting containment. It is assumed that the vent can be operated (manually) independently of any Level 1 mitigation systems.	Design requirement to prevent venting failure due to common causes.	Design Procedures Training
3. External Events			
3a	Fire in Turbine Building is an important fire initiating event.	Fire barriers, including penetrations, are tested in accordance with fire protection requirements.	Design RAP
3b	Fire in Reactor Building	Fire barriers in the Reactor Building are important for keeping the fire risk low.	Design RAP
3c	Reactor Building flood design	Penetrations to the Control Building are located at elevations above the worst-case flood level to prevent flooding into the Control Building.	Design
3d	Control Building flood design	Fire main pipes are located external to the building to minimize flood potential.	Design
3e	If automatic actuations fail, the operators may manually perform the necessary recovery actuations from the remote shutdown panels.	The remote shutdown panel should be tested periodically to show that it can perform its functions that will lead to safe shutdown. Operators should be trained and instructed in the use of controls in the remote shutdown panels. Instruction should be prepared to decide in which condition the control room must be evacuated.	Procedures Training

Table 19.2-3
Risk Insights and Assumptions

Item	Insight/Assumption	Comment	Disposition
3f	A Circulating Water System pipe break in the turbine building is an important flood initiating event.	Periodically, room barriers should be inspected to ensure that they will prevent the spread of flooding; room drain lines should be checked to ensure no blockage exists; Circulating Water isolation valves should be stroke tested (normally accomplished by switching from an operating pump to a standby pump in a given loop); the ability of Circulating Water pump circuit breakers to trip upon receipt of a trip signal should be demonstrated; and level sensors in the turbine building must be periodically tested to show their functionality.	Design RAP
3g	Risk from tornado strikes on the plant is acceptably low.	Site response procedures address actions to take for high winds. No additional controls are warranted.	Design
3h	The HCLPF analysis identifies seismic-induced loss of DC power and seismic-induced ATWS due to seismic-induced failure of both the fuel channels and the SLC tank as important scenarios.	No maintenance activities other than those already associated with the in-service surveillance of the seismic instruments are needed for seismic events.	Design RAP
4. Shutdown			
4a	Important initiating events in the internal events shutdown PRA are: • Instrument Line Break Below TAF – Mode 6. • RWCU/SDC Drain Line Break Below TAF – Mode 6, Flooded. • Instrument Line Break Below TAF – Mode 6, Unflooded. • LOPP – Mode 6. • CRD line break in the Reactor Bldg. – Mode 6.	Piping integrity is assured by the in-service inspection and testing programs. Given the importance of LOPP to shutdown PRA, inspection and testing of the AC-independent fire protection system in vessel injection mode should be included in RAP. Also, due to the importance of manual alignment, lining up the firewater should be included in the training programs.	Design Procedures Training RAP
4b	An important operator action in the shutdown internal flooding PRA is the failure to recognize the need for low-pressure makeup.	Insights that are covered in operator training and operating procedures.	Procedures Training
4c	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.	Insights that are covered in operator training and operating procedures.	Procedures Training

Table 19.2-3
Risk Insights and Assumptions

Item	Insight/Assumption	Comment	Disposition
4d	Breaks in lines connected to the vessel below the core elevation are important scenarios during shutdown Mode 5. In this mode, the lower drywell equipment hatch or personnel hatch is likely to be open to facilitate work in the lower drywell.	The loss of reactor coolant inventory control function during mode 5 underscores the importance of keeping the lower drywell personnel and equipment hatches closed as long as possible. The lower drywell hatches (equipment and personnel) must remain open only when personnel are working inside the lower drywell, and not left open otherwise. Whenever the hatches are open, procedures shall require personnel to be available and in close proximity to the hatches, with the purpose of providing fast closure of the containment in the case of a water leak.	Procedures Training
4e	During shutdown, Mode 5, with the reactor cavity not flooded, it is important to ensure that the GDCS squib valves do not inadvertently actuate.	Controls on maintenance on GDCS components during Mode 5 when reactor cavity has not been flooded are managed in accordance with 10 CFR 50.65 (a)(4), i.e., Maintenance Rule.	RAP
4f	Relative insights from the shutdown Fire PRA assume the proper functioning of fire barriers to prevent propagation of fires to adjacent zones.	Fire barriers are inspected and maintained in accordance with Fire Protection Program procedures.	RAP

Table 19.2-4
ESBWR Systems and Structures in Seismic Margins Analysis With HCLPF > 2

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 HCLPF > 2

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

DPV
- DPV

GRAVITY-DRIVEN COOLING
- Check valve
- Squib valve
- Piping

VACUUM BREAKERS
- Vacuum breaker valve

PASSIVE CONTAINMENT COOLING
- Heat Exchanger
- Piping

IC/PCC POOL INTERCONNECTION
- Valve (motor operated)

FIRE PROTECTION WATER SYSTEM
- Pump (diesel driven)

19.3 SEVERE ACCIDENT EVALUATIONS

19.3.1 Severe Accident Preventive Features

19.3.1.1 Anticipated Transients Without Scram

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, a fast 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 Class 1E 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 Class 1E system independently isolates itself from the non-Class 1E system, and power to safety-related loads of each safety-related load division is provided uninterrupted by the Class 1E batteries of each division. The divisional batteries are sized to provide power to required loads for a minimum of 24 or 72 hours, depending on the division and the load requirement, without the need for recharging. In addition, devices that monitor the input voltage and frequency from the non-Class 1E system, and automatically isolate the division on degraded conditions, protect each division of the Class 1E 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 non-Class 1E 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 (i.e., 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 upon opening of the condensate return valves to initiate the system. ICS also provides the reactor with initial depressurization before ADS in event of loss of feed water, such that the ADS can take place from a lower water level.

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 section 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.

Analysis Assumptions

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

- Reactor power is 102% of rated
- G(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%
- Adequate gas mixing throughout containment

Analysis Results

The analysis results show that the time required for the oxygen concentration to increase to the de-inerting value of 5% is significantly greater than 24 hours for a wide range of fuel clad-coolant interaction and iodine release assumptions up to and including 100%. Thus, the containment failure due to combustible gas deflagration 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.
- 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.

In accordance with Regulatory Guide 1.7 Revision 3, an acceptable method for demonstration of containment structural integrity is to meet the ASME Section III acceptance criteria as follows:

(1) 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, Sub article NE - 3220, Service Level C Limits, considering pressure and dead load alone (evaluation of instability is not required).

