GE Energy

David H. Hinds
Manager, ESBWR

PO Box 780 M/C L60
Wilmington, NC 28402-0780
USA

T 910 675 6363
F 910 362 6363
david.hinds@ge.com

MFN 06-267

Docket No. 52-010

August 9, 2006

U.S. Nuclear Regulatory Commission
Document Control Desk
Washington, D.C. 20555-0001

Subject: **NEDO-33201, Revision 1, "ESBWR Probabilistic Risk Assessment," Section 19**

Enclosure 1 contains the subject partial ESBWR Probabilistic Risk Assessment (PRA) document (Revision 1).

If you have any questions about the information provided here, please let me know.

Sincerely,

Kathy Sedney for

David H. Hinds
Manager, ESBWR

D068

Enclosure:

1. MFN 06-267 – NEDO-33201, Revision 1, "ESBWR Probabilistic Risk Assessment:"
    - Section 19 – Reliability and Maintainability

cc:	WD Beckner	USNRC (w/o enclosures)
	AE Cubbage	USNRC (with enclosures)
	LA Dudes	USNRC (w/o enclosures)
	GB Stramback	GE/San Jose (with enclosures)
	eDRF	0000-0052-9465

ENCLOSURE 1

MFN 06-267

NEDO-33201, Revision 1, "ESBWR Probabilistic Risk Assessment"

- **Section 19 – Reliability and Maintainability**

19 RELIABILITY AND MAINTAINABILITY

Contents

List of Tables

19 RELIABILITY AND MAINTAINABILITY

19.1 INTRODUCTION

In this section, the results of the PRA are reviewed to determine the appropriate reliability and maintenance actions to be considered throughout the life of an ESBWR plant so that the PRA remains an adequate basis for quantifying plant safety. These actions comprise a part of the plant's reliability assurance program (RAP).

The PRA models at this point in the design phase do not contain specific component logic or reliability data, and may contain conservative values. As the design of the ESBWR becomes finalized, the PRA models will be updated accordingly, and thus will be capable of providing the level of insights that are required for determining operation, maintenance and monitoring activities for the COL applicant to consider.

To determine the appropriate reliability and maintenance-related activities that should be considered to assure that plant safety is maintained as operation proceeds, the results of PRA and other analyses are reviewed. The objective of the review is to determine the relative importance of prevention and mitigation features of the ESBWR in satisfying the key PRA goals related to core damage frequency (CDF) and frequency of offsite release. Also considered are the initiating events that have a significant impact on CDF. This review allows the most important plant features to be identified.

The level 1 PRA evaluates accident sequences from initiating events and failures of safety functions that lead to core damage. An assessment is performed for operating conditions and shutdown conditions. The external events analysis considers events whose cause is external to systems associated with normal plant operations, including internal flooding, fire, high winds, and seismic events. The seismic events were analyzed using a seismic margins approach that provided qualitative conclusions on the ability of ESBWR SSCs to cope with seismic events. The other external events are quantified using the level 1 PRA model. Basic events representing component failures are identified as risk-significant if their importance values for Risk Achievement Worth (RAW) were greater than or equal to 2.0, or Fussell-Vesely Importance (FVI) were greater than or equal to 0.005. The results are summarized in Table 19.2-1.

The level 2 PRA analyzes the plant response to severe accidents and offsite release of fission products. The analysis includes the evaluation of severe accident phenomena and fission product source terms, and containment integrity strategies including pressure suppression, decay heat removal, and hydrogen generation.

In Subsection 19.5, the individual features identified in Subsections 19.2 through 19.4 are reviewed to determine appropriate maintenance and surveillance actions, including implementation in the Reliability Assurance Program (RAP). The objective of the RAP is to ensure safe and reliable design and operation of the ESBWR, consistent with the NRC-established PRA safety goals, by using PRA insights during the design phase to establish risk-based design, operation, maintenance and performance monitoring practices. The process used to determine dominant failure modes is based on the standard PRA modeling practices, e.g., dominant accident sequences, importance analyses and insights. Phase 2 of the D-RAP will identify key assumptions regarding any operation, maintenance and monitoring activities that the

COL applicant will consider in developing the O-RAP to assure that such SSCs can be expected to operate throughout plant life with reliable performance that is consistent with the PRA.

19.2 RISK FROM INTERNAL EVENTS

To determine which plant structures, systems and components (SSCs) are the most important with respect to CDF, the Level 1 analysis results are analyzed. The SSCs are listed in order of Fussell-Vesely (FV) importance, as calculated by the CAFTA code. A second criterion for selecting SSCs is to consider those SSCs with high "risk achievement worth", or the increase in CDF if that SSC always fails. The identified SSCs are grouped by similarity of the functions performed. Basic events representing component failures are identified as risk-significant if their importance values for Risk Achievement Worth (RAW) are greater than or equal to 2.0, or Fussell-Vesely Importance (FVI) are greater than or equal to .005. The results are listed in Table 19.2-1.

