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 06-248

Docket No. 52-010

July 27, 2006

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

Subject: **NEDO-33201, Revision 1, "ESBWR Probabilistic Risk Assessment," Section 20**

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

In RAI 19.1.0-2, the NRC asked GE to provide additional documentation and analyses in support of the process used to identify requirements for RTNSS. Four specific topics were to be addressed:

(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).

(b) A risk analysis supporting the RTNSS process at shutdown. In particular, the RWCU function was asked to be addressed.

(c) Uncertainties and initiating event frequencies.

(d) A list of the dominant cutsets from the Focused PRAs.

NEDO-33201, Revision 1 Section 20 provides a greatly expanded description of the RTNSS selection process. It addresses some, but not all, of these topics. LRF has been added to the focused PRA, but for full power, internal events only. RTNSS for shutdown and external events is addressed in a qualitative rather than quantitative manner. A

D068

section has been included to address uncertainties and another for initiating event frequencies (for all modes and initiators).

The dominant cutsets from the focused PRA (internal events, full power) are not contained in the report. GE will provide these cutsets separately by August 10, 2006.

GE is currently performing the additional analyses to fully answer this RAI, however we did not want to delay the issuance of this Section while these analyses are being finalized. The full response to RAI 19.1.0-2 will be transmitted to the NRC by September 20, 2006.

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

Sincerely,

Kathy Sedney for

David H. Hinds
Manager, ESBWR

Enclosure:

1. MFN 06-248 – NEDO-33201, Revision 1, "ESBWR Probabilistic Risk Assessment:"
    - Section 20 – Regulatory Treatment of Non-Safety Systems (RTNSS)

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	0000-0044-8542	

ENCLOSURE 1

MFN 06-248

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

- **Section 20 – Regulatory Treatment of Non-Safety Systems**

20 REGULATORY TREATMENT OF NON-SAFETY SYSTEMS (RTNSS)

Contents

List of Tables

20 REGULATORY TREATMENT OF NON-SAFETY SYSTEMS (RTNSS)

20.1 INTRODUCTION

20.1.1 Background

The ESBWR plant design uses passive safety systems to supply safety injection water and provide core and containment cooling. As the ESBWR relies on passive safety systems to perform the design-basis, safety-related functions of reactor inventory control and decay heat removal, different portions of the passive systems also provide certain defense-in-depth backup to the primary passive features. For example, while the Isolation Condenser System (ICS) is the primary safety-related heat removal and inventory control feature in a non-loss-of-coolant transient, the automatic depressurization system (ADS), together with the Gravity Driven Cooling System (GDCS), provide safety-related, defense-in depth backup. All active systems requiring AC power to operate are designated as non-safety related.

The ALWR Utility Requirements Document (URD) for passive plants, issued by the Electric Power Research Institute, recommends that the plant designer specifically define the active systems relied upon for defense-in-depth. Passive systems are able to perform their safety functions for 72 hours after an initiating event. After 72 hours, non-safety or active systems may be required to replenish the passive systems or to perform core and containment heat removal duties directly. The ESBWR includes active systems that provide defense-in-depth capabilities for reactor coolant system makeup and decay heat removal. These active systems are the first line of defense in reducing challenges to the passive systems in the event of transients or plant upsets. In general, these systems are designated as non-safety related.

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

- Determine whether regulatory oversight for certain non-safety 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 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 resolve 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.

20.1.2 Systematic Approach

Sections 20.2 through 20.6 of this report address Criteria A through E above by systematically identifying non-safety 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. Any outliers identified in this process are noted as candidates for RTNSS and are further analyzed in Section 20.7.

Criterion C is assessed probabilistically, by quantitative and qualitative methods based on information derived from the baseline PRA and also a focused PRA. The baseline PRA (NEDO-33201) is a comprehensive analysis that is being performed in conjunction with the design phase of the ESBWR. It provides an integrated assessment of the ESBWR design in response to transient and accident conditions; identifies areas where further improvement can reduce risk in the design and operational phases; and quantifies the risk estimates to assess the capability of the ESBWR design to meet the NRC safety goals of CDF less than 1 E-4 per year and LRF less than 1 E-6 per year. In addition, a focused PRA was developed to evaluate the whether existing passive systems were adequate to meet the NRC safety goals without the capability of non safety related active systems. If the probabilistic analyses determine that the NRC Safety Goals cannot be met without certain non-safety systems, they are identified as candidates SSCs for RTNSS.

Each candidate system is analyzed in Section 20.7 to determine whether or not it should be considered for regulatory oversight in accordance with the RTNSS process. Section 20.8 provides the basis for an appropriate level of regulatory oversight for the final list of SSCs that are considered to be RTNSS.

