GE Energy

James C. Kinsey
Project Manager, ESBWR Licensing

PO Box 780 M/C J-70
Wilmington, NC 28402-0780
USA

T 910 675 5057
F 910 362 5057
jim.kinsey@ge.com

MFN 07-066

Docket No. 52-010

January 30, 2007

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

Subject: **Response to Portion of NRC Request for Additional Information Letter No. 3 Related to ESBWR Design Certification Application ESBWR Probabilistic Risk Assessment RAI Number 19.1.0-2**

Enclosure 1 contains GE's response to the subject NRC RAI transmitted via the Reference 1 letter.

If you have any questions or require additional information regarding the information provided here, please contact me.

Sincerely,

Kathy Sedney for

James C. Kinsey
Project Manager, ESBWR Licensing

D068

NRO

Reference:

1. MFN 05-156, Letter from NRC to David Hinds, *Request for Additional Information Letter No. 3 Related to ESBWR Design Certification*, dated December 8, 2005

Enclosures:

1. MFN 07-066, Response to Portion of NRC Request for Additional Information Letter No. 3 Related to ESBWR Design Certification Application ESBWR Probabilistic Risk Assessment RAI Number 19.1.0-2

cc: AE Cubbage USNRC (with enclosures)
David Hinds GE/Wilmington (with enclosures)
eDRF 0000-0064-0587

Enclosure 1

MFN 07-066

Response to Portion of NRC Request for

Additional Information Letter No. 3

Related to ESBWR Design Certification Application

ESBWR Probabilistic Risk Assessment

RAI Number 19.1.0-2

NRC RAI 19.1.0-2

The U.S. Nuclear Regulatory Commission and the Advanced Light-Water Reactor Steering Committee reached consensus on a process for resolving the RTNSS issue (SECY-94-084). This process included the use of both probabilistic and deterministic criteria to achieve the following objectives: (1) determine whether regulatory oversight for certain non-safety-related systems was needed, (2) identify risk important structures, systems and components (SSCs) for regulatory oversight (if it were determined that regulatory oversight was needed), and (3) decide on an appropriate level of regulatory oversight for the various identified SSCs commensurate with their risk importance. No adequate documentation of this process is provided in the submitted ESBWR PRA. Provide the following information:

(a) Assessment of risk, in terms of both core damage frequency (CDF) and large release frequency (LRF), for external events at power and during shutdown assuming no credit for non-safety systems (focused PRA). This information is needed in the two probabilistic criteria (total CDF less than 1E-04/yr and total LRF less than 1E-06/yr).

(b) A risk analysis supporting the RTNSS process at shutdown. As one would expect, failure of the non-safety related reactor water cleanup/shutdown cooling system (RWCU/SDC) would cause an initiating event and loss of the decay heat removal function. This condition may require additional regulatory treatment for the RWCU/SDC system and its non-safety related support systems because this system is not in the technical specifications and its failure drives the shutdown PRA results. It should be noted that Westinghouse had additional regulatory controls for the analogous non-safety residual heat removal system and its support systems in the AP1000 design in accordance with RTNSS criteria.

(c) In applying the probabilistic criteria, the RTNSS process stresses the importance of accounting for uncertainties and also taking into consideration the risk importance of SSCs contributing to initiating event frequencies. No such information is provided in the submitted ESBWR PRA.

(d) Results (dominant accident sequences and cutsets with associated frequencies) of the "focused" PRA sensitivity study must be submitted. Cutsets contributing to 90 percent of CDF and/or LRF or top 200 cutsets, whichever is smaller, are needed to provide adequate information for the staff's review. Also, a discussion regarding the use of PRA results in the RTNSS decision-making process is needed (e.g., how it is decided whether regulatory oversight for certain non-safety systems is needed; how risk important SSCs for regulatory oversight are identified; and what is the basis for deciding on an appropriate level of regulatory oversight for these SSCs).

GE Response

REGULATORY TREATMENT OF NON-SAFETY SYSTEMS

Introduction

Background

The purpose of this response to RAI 19.1.0-2 is to demonstrate that the ESBWR design adequately addresses Regulatory Treatment of Non-Safety Systems (RTNSS) issues. A systematic process is used in the on-going ESBWR design process to identify regulatory guidance and compare it to specified ESBWR design features to determine if additional regulatory treatment is warranted for structures, systems, or components that perform a significant safety function. This RAI response documents the results that the process has produced to date.

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

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

- Determine whether regulatory oversight for certain nonsafety-related systems is needed,
- Identify risk important SSCs for regulatory oversight (if it is determined that regulatory oversight is needed)
- 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 being applied to the ESBWR design to determine the systems that are candidates for RTNSS consideration:

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

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

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

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

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

Following the identification of candidates for RTNSS consideration, the ESBWR design process evaluates each candidate to determine if RTNSS designation is made and what regulatory controls are appropriate.

Systematic Approach

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

Criteria A, B, D, and E are assessed using deterministic methods, including an assessment of containment performance. Criterion C is assessed probabilistically, by quantitative and qualitative methods based on information derived from the baseline PRA and also a focused PRA sensitivity study. The baseline PRA (NEDO-33201) is a comprehensive analysis that is performed in conjunction with the design phase of the ESBWR. It is an integrated assessment of the ESBWR design as it applies to transient and accident conditions. It identifies areas where further improvement can reduce risk in the design and operational phases and it quantifies the risk estimates to assess the capability of the ESBWR design to meet the NRC safety goals of CDF less than 1.0 E-4 per year and LRF less than 1.0 E-6 per year. The focused PRA sensitivity study evaluates whether the existing passive systems are solely adequate to meet the NRC safety goals, i.e., without the benefit of the available nonsafety-related active systems.