The Level 2 analysis evaluates the offsite release of fission products following core damage. Those analyses related to the consequences of core damage were reviewed, including source term sensitivity studies, deterministic analysis of plant performance, and containment event trees. Those systems that would be important with regard to mitigating a core damage event were considered as potentially risk-significant SSCs.

19.2.1 Significant Core Damage Sequences

The internal events CDF is 2.92×10^{-8} per year. The sequence with the highest core damage frequency is a Loss of Preferred Power event. This sequence includes a loss of preferred power, failure of two CRD pumps to maintain RPV water level above level 1.5, RPV depressurizes successfully, and low-pressure injection is unavailable. This Class I accident sequence has a frequency of 1.67×10^{-8} per year, and represents 57% of total CDF.

The sequence with the next highest frequency is a Loss of Feedwater transient with human errors involving mispositioning of injection valves, successful depressurization, common cause failure of the GDCS squib valves, and a failure of the operator to recognize the need for manually aligning injection. This is also a Class I accident sequence, and has a frequency of 1.20×10^{-8} per year, which represents 41% of total CDF.

The dominant initiating events in the internal events full power PRA are:

- Loss of Preferred Power (57% contribution to internal events CDF)
- Loss of Feedwater (41% contribution to internal events CDF)

Each of the remaining initiating events individually represents less than 1% of CDF.

The dominant post-initiator operator actions in the internal events full power PRA are:

- Failure to Recognize Need for LP Makeup (72% contribution to internal events CDF)
- Failure to Start Standby RCCW Pump (2% contribution to internal events CDF)

Each of the remaining operator actions individually represents less than 1% of the internal events CDF.

The dominant recovery action is Failure to Recover Offsite Power. The model includes multiple LOPP recovery actions for different time phases of the LOPP accident progression; collectively they contribute approximately 36% to internal events CDF.

The dominant common cause failures in the internal event full power PRA are:

- CCF of 7 Squib Valves in GDCS Lines (43% contribution to internal events CDF)
- CCF of All Squib Valves (43% contribution to internal events CDF)
- CCF of All DC Batteries (1% contribution to internal events CDF)

Each of the remaining CCF events in the PRA individually represents less than 1% of the internal events CDF.

Important assumptions from the internal events analyses are as follows:

- An alarm located within the control room alerts the operator if the battery connection switch is inadvertently left open after test or maintenance.
- The opening of five SRVs is sufficient for reactor depressurization to allow the low pressure system injection if these systems are available. Either the FAPCS or the Fire Protection System (FPS), in the injection mode, has the capability to successfully perform the coolant makeup function for both the short and long term.

19.2.2 Significant Large Release Sequences

The frequency of a given release category for each initiator is found by quantifying the Containment Phenomena Event Tree (CPET) or Containment Systems Event Tree (CSET) path ending with that release category. To provide the total probability of a release category for all initiators, the CPET is evaluated for each entry event and the probabilities for the failure paths are summed. The remaining fraction is quantified through the CSET logic, and once again the failure paths are summed.

There are two non-negligible paths resulting in a release from the CPET, steam explosion in the lower drywell (representing about 1% of CDF) and failure of the BiMAC thermal barrier (representing about 1% of CDF). These issues are associated with passive components, and would be addressed in the RAP program through inspections. Steam explosions are caused by breaks in pipes connected to the vessel below Level 3 and by breaks in feedwater lines. BiMAC thermal barrier failures are significant because the failure probability was artificially increased to account for uncertainty in the reliability of the first of a kind devise.

The CSET deals with the performance of containment systems, which are better suited for controls in the RAP program. The most likely CSET end state is associated with leakage from an intact containment (representing about 97% of CDF) and is not considered a large release in the ESBWR PRA. Controlled, filtered venting is the next most likely release category (representing about 1% of CDF), but with a release frequency two orders of magnitude lower than the leakage category. Release categories associated with containment failure or bypass are several orders of magnitude less likely than the dominant leakage from intact containment release category.

The large release frequency (LRF) for internal events is estimated to be $1x10^{-9}$ per year.

Because of the passive nature of the ESBWR containment systems, there are no operator actions required to support the containment response to a severe accident in the 24-hour period after onset of core damage. The containment isolation system, vacuum breakers, and PCCS do not require operator action to initiate or function.

The design of the ESBWR containment provides for holdup and delay for fission product release should the containment integrity be challenged. The containment design is a low leakage that is expected to apply to severe accidents. Long-term containment pressurization is governed by the generation of decay heat and non-condensable gases. The primary source of noncondensable gas generation is metal-water reaction of the zirconium in the core. The containment is designed to withstand the generation of 100% metal-water reaction of the clad surrounding the fuel. The ultimate strength capability is important for rapid containment challenges such as direct containment heating and rapid steam generation.

The mitigating systems listed below ensure that the decay energy results in steam production. The suppression pool absorbs this energy, resulting in very slow containment response that ensures ample time for fission product removal. These systems are considered to be important relative to containment and are discussed further in Table 19.5-1.