(2) Concrete containments meet the requirements of the ASME Boiler and Pressure Vessel Code, Section III, Division 2, Sub article CC - 3720, Factored Load Category, considering pressure and dead load alone.

The governing pressure is calculated to be 1.182 MPa, which is controlled by buckling strength of the drywell head.

The PCCS heat exchangers are part of containment boundary. The Level C pressure capacity of the most critical component in the PCCS heat exchangers is calculated to be 1.33 MPa.

Level C pressure capability of the concrete containment is evaluated to meet the liner strain limits stipulated in ASME Section III, Division 2, CC-3720. A nonlinear finite element analysis of the containment concrete structure including liner plates is performed for over-pressurization. The analysis results show that when the internal pressure reaches as high as 1.468 MPa, the maximum liner strain is only 0.165% tension, which is well within the 0.3% limit for Factored Load Category specified in ASME Table CC-3720-1. Thus, Level C pressure capacity of the concrete containment is at least 1.468 MPa and it is higher than the 1.182 MPa controlling pressure for the steel components. This analysis is presented 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 no penetrations that require isolation to prevent significant offsite consequences. Thus, the probability of the bypass failure mode is dominated by a common isolation signal failure probability, resulting in a calculated frequency of containment bypass about four 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; i.e., 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)

19.3.2.7 Containment Isolation

The ESBWR containment design to 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 non-essential 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 addressed in detail 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 non safety-related, active vent is acceptable.

19.3.4 Equipment Survivability

The safety-related SSCs that are required for severe accident response are designed to withstand the severe accident environments they would experience in postulated accident scenarios, for the duration of the period in which they are needed, including the effects of pressure, temperature, and radiation. The ESBWR design considers the following attributes:

- SSCs required for severe accident response from the PRA End States;
- Accident conditions for each end state (e.g., submerged, high temperature, high radiation);
- Functional performance criteria for each SSC, including mission times; and
- Design requirements for each SSC relative to temperature, pressure, water, and radiation.

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 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 more than 24 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.

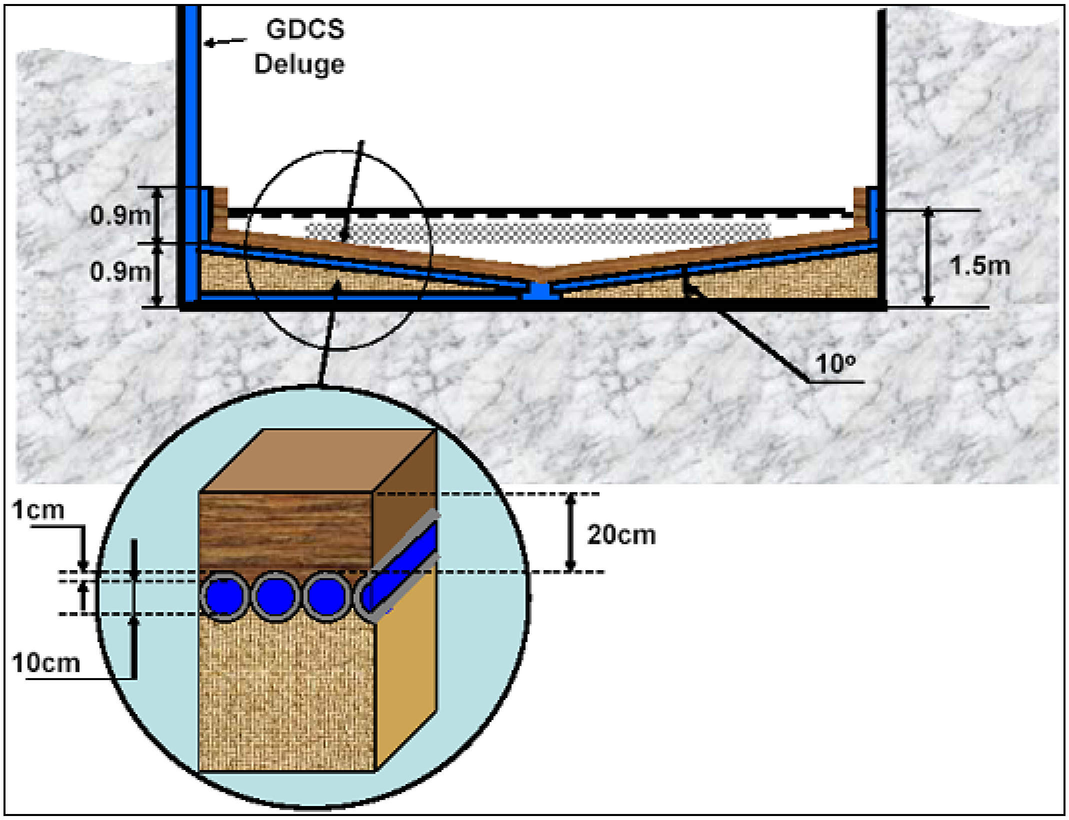


Figure 19.3-1. BiMAC Pipes and Protective Ceramic Layer

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

19.4 PRA MAINTENANCE

19.4.1 Description of 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, controls are implemented to:

- Monitor PRA inputs and collect new information;
- Maintain and upgrade the PRA model;
- 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

In order to ensure that the PRA model maintains the appropriate scope, level of detail and technical adequacy, it is initially reviewed in a peer review process, using the guidance in ASME RA-S-2002, "Standard for Probabilistic Risk Assessment for Nuclear Power Plant Applications." The PRA model may be updated by the COL holder to meet the standards necessary for specific risk-informed applications. Standards are assessed in a peer review process, which uses the ASME guidance. Findings from the peer review, i.e., facts and observations are identified and incorporated into the PRA model. Subsequent updates to the PRA model are processed and controlled by the licensee. They are necessary incorporate plant changes that have been implemented since the date of the current PRA model and updates to component failure data and initiating event frequencies based on in-house and industry operating experience.

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:

(1) 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.

(2) 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.

(3) 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 every other fuel cycle, not to exceed 5 years. The licensee maintains this information in accordance with documentation and records retention requirements.

19.4.2 Description of Significant Plant, Operational, and Modeling Changes

19.4.2.1 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.