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

<u>Criterion A: Beyond Design Basis Events Assessment</u>

A1.) ATWS Assessment

ATWS events are described in Section 15.5.4 of the DCD Tier 2. Based upon the results of the analyses, the design for the ESBWR is satisfactory for mitigating the consequences of an ATWS. All performance requirements specified in Subsection 15.5.4.3.2 are met.

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

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

In addition, the ESBWR design uses an electrical insertion of Fine Motion Control Rod Drives (FMCRDs) for ATWS mitigation.

The ESBWR does not use pumps for forced coolant recirculation. Therefore, RPT logic does not exist in the ESBWR design. However, an ATWS automatic feedwater runback feature provides the analogous protection feature by rapidly reducing water level, core flow and reactor power.

SLCS is safety-related and therefore has adequate regulatory oversight. The ARI system and the feedwater runback logic are not safety-related and are therefore candidates for RTNSS.

A2.) Station Blackout Assessment

The ESBWR is designed to cope with a station blackout (SBO) event for 72-hours. The analysis in DCD Tier 2, Section 15.5.5 demonstrates that reactor water level is maintained above the top of active fuel and containment and suppression pool pressures and temperatures are maintained within their design limits. The integrity for containment is maintained and each acceptance criterion in Subsection 15.5.5.1 is met. Therefore the ESBWR is designed to successfully mitigate an SBO event to meet the requirements of 10 CFR 50.63, and there are no candidates for RTNSS.

Criterion B: Long-Term Safety Assessment

B.1) Actions Required Beyond 72 Hours

The safety functions that are required to maintain long-term safe-shutdown conditions are:

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

The ESBWR is designed so that passive systems are able to perform all safety functions for 72 hours after an initiating event without the need for active systems or operator actions. After 72 hours, nonsafety-related systems can be used to replenish the passive systems or to perform safety functions directly. Between 72 hours and 7 days, the resources for performing safety functions must be available on-site. After 7 days it is reasonable to assume that certain commodities can be replaced or replenished from offsite sources, e.g., diesel fuel. Each required safety function must be sustained to ensure that reactor and containment conditions are stable and improving. Systems used to perform safety functions after 72 hours need to be designed to appropriate seismic and high wind criteria, and must be flood protected. Each safety function is analyzed below to identify nonsafety-related systems that are required after 72 hours to maintain the safety function within its limits. Such systems are candidates for RTNSS.

Core Cooling

The safety function is to provide an adequate inventory of water to ensure that the fuel remains cooled and covered, with stable and improving conditions, beyond 72 hours. This function is met by the safety-related Gravity-Driven Cooling System (GDCS) injection function.

Decay Heat Removal

The safety function is to remove reactor decay heat from the core, containment, and spent fuel pool. The passive systems that provide this function for the core and containment are the safety-related Isolation Condenser System (ICS) and the safety-related Passive Containment Cooling System (PCCS). Theses systems are capable of removing decay heat for at least 72 hours without the need for active systems or operator actions. After 72 hours, makeup water is needed to replenish the boil-off from the upper containment pools. The ESBWR design includes permanently installed piping in the Fuel and Auxiliary Pools Cooling System (FAPCS), which connects directly to a dedicated diesel-driven makeup pump system. This connection enables the upper containment pools and spent fuel pools to be filled with water from the Fire Protection System (FPS), which provides on-site makeup water to extend the cooling period from 72 hours through 7 days. The dedicated makeup pump system is classified as nonsafety-related but is designed to remain operable following a seismic event. This includes a diesel-driven pump, the water supply, the suction pipe from the water supply to the pump, a supply pipe from the makeup pump to the Reactor Building, and the connections to the FAPCS.

The spent fuel pool is normally cooled by FAPCS. However, on a complete loss of FAPCS cooling under the condition of maximum heat load, a sufficient quantity of water is available in the spent fuel pool to allow boiling for 72 hours and still cover the top of active fuel. The line from the diesel makeup pump to the spent fuel pool is seismically qualified.

A dedicated external connection to the FAPCS line allows for manual hook-up of external water sources, if needed, after 7 days for either upper containment pool replenishment and for spent fuel pool makeup.

As a result of the RTNSS Criterion B evaluation, the following components are RTNSS candidates: the diesel-driven makeup pump system, FAPCS piping connecting to the diesel-driven makeup pump system, and the external connection.

Post-Accident Monitoring

Operator actions are not required for successful operation of safety-related systems for the first 72 hours following an event. Beyond that, operator actions are necessary to support continued operation of safety systems. Therefore the operators require information on the condition of the plant SSCs, which is acquired through monitoring instrumentation.