20.2 CRITERION A: BEYOND DESIGN BASIS EVENTS ASSESSMENT

20.2.1 ATWS Assessment

ATWS events are described in Section 15.5.4 of the DCD. Based upon the results of the analyses, the proposed design for the ESBWR is satisfactory for mitigating the consequences of an ATWS. All performance requirements specified in Subsection 15.5.4.3.2 are met. The Standby Liquid Control (SLC) system, used to mitigate an ATWS event, is classified as safety-related. Therefore, the SLC system is not a candidate for regulatory oversight in accordance with RTNSS Criterion A.

20.2.2 Station Blackout Assessment

Response to an SBO event is analyzed in Section 15.5.5 of the DCD. The analysis demonstrates that reactor water level is maintained above the top of active fuel. With operation of PCCS, the containment and suppression pool pressures and temperatures are maintained within their design limits. Therefore, the integrity for containment is maintained. Each acceptance criterion in Subsection 15.5.5.1 is met. The ESBWR is designed to successfully mitigate an SBO event to meet the requirements of 10 CFR 50.63.

In summary, there are no AC Power systems needed to address SBO issues and therefore, there are no candidates for regulatory oversight based on Criterion A.

20.3 CRITERION B: LONG-TERM SAFETY ASSESSMENT

20.3.1 Actions Required Beyond 72 Hours

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

FPS has one motor-driven and two diesel driven pumps, and is classified as non-safety related but is designed so that portions of the system remain operable following a seismic event. These portions include the diesel driven pump in the Fire Protection Enclosure (FPE), the water supply, the suction pipe from the water supply to the pump, one of the supply pipes from the FPE to the Reactor Building, and the connections to the FAPCS. Therefore, RTNSS Criterion B applies to selected portions of the ESBWR fire protection system.

There are other long-term manual actions required to maintain plant support systems such as establishing long-term room cooling, and maintaining AC and DC power. These actions are considered to be routine recovery tasks that do not require special hardware and do not meet Criterion B.

20.3.2 Criterion B: Seismic Assessment

The seismic margins analysis in Section 15 of NEDO-33201 assesses the seismic ruggedness of plant systems, both safety-related and non safety-related. The conclusion is that no accident sequence has a HCLPF lower than 0.60 g, which is twice the magnitude of the safe shutdown earthquake (SSE).

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

20.4 CRITERION C: PRA MITIGATING SYSTEMS ASSESSMENT

20.4.1 Focused PRA Sensitivity Study

A sensitivity study was performed which used a focused PRA to evaluate the whether the passive systems alone were adequate to meet the NRC safety goals of CDF less than 1 E-4 per year and LRF less than 1 E-6 per year. If non-safety related systems were needed to reduce CDF or LRF results to meet the safety goals, they would be candidates for additional regulatory oversight.

The focused PRA retained the same initiating event frequencies as the baseline PRA, and set the failure probabilities of non-safety related systems to TRUE, i.e., failed, while safety related system failure probabilities remained unchanged. The PRA model was revised using the systems shown in Table 20.4-1. As the table shows, only safety systems were credited. The CDF for this case is 8.13 E-6/year, which is lower than the NRC safety goal.

The results of the internal events PRA were evaluated in containment event trees to calculate an LRF value for the focused PRA of 4.2 E-7/year, which is also lower than the NRC safety goal. Approximately 80% of the LRF contribution is associated with steam explosions caused by a high water level in the lower drywell at the time of vessel failure. In the baseline PRA, no Class III scenarios had high water in the lower drywell. In the focused PRA, however, some cutsets did result in high water level in the lower drywell. These cutsets were conservatively treated as containment failure scenarios. Further discussion on containment performance is provided in Section 20.5.

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

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

20.4.2 Assessment of Non-Safety Systems on External Events

The risk impact of non-safety systems relative to external events, at power and during shutdown, has a negligible effect on the CDF and LRF goals. The following insights support this conclusion:

20.4.2.1 Fire

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 or LRF values from this Fire PRA relative to the Focused PRA. Instead, the qualitative insights from the Fire PRA are considered in the RTNSS process.

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

(1) The ESBWR, due to its basic layout and safety design features, is inherently capable of mitigating potential 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 from there. One feature relevant to the design is that 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 opportunity to perform manual actuations for failed automatic actuations that may occur.

The separation, redundancy, fire protection and suppression features built into the design result in CDF and LRF risks due to internal fires are not significant. Although the effects of non-safety systems are not specifically addressed in the fire scoping analysis due to the conservative bounding methods that were used, they do not play a significant role in mitigation because fire separation typically results in one division of SSCs being damaged while the safety functions from the remaining divisions are intact and capable of achieving safe shutdown conditions.

20.4.2.2 Flood

Due to the inherent ESBWR flooding mitigation capability, some flooding specific design features are key in the mitigation of significant flood sources. Although not highly risk significant, the shutdown flooding analysis identified the need to be able 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. Although the effects of non-safety systems are not specifically addressed in the flooding analysis due to the conservative screening methods that were used, they do not play a significant role in mitigation because separation typically results in one division of SSCs being damaged while the safety functions from the remaining divisions are intact and capable of achieving safe shutdown conditions.