19.4.2.2 COL Application Phase Changes

Not Applicable

19.4.2.3 Construction Phase Changes

Not Applicable

19.4.2.4 Operational Update Phase Changes

Not Applicable

19.5 COL Information

Action Items

- Develop guidance to control the opening of the lower drywell hatches during shutdown conditions.
- Provide program procedures for maintenance and update of PRA.
- Provide program document for the reliability assurance program.
- Update the PRA during the construction phase of the project.
- Implement a severe accident management program in accordance with NEI 91-04, Revision 1, "Severe Accident Issue Closure Guidelines."

19.6 CONCLUSIONS

The PRA and severe accident evaluations contained in this chapter 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.

Core damage frequency is significantly less than the NRC Safety Goal of 1 E-4 per year, and the large release frequency is also less than the 1 E-6 per year NRC Safety Goal. The conditional probability of containment failure Probability is less than 0.1 when all credible severe accident scenarios are considered.

From the perspective of public health and safety, the frequency of radiation dose of 0.25 Sv at the site boundary is less than 1 E-6 per year.

Operating experience and PRA insights have been used extensively to improve upon the design of conventional BWRs. This includes passive engineered safety systems that require little or no human actions during the early stages of a transient or accident. In cases where active systems support or interact with these passive features, they have been evaluated to determine if their functions warrant enhanced regulatory oversight.

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

19A.1 INTRODUCTION

Nonsafety-related systems that are identified as risk-significant are designated as RTNSS candidates and are considered for regulatory oversight.

SECY-94-084, "Policy and Technical Issues Associated with the Regulatory Treatment of Non-Safety Systems in Passive Plant Designs," outlines a process that includes the use of both probabilistic and deterministic criteria to achieve the following objectives:

(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:

(1) 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).

(2) SSC functions relied upon to resolve long-term safety (beyond 72 hours) and to address seismic events.

(3) 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.

(4) 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.

(5) SSC functions relied upon to prevent significant adverse systems interactions.

19A.1.1 Selection of Important Non-Safety Systems

For the purpose of this report, SSCs that are candidates for regulatory oversight are referred to as "RTNSS candidates." They are identified using a systematic approach to evaluate these objectives. Criteria A, B, D and E are assessed using deterministic methods, including an assessment of containment performance. Any outliers identified in this process are noted as candidates for RTNSS and are considered for regulatory oversight. 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 results are compared to the NRC safety goals of CDF less than 1 E-4 per year and LRF less than 1 E-6 per year. If the probabilistic analyses determine that the NRC Safety Goals cannot be met without certain non-safety systems, they are identified as candidates for RTNSS.

Upon identifying the RTNSS candidates, they are analyzed to determine whether or not regulatory oversight is appropriate. SSCs that are determined to require regulatory oversight are referred to as “RTNSS Systems.

If the quantitative and qualitative analyses determine a RTNSS candidate to be significant to public health and safety then a Technical Specification Limiting Condition for Operation should be established for the system/component, in accordance with 10 CFR 50.36. Otherwise, reliability and availability controls should be assigned in accordance with the Reliability Assurance Program.

19A.2 CRITERION A: BEYOND DESIGN BASIS EVENTS ASSESSMENT

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. The Standby Liquid Control (SLC) system, used to mitigate an ATWS event, is classified as safety-related. Therefore, the SLC system is not a RTNSS candidate based on Criterion A.

Station Blackout Assessment

Response to an SBO event is analyzed in Subsection 15.5.5 of the DCD. The analysis demonstrates that reactor water level is maintained above the top of active fuel. With operation of 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

Actions Required Beyond 72 Hours

One function that requires manual actions to maintain the plant in a safe shutdown condition after 72 hours is the need to provide makeup water to the upper containment pools, i.e., Passive Containment Cooling (PCC), Isolation Condenser (IC), and Spent Fuel pools. This has been addressed in the plant design by including permanently installed piping in the Fuel and Auxiliary Pool Cooling System (FAPCS), which connects directly to the site Fire Protection System (FPS). This connection enables the pools to be filled with water from FPS, which is capable of providing makeup water to extend the cooling period from 72 hours through 7 days.

FPS is designed so that portions of the system remain operable following a seismic event. These portions include the diesel driven pump in the Fire Protection 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.

RTNSS Criterion B applies to selected portions of the ESBWR fire protection system.

Seismic Assessment

The seismic margins analysis performed for the ESBWR assesses the seismic ruggedness of plant systems, both safety-related and nonsafety-related. The conclusion is that no accident sequence has a HCLPF lower than 0.60 g, which is twice the magnitude of the safe shutdown earthquake (SSE).

Therefore, there are no RTNSS candidates due to seismic events based on Criterion B.

19A.4 CRITERION C: PRA MITIGATING SYSTEMS ASSESSMENT

Focused PRA Sensitivity Study

A focused PRA sensitivity study has been performed to evaluate whether passive systems alone are adequate to meet the NRC safety goals of CDF less than 1 E-4 per year and LRF less than 1 E-6 per year. Any nonsafety-related systems that are needed to reduce CDF or LRF results to meet the safety goals are RTNSS candidates. The focused PRA retains the same initiating event frequencies as the baseline PRA, and the safety-related system failure probabilities also remain unchanged. The CDF for the focused PRA is lower than the NRC safety goal.

In addition, the results of the internal events PRA are evaluated in containment event trees to calculate an LRF value for the focused PRA, which is also lower than the NRC safety goal.

The sensitivity of non-safety systems to shutdown risk is also considered to be negligible. Insights from the baseline Shutdown results indicate that the dominant risk contributor is a LOCA in an instrument line located below the top of active fuel. LOCAs during shutdown are mitigated by passive GDCS injection. The other major contributions from loss of shutdown cooling and loss of preferred power are less significant and, therefore, would not be expected to identify any non-safety systems as candidates for regulatory oversight.

The conclusion is that the NRC safety goals are met without the need for active safety systems. Therefore, there are no additional candidates for RTNSS from the Focused PRA.

Assessment of Non-Safety Systems on External Events

The risk impact of non-safety systems relative to external events, at power and during shutdown, has been determined to have a negligible effect on the CDF and LRF goals.

Assessment of Uncertainties

Some non-safety SSCs are considered for regulatory oversight because of uncertainties inherent in their passive safety functions. An evaluation of these types of uncertainties, such as squib valve reliability, identified no RTNSS candidates. However, there are uncertainties in the design of Basemat-Internal Melt Arrest and Coolability System (BiMAC) device because it is a new component that at this time has not been tested. Therefore, the BiMAC device is a RTNSS candidate.