- AC-Independent Fire Water Addition System
- GDCS Deluge Subsystem
- Containment Inerting System Bleed Line
- Vessel Depressurization
- Inerted Containment
- Containment Isolation
- Upgraded Low Pressure Piping
- Drywell-Wetwell Vacuum Breakers
- Basemat Internal Melt Arrest and Coolability Device (BiMAC)

Important assumptions from the level 2 analyses are as follows:

Operator guidance for the use of the suppression chamber vent to prevent containment overpressurization has not been developed. For modeling purposes, it was assumed that venting would occur only if containment pressure reached 90% of the ultimate pressure capability.

19.2.3 Summary of Important Results and Insights

The results of the PRA analysis demonstrate that the ESBWR is designed with redundant accident prevention and mitigation features that result in CDF and LRF values significantly lower than those of the current generation of light water reactors.

Relative to the very low internal events CDF:

- The dominant initiating events in the internal events analysis for full power operation are a Loss of Preferred Power and a Loss of Feedwater.
- The dominant post-initiator operator actions in the internal events full power PRA the Failure to Recognize Need for LP Makeup.
- The dominant recovery action is Failure to Recover Offsite Power.

- The dominant common cause failures in the internal event full power PRA are of the GDCS Squib valves.

The largest accident class contributor is Class I, which involves core damage events occurring at low RPV pressures with the containment initially intact.

Because of the passive nature of the ESBWR containment systems, there are no operator actions required to support the containment response to a severe accident in the 24 hour period after onset of core damage.

The important results and insights are summarized in Table 19.5-1.

19.3 RISK FROM EXTERNAL EVENTS

19.3.1 Evaluation of External Event Fire

19.3.1.1 Significant Core Damage Sequences

The Fire PRA is a bounding analysis that incorporates several conservative assumptions. Fires are conservatively assumed to propagate unsuppressed in each fire area and damage all functions in the fire area. The analysis assumes that a fire ignition in any fire area continues to grow unchecked into a fully developed fire, and does not account for the amount of combustible material present, or for the distance between fire sources and targets. Due to the bounding approach that was used, it is inappropriate to directly compare CDF value (1.21×10^{-8} per year) from this Fire PRA relative to the internal events PRA. Instead, the qualitative insights from the Fire PRA are considered in the following discussion.

The dominant fire initiating events in the full power internal fires PRA are:

- Fire in Turbine Building (80% contribution to full power fire CDF)
- Fire in Rx Bldg. Division I Zone (6% contribution to full power fire CDF)
- Fire in Rx Bldg. Division II Zone (6% contribution to full power fire CDF)
- Fire in Rx Bldg. Division III Zone (3% contribution to full power fire CDF)
- Fire in Rx Bldg. Division IV Zone (3% contribution to full power fire CDF)

Each of the remaining fire initiating events individually represents less than 1% of the full power internal fires CDF.

The dominant operator actions in the full power internal fires PRA are:

- Failure to Recognize Need for LP Makeup (60% contribution to full power fire CDF)
- Failure to Recognize Need for RPV Depressurization (13% contribution to full power fire CDF)

Each of the remaining operator actions individually represents less than 1% of the full power internal fires CDF.

The dominant common cause failures in the full power internal fires PRA are:

- CCF of 7 Squib Valves in GDCS Lines (35% contribution to full power fire CDF)
- CCF of All Squib Valves (35% contribution to full power fire CDF)
- CCF of DPVs to Open (1% contribution to full power fire CDF)

Each of the remaining common cause failures in the model individually represents less than 1% of the full power internal fires CDF.

The dominant system, structure or component random failures in the full power internal fires PRA are:

- Reactor Building Fire Barrier Fails (16% contribution to full power fire CDF)

- TCCW HXs Bypass Valve Fails to Regulate (9% contribution to full power fire CDF)
- Check Valve #1 in FW Line B Fails to Open (6% contribution to full power fire CDF)
- Check Valve #2 in FW Line B Fails to Open (6% contribution to full power fire CDF)
- CRD Check Valve F022 Fails to Open (6% contribution to full power fire CDF)

Important assumptions from the fire analysis are as follows:

The analysis of fires 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.

19.3.1.2 Significant Large Release Sequences

Due to the bounding method that was used to calculate the fire core damage frequency, it was considered to be unnecessary to extrapolate large release frequency calculations.

19.3.1.3 Summary of Important Results and Insights

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.

The important results and insights are summarized in Table 19.5-1.

19.3.2 Evaluation of External Event Flood

19.3.2.1 Significant Core Damage Sequences

The flood CDF is 3.68×10^{-9} per year for full power. The dominant flood initiating event in the full power internal flooding PRA is a Circulating Water System pipe break in the turbine building, contributing over 99% to the full power internal flooding CDF.