The details of post-accident monitoring and supporting functions are still being developed. It is expected that certain portions of the Distributed Control and Instrumentation System (DCIS) will be included within the scope of RTNSS. In order to support post-accident monitoring beyond 72

hours, it will be necessary to provide power for and component cooling to the DCIS components. Power for DCIS is provided by recharging the batteries. Component cooling is performed by portions of the HVAC systems in the Reactor Building, Electrical Building, Fuel Building, Control Building, and Turbine Building. In addition, support for HVAC is required from AC power (a RTNSS candidate, as discussed below) and cooling from Reactor Component Cooling Water, Turbine Component Cooling Water, Plant Service Water, and the Chilled Water System.

CONTROL ROOM HABITABILITY

The details of control room habitability and supporting functions are still being developed. Preliminary assessment of the design concludes that control room habitability and supporting functions are either passive or require minor operator actions or battery-powered actuations, and thus do not need to be included within the scope of RTNSS.

B.2) Seismic Assessment

The seismic margins analysis in Section 15 of NEDO-33201 assesses the seismic ruggedness of plant systems, both safety-related and nonsafety-related. No accident sequence has a High Confidence for Low Probability of Failure (HCLPF) value 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.

Criterion C: PRA Mitigating Systems Assessment

Introduction

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

Focused PRA Sensitivity Study

A focused PRA sensitivity study evaluates whether passive systems alone are adequate to meet the NRC safety goals of CDF less than 1.0 E-4 per year and LRF less than 1.0 E-6 per year. The focused PRA retains the same initiating event frequencies as the baseline PRA, and sets the failure probabilities of nonsafety-related systems to "True", i.e., failed, while safety-related system failure probabilities remain unchanged. The focused PRA model is evaluated using only the safety-related systems shown in Table 1 adding nonsafety-related systems only if they are required to meet the CDF or LRF goals. The additional nonsafety-related systems required to meet the CDF and LRF goals are candidates for RTNSS.

The quantification of the affect of nonsafety-related systems on at-power risk is not complete due to recent design changes that have a significant effect on the PRA results. Based on preliminary

quantification results of CDF and LRF from the previous revision of the PRA, it is expected that the CDF and LRF goals will be met only with the addition of certain portions of the Diverse Protection System (DPS). This is needed to counter the effects of the dominant risk contribution, which is due to common cause failures of actuation instrumentation. The dominant accident sequences and cutsets with associated frequencies will be submitted in an update to the RTNSS response.

Insights from the preliminary shutdown model 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. Therefore, no nonsafety-related systems for shutdown conditions are expected to be candidates for regulatory oversight.

Assessment of Non-Safety Systems on External Events

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

Fire

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

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

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

(2) Fires in the control room are assumed to affect the execution of human actions. A fire in the control room does not affect the automatic actuations of the safety systems. Additionally, the existence of remote shutdown panels allows the detection of failed automatic actuations and the performance of compensation manual actuations.

The separation and redundancy of safety systems coupled with the fire protection and suppression features built into the design result in CDF and LRF risks due to internal fires that are not significant. The effects of nonsafety-related systems are not specifically addressed in the fire scoping analysis because conservative bounding methods were used. Nonsafety-related systems do not play a significant role in mitigation because fire separation results in one division

of safety-related SSCs being damaged while the functions from the remaining three safety-related divisions are intact and capable of achieving safe shutdown conditions.

Flood

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

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

Wind

The conclusion from the ESBWR tornado risk analysis is that the risk from tornado strikes on the plant is acceptably low. The effect of high winds on the Focused PRA is bounded by a loss of offsite power with the plant safety systems available, and is thus negligible with respect to CDF and LRF.

Seismic

The ESBWR plant and equipment are capable of withstanding an earthquake with a magnitude at least 1.67 times the safe shutdown earthquake (SSE). No accident sequence has a HCLPF lower than 0.60 g. In addition, only passive safety-related systems are credited in the seismic event tree. In addition, FPS is classified as nonsafety-related but is designed so that the diesel driven pump in the Fire Protection Enclosure (FPE), the FPS water supply, the FPS suction pipe from the water supply to the pump, one of the FPS supply pipes from the FPE to the Reactor Building, and the FPS connections to the FAPCS remain operable following a seismic event. Therefore, there are no seismic-related candidates for RTNSS consideration.

Assessment of Uncertainties

The ESBWR PRA addresses passive system thermal-hydraulic (T-H) uncertainty issues in a systematic process that identifies potential uncertainties in passive components and then applies an appropriate treatment to the component to ensure that the uncertainties are treated conservatively. Passive system T-H uncertainties manifest themselves in the PRA model within failure probabilities and success criteria. Passive components that must rely on natural forces, such as gravity, have lower driving forces than conventional pumped systems. Some passive functions are based on new engineering design, without significant operating experience to apply confidence in the failure rate estimates. The PRA models the effectiveness of passive safety

functions in the success criteria that are factored into the event trees. Therefore, assessing the event tree success criteria in the PRA model identifies T-H uncertainties.

An assessment of the PRA success criteria will be performed during the Revision 2 of the PRA. The assessment will be performed by evaluating the ESBWR PRA success criteria to identify potential passive uncertainties. Each potential uncertainty is then assigned an appropriate conservative treatment. Uncertainties are associated with physical parameters; such as low driving head, squib valve performance, check valve performance at low differential pressure, low flow rates, or heat removal capability.