PRA Initiating Events Assessment

The At-Power and Shutdown PRA models have been 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) Could these non-safety SSCs significantly contribute to the occurrence of an initiating event?

(2) Do these non-safety SSCs have a significant impact on CDF and LRF?

If the answer to both of these questions is “Yes”, then the non-safety SSC is a RTNSS candidate.

Based on the systematic evaluation of initiating events for at-power and shutdown conditions, there are no candidates for regulatory oversight from initiating events.

19A.5 CRITERION D: CONTAINMENT PERFORMANCE ASSESSMENT

The containment performance goal in SECY-93-087, Issue I.J is addressed in detail in NEDO-33201 Section 8.2, “Frequency of Overpressure and Bypass Release Categories,” and Section 8.3, “Containment Performance Against Overpressure.”

The containment bypass issue from SECY-93-087, Issue II.G, during severe accidents is concerned with potential sources of steam bypassing the suppression pool and failure of heat exchanger tubes in passive containment cooling systems. These concerns are addressed in the Design Control Document. Subsection 6.2.1.1.5 addresses the steam bypass of the suppression pool. 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

A systematic approach identifies and analyzes potential adverse effects that active systems may impose upon passive safety systems. Overall, the design features incorporated into the ESBWR utilize extensive operating experience, standards and regulations to provide adequate protective measures against the potential for adverse systems interactions. Therefore, there are no RTNSS candidates identified based on the potential for adverse systems interactions.

19A.7 SELECTION OF IMPORTANT NON-SAFETY SYSTEMS

The following non-safety systems have been determined to be candidates for regulatory oversight.

Fire Protection Makeup to Upper Containment Pools

The FPS makeup to the upper containment pools should be considered for regulatory oversight in accordance with Criterion B, long-term actions, i.e., actions required beyond 72 hours to ensure safe shutdown conditions. The FPS is classified as nonsafety-related but is designed so that portions of the system remain operable following a seismic event. These portions include the diesel driven pump in the Fire Protection 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.

Basemat-Internal Melt Arrest and Coolability System (BiMAC)

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 1 E-3. BiMAC plays an important role in mitigating core melt scenarios, therefore, it is a candidate for RTNSS consideration.

19A.8 PROPOSED REGULATORY OVERSIGHT

Fire Protection Makeup to Upper Containment Pools

FPS makeup to the upper containment pools is a RTNSS candidate in accordance with Criterion B, actions that are required beyond 72 hours to ensure safe shutdown conditions. This function does not affect the level 1 PRA results, which terminate after 24 hours, nor does it measurably affect the LRF. Therefore, the relative risk significance is low.

The proposed level of regulatory oversight is to include the FPS makeup function and related components within the Reliability Assurance Program.

Basemat-Internal Melt Arrest and Coolability System (BiMAC)

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 good heat transfer between a 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. BiMAC device failure could occur if there were no water 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.

The proposed level of regulatory oversight is to include the BiMAC function and related components within the Reliability Assurance Program.

Appendix 19B. CONTAINMENT ULTIMATE STRENGTH

19B.1 INTRODUCTION

This section describes the analysis and evaluation used to estimate the containment internal pressure capability and associated failure mode and location. The ultimate pressure capability of the containment structure is limited by the drywell head whose failure mode is plastic yielding of the torispherical dome. The calculated containment pressure capability is discussed in NEDO-33201, Section 8.0. The containment is conservatively assumed to depressurize rapidly when the pressure capability is reached. No significant leakage through penetrations is anticipated before the capability pressure is reached.

The primary function of the containment structure is to serve as the principal barrier to control potential fission product releases. The design basis event for this function is a postulated loss-of-coolant accident (LOCA). Based on this functional requirement, the containment pressure vessel is designed to withstand the maximum pressure and temperature conditions which would occur during a postulated LOCA. The ESBWR containment system employs pressure suppression, which allows a design pressure of 0.310 MPa and a design temperature of 444ºK (340°F) for the primary containment pressure vessel. In addition, the suppression pool retains fission products that could be released in the event of an accident. In this section the capability of the containment structural system of the ESBWR standard plant to resist potentially higher internal pressures and temperatures associated with severe accidents is evaluated.

Primary containment, also referred to as "RCCV" for reinforced concrete containment vessel, is a cylindrical structure of steel-lined reinforced concrete. The containment is integrated with the reactor building (RB) walls from the basemat up to the elevation of the containment top slab. The top slab, together with pool girders and building walls, form the IC/PCCS pools and the services pools for storage of Dryer/Separator, fuel handling, new fuel storage and other uses. The containment is divided by the diaphragm floor and the vent wall into a drywell chamber and a suppression chamber or wetwell chamber. The drywell chamber above the diaphragm floor is called the upper drywell (U/D). The drywell chamber enclosed by the RPV support pedestal (a part of RCCV) beneath the RPV is called the lower drywell (L/D). The major penetrations in the containment wall include:

- Drywell head;
- The upper drywell equipment and personnel hatches at azimuth 307° and 52°;
- The lower drywell personnel and equipment hatches at azimuth 0° and 180°;
- The wetwell hatch at azimuth 115º; and
- The main steam and feedwater pipe penetrations at the level of the steam tunnel.

Additional detail of the containment design is provided in Section 4.0.

The pressure boundary of the containment structure consists of the reinforced concrete containment vessel (RCCV) and the steel drywell head. The structural integrity of the RCCV is investigated for its global strength under internal pressure beyond the design basis using the ANSYS computer program, which is based on the nonlinear finite element method of analysis for 3D reinforced concrete structures. During various severe accident conditions, the ESBWR containment could also be challenged by high temperatures with a typical temperature of 533ºK (500°F) for most accident sequences). At typical accident temperature of 533ºK (500°F), the calculated pressure capability is associated with the plastic yielding of the drywell head. For a postulated severe accident with hydrogen generation equivalent to 100-percent metal-water reaction of the fuel cladding, the maximum calculated containment pressure is less than the calculated containment pressure capability.

In order to evaluate liner response to over-pressurization, liner plates are included in the ANSYS analysis. The analysis results show that the liner strains are much smaller than the ASME code allowable for factory load category when the internal pressure is as high as 1.468 MPa. A separate evaluation further demonstrates that at the calculated containment pressure capability, the liner and anchor system will maintain its structural integrity and no liner tearing will occur.