Operator actions are non-significant contributors to the full power internal flooding risk profile. All operator actions in the model individually contribute less than 1% to internal flooding CDF. The highest risk important post-initiator operator action failure in the full power internal floods analysis, using the F-V importance measure, is Failure to Align FAPCS in LPCI Mode (0.2% contribution to full power flooding CDF).

The dominant common cause failures in the full power internal flooding PRA are:

- CCF of 7 Squib Valves in GDCS Lines (41% contribution to full power flood CDF)
- CCF of All Squib Valves (41% contribution to full power flood CDF)

Each of the remaining common cause failures in the model individually represents less than 1% of the full power internal flooding CDF.

In the original development of the fire PRA, the only significant flood risk in the Control Building was represented by the presence of Fire Protection System pipes. To address this, a design requirement was implemented so that the FPS pipes and firehose stations are located in the stairwells. It is also assumed that the plant design directs the flood water out of the building to a dewatering pit, and that this system has sufficient capacity to remove the water flow resulting from an FPS pipe break. In addition, it is assumed that the stairwell doors communicating with the cabinet areas are watertight.

19.3.2.2 Significant Large Release Sequences

Due to the low CDF value, flood-induced external events were not analyzed for large release frequency.

19.3.2.3 Summary of Important Results and Insights

The ESBWR, due to its basic layout and safety design features, is inherently capable of mitigating potential internal flooding. Safety system redundancy and physical separation providing protection from flooding by large water sources, along with alternate safe shutdown features in buildings separated from flooding of safety systems, provide the ESBWR significant flooding mitigation capability.

The important results and insights are summarized in Table 19.5-1.

19.3.3 Evaluation of External Event High Wind

19.3.3.1 Significant Core Damage Sequences

The total core damage frequency for both at-power and shutdown conditions is 4.86×10^{-11} per year (4.77×10^{-11} per year at-power and 8.67×10^{-13} per year during shutdown). 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 are not specifically analyzed in this analysis. This frequency is insignificant in comparison to the internal events result and the core damage frequency goal.

Relative insights from this analysis pertain to the Condensate storage tank and condenser, which are assumed to be vulnerable to tornado effects and no credit is taken for either one. In addition, the power conversion and feedwater systems are assumed unavailable due to loss of offsite power.

19.3.3.2 Significant Large Release Sequences

Due to the low CDF value and the fact that high winds do not affect containment operability as they would in conventional light water reactors, high wind-induced external events were not analyzed for large release frequency.

19.3.3.3 Summary of Important Results and Insights

The main conclusion that can be drawn from the ESBWR tornado risk analysis is that the risk from tornado strikes on the plant is acceptably low. The estimated core damage frequency (both at-power and shutdown conditions) from tornadoes is 4.86×10^{-11} per year. The ESBWR is inherently safe with respect to tornado events and the plant can be safely shut down at low risk to plant personnel and the general public.

19.3.4 Evaluation of External Event Seismic

A Seismic Margins Approach was used to derive seismic vulnerability insights. Therefore, there is no CDF calculation.

The primary containment and the Reactor Building are the Category I structures in the design certification scope with the lowest values of HCLPF, but because both have HCLPF greater than 1.1 no special RAP activities are deemed necessary for these structures. Other SSCs identified by the seismic analysis as being important are as follows:

- The motor control centers of the emergency DC distribution System
- The heat exchangers of the Passive Containment Cooling System and the Isolation Condenser System
- The Fuel Assemblies and Hydraulic Control Units
- The SLC tank of the Standby Liquid Control System
- The diesel-driven pump of the Fire Water System

No accident sequence has a HCLPF lower than 0.60 g. As such, the ESBWR plant and equipment are shown to be capable of withstanding an earthquake with a magnitude at least two times the safe shutdown earthquake.

19.3.4.1 Summary of Important Results and Insights

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 (both 0.62g HCLPF) 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.

19.4 EVALUATION OF OTHER MODES OF OPERATION - SHUTDOWN

19.4.1 Evaluation of Shutdown Mode

19.4.1.1 Significant Core Damage Sequences

The internal events shutdown CDF is estimated at 5.56×10^{-9} per year. The dominant initiating events in the internal events shutdown PRA are:

- Instrument Line Break Below TAF – Mode 6, Flooded (42% contribution to internal events shutdown CDF)
- LOPP – Mode 6, Unflooded (31% contribution to internal events shutdown CDF)
- RWCU/SDC Drain Line Break Below TAF – Mode 6, Flooded (12% contribution to internal events shutdown CDF)
- Instrument Line Break Below TAF – Mode 6, Unflooded (10% contribution to internal events shutdown CDF)
- RWCU/SDC Drain Line Break Below TAF – Mode 6, Unflooded (3% contribution to internal events shutdown CDF)

Each of the remaining initiating events individually represents less than 1% of the internal events shutdown CDF.