Upon identification of these potential uncertainties, the appropriate treatment will be assessed. To ensure that passive uncertainties are conservatively treated in the PRA model, at least one of the following alternatives will be applied to address each potential uncertainty:

- Use conservative success criterion, (i.e., n+1).
- Perform a sensitivity study to determine if the passive feature is sensitive to variations in failure rate.
  - If feature is sensitive, apply a conservative unreliability rate.
- Manage uncertainty through the reliability assurance program and regulatory oversight.
  - Designate appropriate components as RTNSS if nonsafety-related.

The BiMAC device provides an engineered method to assure heat transfer between the debris bed and cooling water. Flooding the lower drywell after the introduction of core material minimizes the potential for energetic fuel-coolant interaction. Covering core debris with water provides scrubbing of fission products released from the debris and cools the corium, thus limiting potential core-concrete interaction. The BiMAC device provides additional assurance of debris bed cooling by providing engineered pathways for water flow through the debris bed. BiMAC failure could occur if no water was supplied. The BiMAC device is not safety-related. It is a first of a kind design that is added to the ESBWR to reduce the uncertainties involved with severe accident phenomenology. As such, it is a candidate for RTNSS.

In addition, an assessment of the preliminary PRA results indicates that, in several PRA transient (non-seismic) sequences, FAPCS is relied upon for defense-in-depth as a backup means for core cooling and containment heat removal. Therefore, it is considered to be a RTNSS system

PRA Initiating Events Assessment

The at-power and shutdown PRA models are reviewed to determine whether nonsafety-related 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 nonsafety-related SSCs significantly contribute to the occurrence of an initiating event?

(2) Does the unavailability of these nonsafety-related SSCs have a significant impact on the initiating event frequency?

(3) Does the initiating event significantly affect CDF or LRF for the baseline PRA?

If the answer to all three of these questions is "Yes", then the nonsafety-related SSC is a candidate for RTNSS. The results are discussed below.

At-Power Generic Transients

Initiating events that are considered Generic Transients are described in Chapter 2 of NEDO-33201. Because several initiating events in this group are caused by the failures of nonsafety-related SSCs, screening questions 1, 2, and 3 in Table 2 are answered "Yes." However, the Generic Transient contributes less than 1% to CDF and LRF (NEDO-33201 Section 7.2). Therefore, there are no specific nonsafety-related systems that have a significant effect on risk, and there are no RTNSS candidates from this category.

At-Power Transient with Loss of Feedwater

The initiating events in this group begin with a prompt and total loss of feedwater and require the success of other mitigating systems for reactor vessel level control. The SSCs related to feedwater and condensate are nonsafety-related, and thus Questions 1, 2, and 3 are answered "Yes." The loss of feedwater has a significant effect on CDF and LRF (NEDO-33201 Section 7.2). Therefore, the feedwater and condensate systems are potential RTNSS candidates.

At-Power Loss of Preferred Power

Loss of Preferred Power (LOPP) occurs as a result of severe weather, grid failures, or switchyard faults. Loss of preferred power causes a plant trip and a loss of feedwater, with longer-term effects on other mitigating systems requiring AC power. The associated systems that comprise the onsite AC power distribution system are nonsafety-related, and thus, Questions 1, 2, and 3 are answered "Yes." LOPP is a significant contributor to CDF and LRF (NEDO-33201 Section 7.2). Therefore, the AC power system is a potential RTNSS candidate.

At-Power LOCA

Loss of coolant accidents are initiated by piping leaks, valve leaks, or breaks. LOCAs are postulated to initiate in nonsafety-related systems, such as RWCU/SDC and Main Steam. However, general design considerations require that all piping and components within the reactor coolant pressure boundary be safety-related. The RWCU/SDC and Main Steam piping have redundant safety-related isolation valves that automatically close on a LOCA signal.

Safety/Relief Valves are safety-related.

Therefore, there are no RTNSS candidates from this category.

Shutdown Loss of Preferred Power

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

Loss of Shutdown Cooling

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

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

With the reactor well unflooded, it is assumed that both RWCU/SDCS trains are in service and that one train is sufficient to remove decay heat while keeping the reactor coolant from boiling. Therefore, if one RWCU pump were to trip in this configuration, it would not initiate a loss of shutdown cooling event, and Questions 1, 2, and 3 are answered "No."

There are no RTNSS candidates for regulatory oversight.

Shutdown LOCA

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

Breaks outside containment can be originated only in RWCU/SDCS or FAPCS piping, because these are the only systems that remove reactor coolant from the containment during shutdown. The rest of the RPV vessel piping is isolated. The RWCU/SDCS and FAPCS containment penetrations have redundant and automatic power-operated safety-related containment isolation valves that close on signals from the leak detection and isolation system and the reactor protection system.

There are no RTNSS candidates from this category.

Summary of RTNSS Candidates from Criterion C

The focused PRA sensitivity study is expected to result in certain portions of DPS being a RTNSS candidate.

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

Based on the assessment of the importance of nonsafety-related SSCs with respect to initiating events, the following SSCs are RTNSS candidates:

- Feedwater System
- Condensate System
- AC Power – Offsite Power Distribution System

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." Containment bypass issue during severe accidents (SECY-93-087, Issue II.G),is concerned with potential sources of steam bypassing the suppression pool and failure of heat exchanger tubes in passive containment cooling systems. These concerns are addressed in the Design Control Document. Tier 2 Section 6.2.1.1.5 addresses steam bypass of the suppression pool. Tier 2 Section 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. Therefore, there are no RTNSS candidates for regulatory oversight.