The leakage potential through penetrations is expected to be insignificant.

In conclusion, the ultimate pressure capability is limited by the drywell head. The postulated failure mechanism is the plastic yield of the drywell head. The pressure capability evaluation described above is based on the deterministic approach. The uncertainties associated with the failure pressure are assessed in Section 19C-3.

19B.2 RCCV NON-LINEAR ANALYSIS

This subsection describes the non-linear analysis performed for the reinforced concrete containment vessel (RCCV) of the ESBWR Standard Plant. Computer code ANSYS is used for evaluation of the RCCV.

19B.2.1 Finite Element (FE) Model Description

The containment and the containment internal structures (excluding GDCS pools structures) are axi-symmetric while the RCCV top slab together with the reinforced concrete girders even though not axi-symmetric, are idealized and included in the axi-symmetrical model. Solid elements are used to represent the girders at the top of the RCCV, approximating the stiffness of the actual structure from a detailed model of the walls and slabs in the upper pools.

To represent the restraining effects of the floors outside the containment, horizontal restraining slabs are used with equivalent material properties. The model includes concrete elements, the reinforcing steel, the steel liner plate of the drywell, the drywell head, the wetwell with the vent wall and diaphragm floor structures.

The model consists of 3780 nodal points and 2160 elements. There are 1497 elements representing concrete, whereas 249 elements are isotropic, representing steel plates. The soil below the foundation mat is modeled as 72 spring constants, 342 concentrated mass elements.

The ANSYS computer program permits the specification of bi-linear, brittle or ductile material properties. The concrete and soil elements are specified to have properties with no or low tensile capability. The steel plate elements and the rebar elements are specified to have ductile material properties with the same strength in tension and compression. The capability of the ANSYS program to accommodate ductile material behaviors permits both concrete cracking and yielding of steel and rebar. This allows the program to consider redistribution of forces throughout the structure due to the non-linear behavior such as concrete cracking.

19B.2.2 Analysis

The finite element model is analyzed for internal pressure loading incrementally increased up to 1.486 MPa. The four pressure levels whose results are evaluated and summarized in Table 19C-1 are:

- Design pressure, labeled “PD”;
- Structural Integrity Test 1 (SIT-1) pressure, labeled “IT”, with 0.358 MPa pressure in the drywell and wetwell; and
- Severe accident pressures, labeled “SA-1” and “SA-2”.

Because ANSYS performs non-linear analysis, it is necessary to apply simultaneously all loads of a loading combination. In addition to internal pressures, only the dead weights are included. The program utilizes a stepwise linear iteration technique. The first cycle results are for elastic analysis. Based upon results of the first cycle, stiffness of all elements is adjusted by the program prior to the next iteration cycle.

19B.2.3 Results

19CBased on the ANSYS analysis, it can be concluded that the axi-symmetric components of the RCCV, as designed based on ASME Section III Division 2 code requirements, can withstand an internal pressure of 4.8 times the design pressure, with stresses and strains in the rebar, liner plate and concrete within code allowable limits. The strength is governed by the wetwell wall and the S/P slab junction. The strength of the non-axi-symmetric top slab region is evaluated by extrapolation of the elastic analysis results using a 3D finite element model.

Appendix 19C. PREDICTION OF CONTAINMENT ULTIMATE STRENGTH

19C.1 STRUCTURAL CAPABILITY

19C.1.1 Concrete Shell

The structural integrity of the RCCV axi-symmetric components has been demonstrated for an internal pressure of 1.486 MPa at ambient temperature from the ANSYS analysis. Based on extrapolation of analysis results, estimate of the ultimate pressure capability is made and discussed in this subsection. The ultimate pressure capability is assumed reached when rebar at both faces of a cross section reaching yield stress or when concrete fails by shear. During various severe accident conditions, the ESBWR containment could be challenged by high temperatures with a typical temperature about 533ºK (500°F). The effect of elevated temperature on containment pressure capability has been investigated by Argonne National Laboratory (ANL) (Reference 19C-1). The ANL study concluded that for temperatures up to 644ºK (700°F), the failure mode and location do not change from the case of internal pressure alone, and the failure pressure is reduced slightly (11% maximum) from that predicted for the internal pressure alone case. On the basis of the ANL study it is expected that with thermal effects included, the RCCV pressure capability will not be reduced below the drywell head capability for the range of temperatures considered. It is estimated that RCCV pressure capability at 500ºF is 90% of the capacity at ambient temperature.

19C.1.2 Drywell Head

This subsection presents an evaluation of the structural capability of the drywell head under internal pressure and temperature loading. The leakage potential of the head closure is discussed in Subsection 19C.2.2.

The drywell head which covers the 10.4 m diameter opening in the upper drywell top slab is a steel torispherical dome assembly. Under internal pressure loading, the most critical location of this type of configuration is the knuckle (or torus) region of the torispherical dome which may fail by plastic yield or buckling.

For torispherical pressure vessel heads, an approximate formula for the limit pressure at which significant plastic deformation occurs was developed by Shield and Drucker (Reference 19C-2) based on the upper and lower bound theorems of limit analysis, and it is

$$P_c = S_Y \left\{ \left(0.33 + 5.5 \cdot \frac{\mathrm{r}}{\mathrm{D}}\right)\frac{t}{L} + 28(1 - 2.2r/D)\left(\frac{t}{L}\right)^2 - 0.0006 \right\} \quad \text{(19C-1)}$$

where:

P_c = limit pressure

S_y = yield strength of the material

t = uniform thickness of the head

r = radius of the knuckle shell

D = diameter of the cylindrical shell

L = radius of the spherical cap

Substituting the relevant dimensions into Equation 19C-1 gives

$$P = 0.005156 * Sy \tag{19C-2}$$

The material yield strength depends on temperature. The actual strength of as-built material is generally higher than the specified minimum value used in design. To have a more realistic estimate of the structural strength, the minimum yield strength of material SA-516, Gr. 70 as specified in Appendix I of ASME Section III is increased by 10%. The calculated containment pressure capability is at a temperature of 533ºK (500°F). It is noted that due to the presence of water in the reactor cavity, the outer surface of the drywell head will be at a much lower temperature than the inner surface, which is exposed to the drywell temperature. Consideration of the entire drywell head at 500ºF is therefore a conservative assumption.