The fire CDF for shutdown is conservatively estimated at 2.32×10^{-8} per year. Like the internal events Fire PRA, the shutdown Fire PRA is a bounding analysis that incorporates several conservative assumptions. Fires are conservatively assumed to propagate unsuppressed in each fire area and damage all functions in the fire area. The analysis assumes that a fire ignition in any fire area continues to grow unchecked into a fully developed fire, and does not account for the amount of combustible material present, or for the distance between fire sources and targets. Due to the bounding approach that was used, it is inappropriate to directly compare CDF value from the shutdown Fire PRA relative to the other CDF values. Dominant fire initiating events in the shutdown internal fires PRA are:

- Fire in Rx Bldg. Div. II Zone – Mode 5 (33% contribution to shutdown fire CDF)
- Fire in Rx Bldg. Div. I Zone – Mode 5 (31% contribution to shutdown fire CDF)
- Fire in Rx Bldg. Div. IV Zone – Mode 5 (17% contribution to shutdown fire CDF)
- Fire in Rx Bldg. Div. III Zone – Mode 5 (16% contribution to shutdown fire CDF)

Each of the remaining fire initiating events individually represents less than 1% of the shutdown fire CDF.

The flooding CDF during shutdown is estimated to be 1.64×10^{-9} per year. Dominant flood initiating events in the shutdown internal flooding PRA are:

- CRD Break in Rx Bldg. – Mode 6 (91% contribution to shutdown flood CDF)
- FPS Break in Rx Bldg. – Mode 6 (5% contribution to shutdown flood CDF)

- FPS Break in Fuel Bldg. – Mode 6 (4% contribution to shutdown flood CDF)

Each of the remaining flood initiating events individually represents much less than 1% of the shutdown flood CDF.

Shutdown risks due to high winds are estimated to be 9×10^{-13} per year and are therefore negligible.

Operator actions are non-significant contributors to internal events shutdown risk. The dominant post-initiator operator action in the internal events shutdown PRA is Failure to Recognize Need for LP Makeup (1% contribution to internal events shutdown CDF).

The dominant operator actions in the shutdown internal fires PRA are:

- Failure to Recognize Need for RPV Depressurization
- Failure to Start Condensate or Feedwater Pump

The dominant operator actions in the shutdown internal flooding PRA are:

- Failure to Recognize Need for LP Makeup (57% contribution to shutdown flood CDF)
- Failure to Align FAPCS in LPCI Mode (6% contribution to shutdown flood CDF)

Each of the remaining operator actions individually represents less than 1% of the shutdown internal flooding CDF.

The dominant common cause failure in the internal events shutdown PRA is CCF of All DC Batteries (1% contribution to internal events shutdown CDF).

The dominant common cause failures in the shutdown internal fires PRA are:

- CCF of DPVs to Open (6% contribution to shutdown fire CDF)
- CCF of 7 Squib Valves in GDCS Lines (3% contribution to shutdown fire CDF)
- CCF of All Squib Valves (3% contribution to shutdown fire CDF)
- CCF of 3/4 DTMs of SSLC (1% contribution to shutdown fire CDF)

Each of the remaining common cause failures in the model individually represents less than 1% of the shutdown internal fires CDF.

The dominant common cause failures in the shutdown internal flooding PRA are:

- CCF of 7 Squib Valves in GDCS Lines (38% contribution to shutdown flood CDF)
- CCF of All Squib Valves (38% contribution to shutdown flood CDF)

Each of the remaining common cause failures in the model individually represents less than 1% of the shutdown internal flooding CDF.

Random failures of systems, structures or components are not significant contributors to the internal events shutdown CDF.

The dominant system, structure or component random failures in the shutdown internal fires PRA are:

- Reactor Building Fire Barrier Fails (83% contribution to shutdown fire CDF)

- Diesel Fire Pump Injection Hardware Failure (9% contribution shutdown fire CDF)
- Div. 3 EMS Fails to Function (7% contribution to shutdown fire CDF)
- DTM of SSLC Div. 3 Fails to Trip (6% contribution to shutdown fire CDF)
- DTM of SSLC Div. 4 Fails to Trip (6% contribution to shutdown fire CDF)]

The dominant system, structure or component random failures in the shutdown internal flooding PRA are:

- Diesel Fire Pump Injection Hardware Failure (9% contribution shutdown flood CDF)
- GDCS Pool B in Maintenance (8% contribution to shutdown flood CDF)
- GDCS Squib Valve F009A/D/E/H/I/L Spuriously Opens (5% contribution to shutdown flood CDF for each valve)
- GDCS Squib Valve F009B/C/F/G/J/K Spuriously Opens (3% contribution to shutdown flood CDF for each valve)
- GDCS Squib Valve F009A/D/E/H Fails to Operate (2% contribution to shutdown flood CDF for each valve)

Important design assumptions in the shutdown analysis are as follows:

Compared to Residual Heat Removal System in current 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 current 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 L3 does not constitute an initiating event, as RWCU/SDC will continue to ensure normal core cooling.