Criterion E: Assessment of Significant Adverse Interactions

Background

The concerns about adverse system interactions were addressed for currently operating reactors as NRC Unresolved Safety Issue, Item A-17: SYSTEMS INTERACTIONS IN NUCLEAR POWER PLANTS. Item A-17 acknowledged that systems interactions are usually well recognized and, therefore, are accounted for in the evaluation of plant safety by designers and in plant safety assessments. The concern was the potential for unrecognized subtle dependencies among SSCs to be unidentified and possibly lead to safety-significant events. The term used to describe these unrecognized, subtle dependencies is adverse systems interactions (ASIs). The NRC recommended that licensees not conduct broad searches specifically to identify all ASIs because such searches had not proved to be cost-effective in the past, and there was no guarantee after such studies that all ASIs had been uncovered.

Systematic Approach

The purpose of the Criterion E analysis is to systematically evaluate adverse interactions between the active and passive systems. For the purpose of this analysis, an adverse systems interaction exists if the action or condition of an active, interfacing system causes a loss of safety function of a passive safety system. A systematic process will be used to analyze specific features and actions that are designed to prevent postulated adverse interactions, while taking into consideration the extensive operating experience that has been used in the current design criteria to prevent adverse systems interactions.

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

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

Gravity Driven Cooling System (GDCS)

Design Features

GDCS provides flow to the annulus region of the reactor through dedicated nozzles. It provides gravity-driven flow from three separate water pools located within the drywell at an elevation above the active core region. It also provides water flow from the suppression pool to meet long-term post-LOCA core cooling requirements. The system provides these flows by gravity forces alone once the reactor pressure is reduced to containment pressure.

All piping connected with the RPV is classified as Safety-Related, Seismic Category I. The electrical design of the GDCS is classified as Class 1E. GDCS is protected against the effects of pipe whip, which might result from piping failures up to and including the design basis event LOCA. This protection is provided by separation, pipe whip restraints, energy-absorbing materials or by providing structural barriers.

System Interfaces

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

Analysis of Potential Adverse System Interactions

Squib valve and deluge valve initiation circuitry are powered by divisionally separated, safety-related, 250 VDC. To minimize the probability of common mode failure, the deluge valve pyrotechnic booster material is different from the booster material in the other GDCS squib valves. The pyrotechnic charge for the deluge valve is qualified for the severe accident environment in which it must operate.

The following GDCS indications are reported in the control room:

- Status of the locked-open maintenance valves;
- Status of the squib-actuated valves;
- GDCS pools and suppression pool level indication;

- Position of each GDCS check valve;
- Suppression pool high and low level alarm;
- GDCS pools high and low level alarms; and
- Squib valve continuity alarms.

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

Inadvertent actuation of the Lower Drywell Deluge squib valves that supply the BiMAC system would adversely affect the GDCS injection function by emptying the GDCS pools into the lower drywell. The probability of an inadvertent actuation is extremely low because the Deluge squib valves and actuation logic are safety-related, and are thus designed with adequate redundancy, as described in the DCD.

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

Automatic Depressurization System (ADS)

Design Features

The depressurization function is accomplished through the use of safety/relief valves (SRVs) and depressurization valves (DPVs). Supporting systems for ADS include the instrumentation, logic, control and motive power sources. The instrumentation and logic power is obtained from corresponding safety-related divisional uninterruptible and ICP 120 VAC power sources. Either source can support ADS operation. The actual SRV solenoid and DPV squib initiator power is supplied by the corresponding safety-related divisional 250 VDC batteries. The motive power for the electrically operated pneumatic pilot solenoid valves on the SRVs is provided by the High Pressure Nitrogen Supply System.

System Interfaces

Main Steam, Containment, Suppression Pool, DC Power, HPNSS

Analysis of Potential Adverse System Interactions

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

The High Pressure Nitrogen Supply System (HPNSS) provides driving force for the pneumatic pilot solenoid ADS valves. The High Pressure Nitrogen Supply System distributes clean, dry, oil-free nitrogen gas to the Containment Inerting System (CIS). Upstream pressure control valves modulate the CIS nitrogen supply to provide the required nitrogen supply pressure to the nitrogen loads. If CIS fails to maintain the required nitrogen supply pressure, HPNSS provides uninterrupted nitrogen gas supply from the nitrogen storage bottles. When the nitrogen gas pressure in the main header drops below the set pressure, the manifold isolation valve automatically opens to provide nitrogen gas from the storage bottles to all nitrogen loads. One bottle rack train and one pressure-reducing station are utilized to maintain design nitrogen supply as required. The nitrogen bottle station valves and manifold isolation valve on one train are kept open, while the standby train bottle station valves and manifold isolation valves are kept closed. The HPNSS bottled nitrogen normally remains on standby, through an isolation valve located upstream of the pressure reducing station. During low nitrogen supply pressure in the main supply header, the isolation valve automatically opens to allow nitrogen gas supply from the HPNSS nitrogen bottles to all system loads.

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

Isolation Condenser System (ICS)

Design Features

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

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

carryover. IC/PCC pool makeup clean water supply for replenishing level during normal plant operation is provided from FAPCS. A safety-related independent FAPCS makeup line is provided to provide emergency makeup water into the IC/PCC pool from piping connections located in the reactor yard.