Buckling is another potential failure mode of the torispherical head under internal pressure because the knuckle is subjected to compressive stress in the hoop direction. Galletly (Reference 19C-3) has proposed a design equation for preventing buckling in fabricated torispherical shells under internal pressure.

$$P_d = \frac{80\, S_y \left(\frac{r}{D}\right)^{0.825}}{\left(\frac{D}{t}\right)^{1.5} \left(\frac{L}{D}\right)^{1.15}} \tag{19C-3}$$

This equation is based on his previous studies (References 19C-4 and 19C-5) and is formulated for design use with knock-down (capacity reduction) factors included. As compared to all known test results (43 in total), the ratios of the actual buckling pressure to the allowable buckling pressure predicted by this equation were found to range from 1.51 to 4.01. Hence, a minimum factor of safety of 1.5 is ensured by this equation.

The test data presented in Reference 19C-3 (excluding the test performed by Blenkin because no buckling was observed at the maximum test pressure) are at least 1.5 times lower than the test results. The cumulative probability is 8% for the ratio up to 1.5. It means that the probability of the ratio of actual to predicted pressure being less than 1.5 is 8%. In other words, there is 92% confidence that the margin of safety against buckling is at least 1.5 when Equation 19C-3 is used. The 1.5 factor of safety corresponding to 92nd percentile is deemed sufficient for the assurance of no buckling failure against severe accident loadings of very low probabilities of occurrence.

As mentioned earlier, Equation 19C-3 has a factor of safety of 1.5 as compared to the lower bound of all known test results. From a statistical study of these test results, the medium buckling pressure is estimated to be 2.27 times the value predicted by Equation 19C-3. Multiplying by the median 2.27 value of Equation 19C-3 results in a best estimate buckling failure pressure for the drywell head of 2.667 MPa.

A comparison with the plastic yield limit pressure P_c calculated above indicates that plastic yield will occur before buckling and is the governing failure mode of the drywell head. PCCS Heat Exchangers Ultimate Pressure Capacity

The PCCS heat exchangers are part of containment boundary. Evaluation is performed to determine their ultimate pressure capacity. Analytical calculations are carried out to obtain the maximum pressure that each heat exchanger component can resist at severe accident temperature, 533ºK (500ºF).

All of the sections that resist the containment pressure are evaluated in accordance with Service Level D limits of ASME, Section III, Division 1, Subsection NC, Class 2 Components.

The evaluation results reveal that the Level D pressure capacity of the most critical component in the PCCS heat exchangers is 1.5 times higher than the pressure capability of the containment structure. The ultimate pressure capability would be even higher; hence the PCCS heat exchangers are not the weak link of the containment pressure boundary.

19C.2 LEAKAGE POTENTIAL

The previous subsection has addressed the structural capability of the containment structures under severe accident conditions. However, the containment function can be compromised if excessive leakage occurs before the capability pressure is reached. Leakage above the design allowable could result from failure of the liner plate and penetrations at high pressures and temperatures. The leakage potential of the liner plate and penetrations is evaluated in the following subsections.

19C.2.1 Liner Plate

As discussed earlier, the containment liner plates are included in the ANSYS model. The maximum liner strains are found to be well within the code allowable when the internal pressure is as high as 1.468 MPa.

At the calculated containment pressure, the maximum liner strain is 0.117% as shown in Table 19C-1 and it is considered as "free-field" strain away from discontinuities such as penetrations. To account for the effects of discontinuities, a strain concentration factor of 33, based on the Sandia containment test results (Reference 19C-6), is conservatively applied to the free-field strain, resulting in 3.96% strain. This strain level is still far lower than the ultimate fracture strain of 21% for the liner plate material. Therefore, it can be inferred that the liner plate will not tear at the calculated containment pressure capability.

The most significant effect of thermal loading on the liner performance is a potential buckling failure that may occur if the internal pressure-induced tensile stress is not large enough to overcome the thermal-induced compressive stress. The thermal buckling tests conducted by Construction Technology Laboratories for Electric Power Research Institute (EPRI), Reference 19C-10, showed no buckling for a peak thermal transient exceeding 600ºF under a pressure of 65 psi. The representative severe accident temperature for the ESBWR containment is 500ºF. Because the increase in internal pressure could be much faster than the heat conduction through the containment wall, it is expected that liner buckling is unlikely to occur under combined pressure and thermal loading associated with severe accidents. As for the thermal effects on linear tearing, an ANATECH study for EPRI (Reference 19C-11) indicated that, for representative reinforced and pre-stressed concrete containment under WASH-1400 severe accident loading, liner tensile yielding occurred at a higher pressure and the end results near failure were essentially the same as compared to the pressure alone case. On this basis, the liner rupture pressure in excess of the calculated containment pressure capability estimated above for pressure alone is judged to be achievable in combination with temperature. In summary, no liner failure that may lead to leakage can occur before the calculated containment capability pressure is reached.

19C.2.2 Penetrations

An ANL study (Reference 19C-8) assigned high priority to the study of large operable penetrations such as the drywell head closure, equipment hatches, and personnel airlocks because they are expected to have high potential for leakage under severe accident conditions. Leakage from fixed penetrations (both electrical and mechanical) appears to be less likely based on the results of experiments conducted to date by Sandia National Laboratories (SNL) and its contractors (Reference 19C-8). In fact, according to the same reference, no leakage was detected from any of the three current electrical penetration assemblies (EPAs) during the severe accident testing (steam environments).

The leakage potential of operable penetrations depends on both the relative position of the sealing surfaces and the performance of the seal material. The position of the sealing surfaces depends on the initial conditions (metal-to-metal contact is maintained under design conditions for most penetrations) and on the deformations induced by accident pressure and temperature. The seal performance depends mainly on temperature as well as the effect of thermal and radiation aging. The recent SNL tests of seals for mechanical penetrations, Reference 19C-8, indicated that

(1) In a steam environment at a constant pressure of 1.069 MPa, the mean degradation temperature was 544ºK (520°F) for silicon rubber and 606ºK (630°F) for ethylene propylene rubber (EPR),

(2) In a nitrogen environment at a constant pressure of 1.069 MPa, the mean degradation temperature was 528ºK (490°F) for neoprene, and

(3) The degradation temperature was not significantly affected by thermal and radiation aging.