19.4.1.2 Significant Large Release Sequences

All evaluated shutdown core damage events are assumed to result in a large release because of the potential for the containment being open during the outage. CCFP is not affected because the containment is not being used as a mitigating system during shutdown.

19.4.1.3 Summary of Important Results and Insights

The dominant initiating events during shutdown are events involving line breaks or loss of preferred power. In general, the time to diagnose and react to shutdown initiating events is much longer than full power operations due to the reduced temperature and pressure conditions. The highest risk important post-initiator operator action failure in the internal events shutdown risk

analysis, using the F-V importance measure, is failure of the operators to close the DW hatch during instrument line break scenarios inside containment.

The important results and insights are summarized in Table 19.5-1.

19.5 RELIABILITY AND MAINTAINABILITY ACTIONS

Actions relative to the reliability and maintainability of ESBWR SSCs are identified and controlled in a Reliability Assurance Program (RAP). The objective of a RAP is to ensure that the reliability of the plant SSCs is maintained to levels at or above those assumed in the PRA. This is accomplished by analyzing the PRA results and other risk important insights to determine the appropriate reliability and maintenance actions to be considered throughout the life of an ESBWR plant so that the PRA remains an adequate basis for quantifying plant safety.

The PRA models in the design phase lack much of the specific component details, logic, and reliability data, and, in some cases, contain conservative values. As the design of the ESBWR becomes finalized, the PRA models will be revised to include the specific information on components, logic, and human interface, and thus will be capable of providing the level of insights that are required for determining operation, maintenance and monitoring activities for the COL applicant to consider. These activities will ultimately be controlled in accordance with the Maintenance Rule program, 10 CFR 50.65, through the identification of risk-significant SSCs, appropriate performance monitoring criteria, and the assessment of as-operated plant risk. In addition, risk-significant SSCs are identified during the COL application process in the Design Control Document, Section 17.4, "Design Reliability Assurance Program." The Design Reliability Assurance Program (D-RAP) is the first stage of the process and applies to reliability assurance activities that occur before the initial fuel load. In the second stage, the Operational RAP (O-RAP), the activities developed in the D-RAP are used to develop reliability and maintainability actions for the operating life of the plant.

At this point in the design phase, general PRA results and insights are assembled in order to identify risk-significance systems and functions that should be maintained in the RAP.

In Table 19.5-1, the risk-significant features identified in Subsections 19.2 through 19.4 are compiled. Some are identified as insights and design requirements that are controlled by the design process. Other items are insights on operations that are covered in operator training and operating procedures. In addition, several items involve component performance. These items are identified as RAP items in the last column on the table.

Table 19.2-1

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

SSC	BASIS	COMMENTS
		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.
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		

SSC	BASIS	COMMENTS
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).
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

SSC	BASIS	COMMENTS
		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 AC Power		
Breakers	RAW, FV	480 V AC circuit breaker protection.

Table 19.5-1

Important Results and Insights

Findings	Comments	RAP
1) Internal events		
a) The sequence with the highest core damage frequency is Loss of Preferred Power 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 switchyard equipment should be performed periodically in accordance with the RAP.	X
b) The next highest frequency stems from a Loss of Feedwater transient with human errors involving mispositioning of injection valves, successful depressurization, common cause failure of the GDCS squib valves, and a failure of the operator to recognize the need for manually aligning injection.	Insights that are covered in operator training and operating procedures.	
c) The dominant post-initiator operator action in the internal events full power PRA is Failure to Recognize Need for Low Pressure Makeup	Insights that are covered in operator training and operating procedures.	
d) The dominant recovery action is Failure to Recover Offsite Power	Insights that are covered in operator training and operating procedures.	
e) The dominant common cause failures in the internal event full power PRA are: • CCF of 7 Squib Valves in GDCS Lines • CCF of All Squib Valves	The GDCS squib valve pyrotechnic charges shall be replaced during refueling in accordance with the RAP.	X
f) An alarm located within the control room alerts the operator if the battery connection switch is inadvertently left open after test or maintenance.	Insights that are covered in operator training and operating procedures.	
g) The opening of five SRVs is sufficient for reactor depressurization to allow the low pressure system injection	Design requirement	
h) The most likely release category is associated with leakage from an intact containment.	General PRA Insight	
i) There are no operator actions required to support the containment response to a severe accident in the 24 hour period after onset of core damage.	General PRA Insight	
j) Important functions for containment integrity and severe accident response: AC-Independent Fire Water Addition System	The AC-independent Firewater System flow and flow monitoring instrumentation from the fire protection system (FPS) to the FAPCS main loop should be tested in the RAP. All fire protection and FAPCS piping which forms the AC Independent Firewater System should be tested in the RAP to ensure that it is structurally intact and properly supported.	X