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

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

System Interfaces

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

Analysis of Potential Adverse System Interactions

The ICS and Passive Containment Cooling System (PCCS) pools have two local panel-mounted, safety-related level transmitters. Both transmitter signals are indicated on the safety-related displays and sent through the gateways for nonsafety-related display and alarms. Both signals are validated and used to control the valve in the makeup water supply line to the IC/PCCS pool. The FAPCS IC/PCCS pools cooling and cleanup subsystem pump is automatically tripped on low water level in IC/PCCS pools. Water level in the skimmer surge tanks is maintained by automatic open/closure of the makeup water supply isolation valve. Water level in the IC/PCCS pools is maintained by automatic open/closure of the makeup water supply isolation valve.

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

Four sets of differential pressure instrumentation are located on the IC steam line and another four sets on the condensate return line inside the drywell. Detection of excessive flow beyond operational flow rates in the steam supply line or in the condensate return line (2/4 signals)

results in alarms to the operator, plus automatic isolation of both steam supply and condensate return lines.

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

Standby Liquid Control System (SLCS)

Design Features

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

System Interfaces

Control Building, Containment, DC Power

Analysis of Potential Adverse System Interactions

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

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

Passive Containment Cooling System (PCCS)

Design Features

PCCS removes the core decay heat rejected to the containment after a LOCA. It provides containment cooling for a minimum of 72 hours post-LOCA, with containment pressure never exceeding its design pressure limit, and with the Isolation Condenser/Passive Containment Cooling (IC/PCC) pool inventory not being replenished.

System Interfaces

Containment, FAPCS, ICS, Suppression Pool

Analysis of Potential Adverse System Interactions

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

Monitoring Instrumentation

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

Regulatory Oversight of Important Non-Safety Systems

Selection of Important Non-Safety Systems

The selection of RTNSS systems considers nonsafety-related SSCs that are necessary to meet NRC regulations, safety goal guidelines, and containment performance goal objectives. RTNSS systems needed to meet the NRC regulations specified in Criteria A and E are based on deterministic analyses. RTNSS systems needed to meet Criteria C and D are based on PRA analysis, with Criterion B being a combined basis of PRA and deterministic insights to ensure the ability to maintain core cooling and containment integrity beyond 72 hours.

For Criterion C, systems identified as RTNSS are evaluated in the focused PRA sensitivity study to ensure that this combination of safety-related and nonsafety-related systems meets the safety goal guidelines. If the goals are met, PRA importance studies are then performed to determine the risk-significance of these systems.

Results of the regulatory treatment assessment are summarized in Table 3.

Regulatory Oversight Regulatory oversight is applied to each system designated as RTNSS to ensure that it has sufficient reliability and availability to perform its RTNSS function, as defined by the focused PRA, or deterministic criteria. The extent of oversight is commensurate with the safety significance of the RTNSS function, and is categorized as either High Regulatory Oversight, or Low Regulatory Oversight. In addition, design standards are applied commensurate with the safety significance of the RTNSS function. Distinctions are made to account for the ability of the RTNSS system to withstand external events, such as seismic, high winds, and flooding. Fire events are sufficiently addressed with the current regulatory standards. In addition, after the design of I&C systems has been added to the PRA model, graded safety classifications and requirements for important I&C systems will be incorporated into the RTNSS results.

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

Each RTNSS system requiring High Regulatory Oversight shall be described in the DCD Tier 1 and Tier 2 to a similar level of detail as safety-related systems.

If a RTNSS system is not significant, as described above, then the proposed level of regulatory oversight should be in Regulatory Availability Specifications.

Each RTNSS system requiring Low Regulatory Oversight shall be described in the DCD Tier 2 with respect to the RTNSS function that it provides.

Reliability Assurance

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

Augmented Design Standards

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

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

In addition to seismic standards, Criterion B systems must meet design standards to withstand winds and missiles generated from a category 5 hurricane.

The plant design for protection of SSCs from the effects of flooding considers the relevant requirements of General Design Criterion 2, "Design Bases for Protection Against Natural Phenomena," and 10 CFR Part 100, Appendix A, "Seismic and Geologic Siting Criteria for Nuclear Power Plants," Section IV.C as related to protecting safety-related SSC from the effects of floods, tsunamis and seiches. The design meets the guidelines of Regulatory Guide 1.59 with regard to the methods utilized for establishing the probable maximum flood (PMF), probable maximum precipitation (PMP), seiche and other pertinent hydrologic considerations; and the guidelines of Regulatory Guide 1.102 regarding the means utilized for protection of safety-related SSC from the effects of the PMF and PMP.

Systems that meet RTNSS Criterion C for importance due to their contribution on CDF and LRF do not require augmented design standards described above, but must incorporate the defense-in-depth principles of redundancy and physical separation to ensure adequate reliability and availability.

Regulatory Treatment

The proposed regulatory treatment of RTNSS systems is presented below, and is summarized in Table 3.