Neoprene is not used for operable penetrations in the ESBWR containment and the seal degradation temperature is conservatively assumed to be 533ºK (500°F). The SNL study also showed that even a degraded seal can prevent leakage if the separation of the sealing surfaces is small [less than 0.127 mm (0.005 in.)].

Sandia (Reference 19C-8) has proposed the following equations for “available gasket springback”, Sp, for evaluating the leakage potential as a function of the compression set retention and the degradation temperature:

$$S_p = (1\text{-}C_B)\, S_q h_i \text{ for } (T<T_d) \quad (19C\text{-}4)$$

$$S_p = 0.127 \text{ mm } (0.005 \text{ inch}) \text{ for } (T>T_d) \quad (19C\text{-}5)$$

where:

C_B = the compression set retention (a dimensionless measure of the permanent set in the gasket caused by aging),

S_q = the squeeze 19C(a dimensionless measure of the gasket deformation under normal operation conditions),

h_i = the initial seal height, and

T_d = the degradation temperature of the gasket material.

Equation 19C-4 is based on the assumption that significant leakage can be prevented as long as positive compression of the gasket is maintained. Equation 19C-5 is empirical based on test results that even a degraded gasket can effectively prevent leakage if the separation of the sealing surfaces is equal to or less than 0.127 mm (0.005 in).

For the pressure-unseating drywell head closure and equipment hatches, the pressure required to separate the sealing surfaces is a function of the bolt preload, axial stiffness of the bolts and the compression flanges, and the differential thermal expansion between the bolts and the compression flanges. The separation pressure for operable penetrations typically ranges from 1.1 to 1.5 times design pressure (Reference 19C-8). In this study, the separation pressure is assumed to be the average value of 1.3 times design pressure. At and below this pressure, a metal-to-metal contact is maintained and no leakage other than design allowable leak rate is anticipated, even if the seal degradation temperature of about 533ºK (500°F) has reached. Additional pressure in excess of the separation pressure is carried entirely by the bolts. The separation displacement between the sealing surface after the separation pressure is reached is:

$$s = \frac{\pi r^2 (p - p_s)}{K_b} \qquad (19C\text{-}6)$$

where:

r = the inside radius of the equipment hatch sleeve or drywell head,

p_s = the separation pressure, and

K_b = the total bolt axial stiffness.

The above expression neglects the flexibility due to axial deflection of the compression flanges caused by the Poisson effect which contributes little to the total flexibility of the bolts. This approach for predicting leakage is based on the consideration of structural deformations in terms of separation of connecting flanges of pressure unseating equipment hatches and drywell head. The adequacy of this approach has been recently confirmed by the Sandia hatch leakage tests (Reference 19C-9) in that the predicted leakage onset pressures were in favorable agreement with the test results. The drywell head anchorage to the top slab has a pressure capability higher than the drywell head shell and the leakage path of the drywell head assembly before the failure pressure is reached is through the flanges.

The drywell head is a 10.4-m diameter closure with double seal. One hundred twenty 68-mm diameter bolts hold the head in place. There are 2 drywell equipment hatches and 1 wetwell hatch in the containment wall. All of them have twenty 36-mm minimum diameter bolts with double seal; the diameters are 2.4 m for drywell equipment hatches and 2.0 m for the wetwell hatch. According to Equation 19C-6, the separation displacement at the calculated containment capability pressure is calculated to be about 0.146 mm (0.0058 in) for the drywell head and 0.204 mm (0.008 in) for the most flexible hatch. Although they are larger than the springback displacement of 0.127 mm if gaskets are conservatively assumed degraded at 533ºK (500°F), the resulting maximum gap of 0.077 mm is deemed small. Hence, no significant leakage is expected before the capability pressure is reached.

For equipment hatches, another potential leakage mechanism is ovalization of the sleeve which causes the sleeve to slide relative to the tensioning ring (or the cover flange). An initiation of leakage due to sleeve ovalization, however, requires significant deformations of the containment shell around the equipment hatch. The average circumferential membrane strain in the shell that is needed to result in the initiation of leakage from ovalization for equipment hatches identified in the ANL survey (Reference 19C-8) was found to range from 2.5% to 7.3% by SNL (Reference 19C-8). For the equipment hatches under consideration, the ovalization leakage onset strain, which is the ratio of the sleeve wall thickness at the sealing surface to the sleeve radius ranges, as a maximum, from about 5.8% to 7.0%. At a pressure of 1.468 MPa, the maximum radial deflection of the wetwell wall was calculated to be 13.02 mm (0.512 in.) from the ANSYS analysis (Table 19C-1). The corresponding hoop membrane strain is 0.072%. It is less than 1.2% and no leakage from sleeve ovalization of the equipment hatches will occur before the capability pressure is reached.

19C.3 SUMMARY

The ultimate pressure capability of the containment structure is limited by the drywell head whose failure mode is plastic yield of the torispherical dome. No liner leakage will occur before the calculated containment pressure capability is reached. Leakage through penetrations is expected to be insignificant.

19C.4 UNCERTAINTY IN THE FAILURE PRESSURE

The uncertainties in the prediction of the failure pressure generally result from uncertainties in the two general areas listed below:

- Material Strength (yield strength, tensile strength, modulus of elasticity, etc.)
- Modeling (differences between the model and reality, use of simplified models or empirical correlations, uncertainty in dead-loads, etc.)

In a number of the areas listed above very little data may be available to guide the structural analyst in characterizing the uncertainty. Consequently, it is generally necessary to rely to a large extent on engineering judgment and past results to quantify these uncertainties.

As noted above a significant contributor to the uncertainty in the prediction of ultimate capacity derives from uncertainties in the material properties. For most structural materials the lognormal distribution has been shown to be a good model for the variability in material strength. Largely for this reason the lognormal distribution is generally selected to characterize the uncertainty in the prediction of the ultimate pressure capacity for structural components.

The most common form of the lognormal probability density function is:

$$p_f(p) = \frac{1}{p\sqrt{2\pi}\beta_c} \exp\left[-\frac{1}{2}\left[\frac{1}{\beta_c}\ln\left(\frac{P}{P_{med}}\right)\right]^2\right] \tag{19C-7}$$

where:

$p_f(p)$ = the lognormal probability density function for failure pressure,

β_c = logarithmic standard deviation on the pressure capacity p,

p_{med} = the median pressure capacity.