Findings	Comments	RAP
k) Important functions for containment integrity and severe accident response: 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 at temperatures less than 533 K (500 °F) or under differential pressures associated with reactor blowdown and pool hydrodynamic loads.	Reliability of the Deluge Squib valves and actuation logic are in the RAP.	X
l) Important functions for containment integrity and severe accident response: Containment Inerting System Bleed Line. If the containment bleed valves are open and one of the vacuum breakers has not closed there would be a direct pathway from the drywell to the wetwell and to the environment.	Containment Air-operated valves (AOVs) in series of bleed line performing containment isolating function should be maintained in the RAP like other containment isolation valves. During preoperational testing and each refueling outage, each valve should be exercised. Local and control room indications should be tested. A flow test should be conducted as part of the refueling activities to assure that there are no obstructions in the pressure relief path. Special training in operator actions to understand how and in which conditions venting function will be performed should be included in the emergency procedures and in the plant training program.	X
m) Important functions for containment integrity and severe accident response: Vessel Depressurization. The nitrogen supply and battery capacity are sufficient to allow depressurization after potential IC failures.	Insights that are covered in operator training and operating procedures.	
n) Important functions for containment integrity and severe accident response: Inerted Containment	Design Requirement	
o) Important functions for containment integrity and severe accident response: Containment Isolation	Tested in accordance with Tech Spec Surveillance Requirements	X
p) Important functions for containment integrity and severe accident response: Upgraded Low Pressure Piping	Design Requirement	
q) Important functions for containment integrity and severe accident response: Drywell-Wetwell Vacuum Breakers	The failures of these vacuum breakers (VB) to close can be kept to an acceptably low probability if they are incorporated into the RAP.	X
r) Important functions for containment integrity and severe accident response: Basemat Internal Melt Arrest and Coolability Device (BiMAC)	Inspection of the high-temperature actuation function, and structural integrity of the BiMAC structure should be in the RAP.	X
s) Operator guidance for the use of the suppression chamber vent to prevent containment overpressurization has not been developed	Insights that are covered in operator training and operating procedures.	

Findings	Comments	RAP
t) The Safety Relief Valves (SRVs) and 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.	Failures of depressurization (DPVs) and safety relief valves (SRVs) can be kept to an acceptably low probability if they are included in the RAP and Tech Specs.	X
u) Check Valves in Feedwater lines prevent backflow during loss of Feedwater scenarios.	Design requirement	
v) Control Rod Drive Pumps provide high pressure makeup to the reactor vessel.	Testing to be in accordance with technical specifications associated with the control rod drives.	X
w) CRD MOVs provide flow control to allow CRD injection into the reactor vessel.	Testing to be in accordance with technical specifications associated with the control rod drives.	X
x) 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 monitor (APRM) ATWS permissive signal (i.e., APRM signal above a specified setpoint.) The same inhibit condition applies to GDCS function.	Testing to be in accordance with technical specifications.	X
y) The Voter Logic trains in each division are redundant but not independent modules.	The group of component types with the highest FV importance in the Level 1 analysis are common cause failure of scram related I&C components. Common-cause miscalibration of redundant system sensor and transmitters, and of RPV Level and pressure sensors, and common-cause failure (CCF) of digital trip modules (DTMs), will have acceptable probabilities if adequate administrative controls are exercised within the RAP.	X
z) The RMUs in each division are redundant but not independent modules.	See response to item aa above	X
aa) GDCS Injection mode squib valves automatically actuate on ECCS signals.	The GDCS squib valve pyrotechnic charges shall be replaced during refueling in accordance with the RAP.	X
ab) 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.	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.	X

Findings	Comments	RAP
ac) An 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.	Testing of the FAPCS line to RWCU/SDC should be included in the RAP.	X
ad) Long-term makeup to FAPCS provided through dedicated Fire Protection System lines.	The flow capacity of both the AC-driven and the direct diesel-driven fire pumps should be tested and the FAPCS non-safety-related which must operate to provide flow to the vessel, or to the IC/PCC makeup, should be manually opened and closed in accordance with the RAP.	X
ae) Condensate discharge valve and Hotwell makeup valves are necessary for condensate and feedwater operation.	These valves should be tested in accordance with the RAP.	X
af) 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.	These valves should be tested in accordance with the RAP.	X
ag) Service Water Pumps supply cooling water to RCCW and TCCW. Cooling Tower Fans provide heat removal for service water.	These pumps and fans should be tested in accordance with the RAP.	X
ah) Loss of incoming transmission lines results in loss of preferred power scenario. 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).	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.	X