Alternate Rod Insertion

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

Feedwater Runback Logic

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

Feedwater and Condensate Systems

These systems have a significant effect on CDF and LRF relative to the loss of Feedwater initiating event. However, several features in the advanced design of the new generation feedwater level control system add significant reliability and, thus, a lower failure probability for loss of feedwater initiating events. The feedwater level control system is single failure proof. Therefore, a control failure is much less likely to occur in the ESBWR than in the current generation of reactors. In addition, there are added protections not available in the current reactors. These include a FW runback; an automatic scram; and closure signals to the high pressure makeup (CRD) flow control valves on a high reactor water level signal, and trip of the FW pumps on high reactor water level.

The dominant contributor to a total loss of feedwater is a loss of control power to the feedwater controllers. Only a total and immediate loss of all feedwater flow is included in the Loss of Feedwater initiating event category. A controller failure that results in reduced feedwater flow is considered a generic transient, which is much less significant than a complete loss of feedwater. These features are not explicitly modeled in the level 1 PRA, but instead are represented by the conservatively assigned initiating event frequency, which is based on the operating experience of current reactors (typically with conventional feedwater control systems.)

Therefore, due to the conservative treatment of the condensate and feedwater systems in the level 1 PRA, their risk significance does not warrant additional regulatory oversight.

Diesel-Driven Makeup Pump and Dedicated Connection for FPS Makeup

The diesel-driven makeup pump is considered for RTNSS in accordance with Criterion B, long-term actions required beyond 72 hours to ensure safe shutdown conditions. The pump and the FPS are classified as nonsafety-related but are designed so that portions of the system remain operable following a seismic event to keep equipment required for safe shutdown free from fire damage during a safe shutdown earthquake. In conjunction with the diesel-driven pump, the dedicated connection for FPS makeup includes the Fire 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. FPS makeup to the ICS/PCC pools is a candidate for regulatory oversight 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 proposed level of regulatory oversight for this function should be in Regulatory Availability Specifications.

Diverse Protection System

Certain functions of DPS are expected to be significant with respect to the focused PRA sensitivity study to meet the NRC safety goal guidelines. DPS will provide diverse actuation functions that will enhance the plant's ability to mitigate dominant accident sequences involving the common cause failure of actuation logic or controls. The risk significance is expected to be high for the special case of the focused PRA, such that the proposed level of regulatory oversight for portions of DPS should be in Technical Specifications.

Basemat-Internal Melt Arrest and Coolability System

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 1.0 E-3. BiMAC plays an important role in mitigating core melt scenarios. Therefore, it is a candidate for RTNSS consideration. The BiMAC device functions during severe accidents, and thus has no effect on the level 1 PRA. The inclusion of the BiMAC device in the ESBWR design provides an engineered method to assure heat transfer between the debris bed and cooling water. By flooding the lower drywell after the introduction of core material, the potential for energetic fuel-coolant interaction is minimized. Covering core debris with water provides scrubbing of fission products released from the debris and cools the corium, limiting potential core-concrete interaction (CCI). The BiMAC device provides additional assurance of debris bed cooling by providing engineered pathways for water flow through the debris bed. BiMAC failure could occur if no water was 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 release category Core-Concrete Interaction-Wet, (CCIW) applies to sequences in which GDCS deluge function is successful, but lower drywell corium debris bed is not effectively cooled. In these sequences, the BiMAC cooling function has failed, but the debris bed is flooded. The extent of water penetration and thus, the potential for debris bed cooling, is subject to assumption. In the bounding case, the debris bed is impenetrable by the overlying water pool and the CCI would approach that of a dry debris bed. To address this uncertainty, the frequency of the CCIW categories has been combined with the CCID category and a representative CCID source term conservatively used.

The release category Core-Concrete Interaction-Dry, (CCID) applies to sequences in which GDCS deluge function is unsuccessful, so the lower drywell corium debris bed is not effectively cooled. In these sequences, the core-concrete interaction is not limited by any cooling, nor is the radionuclide release limited by the potential scrubbing action of an overlying water pool.

The release frequency for CCIW and CCID combined is 3 E-10 per year, which is not risk significant. The proposed level of regulatory oversight for the BiMAC function should be in Regulatory Availability Specifications.

Distributed Control and Instrumentation System

The details of post-accident monitoring and supporting functions are still being developed. The DCIS provides post-accident monitoring capability, and is therefore expected to be a RTNSS system with low risk significance. The proposed level of regulatory oversight for the RTNSS portion of DCIS should be in Regulatory Availability Specifications.

Fuel and Auxiliary Pool Cooling System

Based on a review of the original PRA results, FAPCS can supply core cooling and containment heat removal in certain non-seismic PRA sequences in a backup capacity (i.e., two 100% capacity trains.) Due to its expected importance in providing redundancy to core cooling and containment heat removal, FAPCS and its supporting functions (e.g., AC power and component cooling) are therefore RTNSS systems. Their risk significance is expected to be relatively low; therefore, the proposed level of regulatory oversight for these functions should be in Regulatory Availability Specifications.

AC Power System

Loss of preferred power is a significant contributor to CDF and LRF for at-power and shutdown risk. The dominating risk contributions to the loss of offsite power during operating and shutdown conditions are from the loss of incoming AC power from the utility grid and transformer faults. Both the grid and the transformers would typically be owned and operated by the COL, but they would be typically maintained by an external transmission organization that is not controlled by the site organization. Consequently, the appropriate controls for maintaining grid and transformer reliability would be handled by the transmission organization. The other SSCs that prevent a loss of offsite power, such as substations, breakers, and motor control centers are much less risk-significant, due to the passive safety features of the ESBWR.