β_c is a combination of the logarithmic standard deviation of material strength uncertainty β_s, and the logarithmic standard deviation of modeling uncertainty β_m. β_c is determined from the standard relationship for combining independent uncertainties.

$$\beta_c = \sqrt{\beta_s^2 + \beta_m^2} \tag{19C-8}$$

The cumulative distribution function (CDF) is obtained by integrating the PDF

$$P_f(P) = (P \leq p) = \int_o^P p_f(p)\,dp \tag{19C-9}$$

$P_f(p)$ = the probability that the failure pressure is less than pressure p.

The failure pressure, i.e., the calculated containment pressure capability at a drywell temperature of 533 K (500°F), is considered to be a lower bound value because a higher failure pressure of 1.632 MPa would be predicted for the drywell head when plastic failure mode is analyzed with Equation 4 of Reference 19C-5 shown below.

$$P_{c2} = \frac{20(r/D)^{1.78} S_y}{(D/t)^{1.08}(L/D)^{0.87}}\left[1 + 0.1\left(\frac{r}{D}\right)^{-1.37}\right](1 + 0.001 S_y^{1.1}) \tag{19C-10}$$

The median failure pressure is therefore assumed to be 1.632 MPa. The uncertainties associated with this analysis were estimated using engineering judgment and the results from prior analysis. Typical values for the uncertainties associated with material properties of steel structures range from a β_s of approximately 0.06 to 0.10 and the uncertainties associated with the modeling of simple steel structures range from a (β_m) of approximately 0.10 to 0.16 (References 19C-12 and 19C-13). Using nominal values for β_s of 0.08 and for β_m of 0.14 results in an estimated value for the standard deviation (β_c) of 0.16. The use of 0.14 for β_m is also consistent with Reference 19C-14 in that the variability associated with the modeling error by the use of approximate methods including that for torispherical heads is 0.12. The adequacy of using 0.08 for β_s associated with material property uncertainties at high temperatures is addressed as follows. The ESBWR drywell head material is ASME SA-516, Gr. 70. This material was tested, according to Reference 19C-16, for temperatures up to 477 K (400°F) using the specimens taken from the Sandia's 1/8 scale steel containment model. No actual test data are given but the inferred stress-strain curves (Figures 3.4 and 3.5 of Reference 19C-15) for Gr. 60 of the same material considered in the nonlinear analysis show the same characteristics of nonlinear stress-strain relationships for temperatures up to 477 K (400°F). The same trend is expected to exist for temperatures up to 811 K (1000°F) because it is the upper temperature limit at which the specified minimum material strength is given in the ASME code. Having established this, the variability associated with material strength is expected to be the same regardless of temperatures. The statistical data of 52 tests of A516, Gr. 70 (same as SA-516, Gr. 70) given in Reference 19C-16 show that the average yield strength is 335 MPa and the standard deviation is 24.3 MPa. The coefficient of variation is thus 0.073, which is close to 0.08 used for β_s.

The pressure at two standard deviations below the mean is 1.111 MPa. This pressure is 3.58 times the design pressure.

19C.5 REFERENCES

19C-1 Pfeiffer, P. A., Kennedy, J. M., and Marchertas, A. H., Thermal Effects in Concrete Containment Analysis, Fourth Containment Integrity Workshop, June 15-17, 1988.

19C-2 Shield, R. T., and Drucker, D. C., Design of Thin-Walled Torispherical and Toriconical Pressure-Vessel Heads, Journal of Applied Mechanics, Transaction of ASME, June 1961.

19C-3 Galletly, G.D., A Simple Design Equation for Preventing Buckling in Fabricated Torispherical Shells under Internal Pressure, ASME Journal of Pressure Vessel Technology, Vol. 108, November 1986.

19C-4 Galletly, G. D., and Radhamohan, S. K., Elastic-Plastic Buckling of Internally-Pressurized Thin Torispherical Shells, Journal of Pressure Vessel Technology, ASME, Vol. 101, August 1979.

19C-5 Galletly, G. D., and Blachnut, J., Torispherical Shells Under Internal Pressure - Failure Due to Asymmetric Plastic Buckling or Axi-symmetric Yielding, Proc. of Institution of Mech. Engineers, Vol. 199, No. C3, 1985.

19C-6 Clauss, D. B., Round Robin Analysis of the Behaviour of a 1:6 scale reinforced concrete containment model pressurized to Failure: Post-test Evaluations, NUREG/CR-5341 SAND 89-0349, Sandia National Laboratories, October 1989.

19C-7 Not used.

19C-8 Clauss, D. B., von Riesemann, W. A., and Parks, M. B., Containment Penetrations, SAND88-0331C.

19C-9 Parks, M.B., Walther, H.P., and Lambert, L.D., Evaluation of the Leakage Behaviour of Pressure-Unseating Equipment Hatches and Drywell Heads, SAND90180C, 18th Water Reactor Safety Meeting, October 1990.

19C-10 Construction Technology Laboratories, Concrete Containment Tests, Phase 2: Structural Elements with Liner Plates, EPRI NP-4867M. August 1987

19C-11 ANATECH International Corporation, Methods for Ultimate Load Analysis of Concrete Containments: Second Phase, EPRI-NP-4869M, March 1987

19C-12 Peek, R., Wesley, D. A., and Chow, T., Internal Pressure Capacity for the Kuosheng Nuclear Generation Station Containment, SMA 14305.01-RA-A-R001, Appendix to Probabilistic Risk Assessment-Kuosheng Nuclear Capacity Power Station, Vol. 4, Atomic Energy Council, Republic of China, July 1985.

19C-13 Maruvada, S. N., Mauchline, R. L., and Schmehl, R. J., Cleveland Electric Illuminating Perry Nuclear Power Plant Individual Plant Examination Containment Capacity Analysis, Gilbert/Commonwealth Corporation, 1991 (Cleveland Electric Illuminating Proprietary).

19C-14 Reliability Analysis of Steel-Containment Strength, NUREG/CR-2442, June 1982.

19C-15 Analysis of Shell-Rupture Failure Due to Hypothetical Elevated- Temperature Pressurization of the Sequoyah Unit 1 Steel Containment Building, NUREG/CR-5405, February 1990.

19C-16 Realistic Seismic Design Margins of Pumps, Valves, and Piping, NUREG/CR-2137, June 1981.