Findings	Comments	RAP
ai) 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.	AC Uninterruptible power supplies will receive periodic checks in accordance with plant Technical Specifications; it was concluded that no additional reliability and maintenance actions are needed.	X
aj) The safety related DC distribution system is arranged in four divisional class 1E 250V DC power supplies	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.	X
ak) Diesel Generators	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.	X
al) The IC and PCC System perform a very significant passive function in the transient and accident conditions. Additionally, 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 significant components.	The RAP activities are aimed at ensuring by periodical testing and more extensively during refueling that the components' reliabilities are maintained as required. Checking of heat exchanger performance requirements should also be performed.	X
2) Fires		
a) The dominant fire initiating events in the full power internal fires PRA is: Fire in Turbine Building	Fire barriers, including penetrations, are tested in accordance with fire protection requirements. The Smoke Removal System should be operated periodically to demonstrate that it is able to maintain a negative pressure in a room with a fire so that probability of propagation of fire and/or smoke to other rooms is low.	X
b) The dominant operator action in the full power internal fires PRA is Failure to Recognize Need for LP Makeup	Operating procedures and training	
c) The dominant common cause failures in the full power internal fires PRA are: • CCF of 7 Squib Valves in GDCS Lines (35% contribution to full power fire CDF) • CCF of All Squib Valves (35% contribution to full power fire CDF)	See response to item 1e above	X

Findings	Comments	RAP
d) Recovery of the actuation of certain systems is credited due to the existence of remote shutdown panels located outside the control room If automatic actuations fail, the operators may manually perform the necessary 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.	X
3) Flood		
a) The dominant flood initiating event in the full power internal flooding PRA is a Circulating Water System pipe break in the turbine building,	Periodically, room water 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; CIRC isolation valves (MOVs) should be stroke tested (normally accomplished by switching from one pump to the standby pump in a given loop); the ability of CIRC 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.	X
4) High Winds		
a) The main conclusion that can be drawn from the ESBWR tornado risk analysis is that the risk from tornado strikes on the plant is acceptably low.	Site response procedures will address actions to take for high winds. No additional controls are warranted.	
5) Seismic		
a) The most significant HCLPF sequences (both 0.62g HCLPF) 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.	No maintenance activities other than those already associated with the in-service surveillance of the seismic instruments are needed for seismic events. The seismic instrumentation program is designed to provide information on the input ground motion and resultant responses of representative Category I structures and equipment in the event a strong enough earthquake occurs to activate the seismic instrumentation. If the earthquake exceeds the operating basis earthquake (OBE) threshold, the plant is shut down, and a detailed post-earthquake evaluation is undertaken. When it is determined that plant structures and equipment were not damaged, the plant can be safely restarted on the basis of seismic considerations.	X
6) Shutdown		
a) The dominant initiating events in the internal events shutdown PRA are: • Instrument Line Break Below TAF – Mode 6, Flooded (42% contribution to internal events shutdown CDF) • LOPP – Mode 6, Unflooded (31% contribution to internal events shutdown CDF) • RWCU/SDC Drain Line Break Below TAF – Mode 6, Flooded (12% contribution to internal events shutdown	Piping integrity is assured by the in-service inspection and testing programs. Given the high contribution of LOPP to shutdown PRA, inspection and testing of AC-independent fire protection system in vessel injection mode should be included in RAP. However, because of the importance of manual alignment, lining up the firewater should be specifically included in the training programs to assure that the system benefits are obtained. Specific procedures have to be	X

Findings	Comments	RAP
CDF) • Instrument Line Break Below TAF – Mode 6, Unflooded (10% contribution to internal events shutdown CDF)	developed by the COL applicant to align the Fire Protection System (FPS) for vessel injection or IC/PCC makeup.	
b) The dominant flood initiating event in the shutdown internal flooding PRA is: CRD Break in Rx Bldg. – Mode 6 (91% contribution to shutdown flood CDF)	Piping integrity is assured by the in-service inspection and testing programs.	X
c) The dominant operator action in the shutdown internal fires PRA is: Failure to Recognize Need for RPV Depressurization (63% contribution to shutdown fire CDF)	Insights that are covered in operator training and operating procedures.	
d) The dominant operator action in the shutdown internal flooding PRA is: Failure to Recognize Need for LP Makeup (57% contribution to shutdown flood CDF	Insights that are covered in operator training and operating procedures.	
e) 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.	
f) The greatest contribution to shutdown risk comes from breaks in lines connected to the vessel below TAF that occur in 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. Although the frequency of these events is very low, 6×10^{-7} per refueling outage, there is only one method for mitigation. This accident can only be terminated by closing the hatches.	The analysis of loss of reactor coolant inventory control function during mode 5 performed within the shutdown PRA clearly underscores the importance of keeping the lower drywell personnel and equipment hatches closed as long as possible. It is therefore recommended that the lower drywell hatches (equipment and personnel) 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. Also, Maintenance procedures requiring entry into the lower drywell should specify that in case of an RPV draining event, personnel must close these hatches before leaving the area.	X
g) The GDCS is of importance to shutdown risk, especially the squib valves. The shutdown PRA points out the high contribution of the mode 5 with reactor cavity not flooded to shutdown risk.	For this reason and considering the brief residence time in this mode of operation, carrying out maintenance on GDCS components during mode 5 when reactor cavity has not been flooded should be restricted in accordance with 10 CFR 50.65 (a)(4), i.e., Maintenance Rule, controls.	
h) 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.	X