Therefore, the SSCs within the site organization's control for preventing a loss of offsite power initiating event are not risk significant, and there are no candidates for RTNSS that warrant additional regulatory oversight.

The Diesel Generators are required to provide power for recharging batteries to support post-accident monitoring (i.e., Criterion B), and for FAPCS in non-seismic PRA sequences (i.e., Criterion C.) The expected risk significance of the Diesel Generators in both applications is judged to be low, such that the proposed level of regulatory oversight for this function should be in Regulatory Availability Specifications.

Component Cooling – HVAC, Cooling Water, Chilled Water, and Plant Service Water

In order to support post-accident monitoring beyond 72 hours and FAPCS operation, it is necessary to provide component cooling to the DCIS and FAPCS components. Component cooling will be performed by the HVAC systems in the Reactor Building, Electrical Building, Fuel Building, Control Building, and Turbine Building. In addition, support for HVAC is required from AC power and cooling from Reactor Component Cooling Water, Turbine Component Cooling Water, Plant Service Water, and the Cooling Towers. The expected risk significance for these supporting functions is judged to be low. The proposed level of regulatory oversight for these functions will be evaluated to determine if adequate oversight is provided by the supported function, or if additional Regulatory Availability Specifications should be applied.

Table 1

Safety and Non-Safety Systems in Sensitivity Study

Non-Safety Systems Set to Fail in Sensitivity Study
Feedwater Condensate Circulating Water Control Rod Drive Fire Protection Injection Containment Venting RWCU/SDC FAPCS AC Power Diverse Protection Logic
Safety Systems Credited in Sensitivity Study
Automatic Depressurization Isolation Condenser Gravity Driven Cooling Standby Liquid Control Main Steam Isolation Valves I&C Logic and Control High Pressure Nitrogen Supply Uninterruptible AC Power DC Power PCCS

Table 2

Initiating Events Assessment for RTNSS

Initiating Events	Could Nonsafety-Related systems contribute to the occurrence of an initiating event?	Does unavailability of these systems significantly affect the initiating event frequency?	Does the initiating event significantly affect Baseline CDF or LRF?
Generic Transients	Yes	Yes	Yes
Transient with Loss of Feedwater	Yes	Yes	Yes
Loss of Preferred Power	Yes	Yes	Yes
LOCA	No	No	No
Shutdown Loss of Preferred Power	Yes	Yes	Yes
Loss of Shutdown Cooling	No	No	No
Shutdown LOCA	No	No	No

Table 3
RTNSS Systems

System	Function	RTNSS Criterion	Regulatory Treatment
ARI	Automatically depressurize SCRAM header on ATWS signal.	A	LRO
Feedwater Runback	Run FW demand to minimum on ATWS signal.	A	LRO
Diesel Fire Pump	Provide post 72-hour refill to PC/ICC and Spent Fuel pools.	B	LRO
External Connection	Provide post 7-day refill to PC/ICC and Spent Fuel pools.	B	LRO
DPS	Diverse actuation of ECCS functions.	C	HRO
BiMAC	Provide core debris cooling in LDW.	C	LRO
PAM Instruments (DCIS)	Provide post accident monitoring (use RG 1.97 to determine scope.)	B	LRO
FAPCS	Suppression pool cooling and low pressure coolant injection modes. (Non-seismic PRA sequences.)	C	LRO
Diesel Generators	Provide power for post accident monitoring to 1E electrical distribution. Provide power for FAPCS and support systems. (Non-seismic PRA sequences.)	B C	LRO LRO
RB HVAC	Provide post 72-hour cooling for DCIS.	B	LRO
FB HVAC	Provide cooling support for FAPCS.	C	LRO
EB HVAC	Provide post 72-hour cooling for DGs and 1E Electrical Distribution. Provide support for electrical power to FAPCS.	B C	LRO LRO
CB HVAC	Provide post 72-hour cooling for DCIS and Control Room habitability.	B	LRO

Table 3
RTNSS Systems

System	Function	RTNSS Criterion	Regulatory Treatment
TB HVAC	Provide post 72-hour cooling for DCIS in Turbine Building.	B	LRO
	Provide room cooling for RCCW pumps.	C	LRO
TCCWS	Provide post 72-hour cooling for TB HVAC.	B	LRO
	Provide support for room cooling for RCCW pumps.	C	LRO
Chilled Water System	Provide post 72-hour cooling for HVAC.	B	LRO
	Provide cooling support for FAPCS.	C	LRO
RCCWS	Provide post 72-hour cooling for Chillers and DGs.	B	LRO
	Provide cooling support for FAPCS.	C	LRO
PSW	Provide post 72-hour cooling for RCCWS.	B	LRO
	Provide cooling support for FAPCS.	C	LRO

Note: LRO = Low Regulatory Oversight, HRO = High Regulatory Oversight

DCD Impact

The analysis presented in this RAI response is complete and accurate for the current state of the design. As detailed design information becomes available, this analysis will be reviewed to ensure that the final RTNSS analysis reflects the final certified design. There are no changes to DCD Tier 2 Chapter 19 Revision 2. DCD Tier 2 Chapter 19 Revision 3 will incorporate the final conclusions for RTNSS compliance.