20.4.2.3 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.

20.4.2.4 Seismic

The ESBWR plant and equipment are capable of withstanding an earthquake with a magnitude at least two times the safe shutdown earthquake (SSE). No accident sequence has a HCLPF lower

than 0.60 g. In addition, only passive safety systems are credited in the seismic event tree. In addition, FPS is classified as non-safety related but is designed so that the diesel driven pump in the Fire Protection Enclosure (FPE), the water supply, the suction pipe from the water supply to the pump, one of the supply pipes from the FPE to the Reactor Building, and the connections to the FAPCS remain operable following a seismic event. There are no seismic-related candidates for RTNSS consideration.

20.4.3 Assessment of Uncertainties

Some non-safety SSCs are considered for regulatory oversight because of uncertainties inherent in their passive safety functions. An evaluation of these types of uncertainties, such as squib valves, is provided in Chapter 11 of NEDO-33201. No SSCs were identified in Chapter 11 as candidates for RTNSS.

There are uncertainties in the design of Basemat-Internal Melt Arrest and Coolability System (BiMAC) system, and this is addressed in the discussion on containment event trees in Section 8 of NEDO-33201. Therefore, the BiMAC system is a candidate for RTNSS.

20.4.4 Criterion C: PRA Initiating Events Assessment

The At-Power and Shutdown PRA models were reviewed to determine whether non-safety SSCs could have a significant effect on the estimated frequency of events. The following screening criteria were imposed on the at-power and shutdown initiating events:

(1) Could these non-safety SSCs significantly contribute to the occurrence of an initiating event?

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

If the answer to both of these questions is "Yes", then the non-safety SSC is a candidate for regulatory oversight. The results are discussed below and are summarized in Table 20.4-2.

20.4.4.1 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 non-safety SSCs, screening question 1 in Table 20.4-2 is answered "Yes." However, the Generic Transient contributes less than 1% to CDF and LRF (NEDO-33201 Section 7.2). Therefore, there are no specific non-safety systems that have a significant effect on risk, and there are no candidates for regulatory oversight from this category.

20.4.4.2 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 non-safety related, and thus Question 1 is 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 will be analyzed in Section 20.7 as potential candidates for regulatory oversight.

20.4.4.3 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 functions requiring AC power. The associated SSCs that comprise the onsite AC power distribution system are non-safety related, and thus, Question 1 is answered "Yes." LOPP is a significant contributor to CDF and LRF (NEDO-33201 Section 7.2). Therefore, the AC power system will be analyzed in Section 20.7 as a potential candidate for regulatory oversight.

20.4.4.4 At-Power LOCA

Loss of coolant accidents are initiated by piping leaks, valve leaks, breaks, or inadvertent opening of relief valves. LOCAs are postulated to initiate in non-safety 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 and Main Steam piping have redundant isolation valves that automatically close on a LOCA signal.

Safety/Relief Valves are safety-related, therefore, a loss of coolant accident due to an inadvertent opening of a Safety/Relief Valve is not a candidate for regulatory oversight.

There are no candidates for regulatory oversight from this category.

20.4.4.5 Shutdown Loss of Preferred Power

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

20.4.4.6 Loss of Shutdown Cooling

The decay heat removal function during all shutdown modes of operation is provided by the Reactor Water Cleanup/Shutdown Cooling System (RWCU/SDCS) operating in shutdown cooling mode. In mode 5 with the reactor well flooded, the Fuel and Auxiliary Pools Cooling System (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.

In modes 4 and 5 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 Question 1 is answered "No."

There are no candidates for regulatory oversight from this category.

20.4.4.7 Shutdown LOCA

The frequency of these events is expected to be lower than at full power, due to the reduced vessel pressure and temperature. Also, control rods are fully inserted, and the reduced pressure and temperature of the reactor coolant, along with 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 in during shutdown. The rest of the RPV vessel piping is isolated. The RWCU/SDCS and FAPCS containment penetrations have redundant and automatic power-operated containment isolation valves that close on signals from the leak detection and isolation system and the reactor protection system.

There are no candidates for regulatory oversight from this category.

20.4.5 Mitigating Systems Summary

The safety goals for CDF and LRF are met with the Focused PRA models. However, due to the considerations of uncertainty, the following system is a candidate for regulatory oversight:

- BiMAC System

The assessment of the importance of non-safety SSCs with respect to initiating events is summarized in Table 20.4-2. Based on the assessment of initiating events, the following SSCs are candidates for regulatory oversight:

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

20.5 CRITERION D: CONTAINMENT PERFORMANCE ASSESSMENT

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

The containment bypass issue from SECY-93-087, Issue II.G, during severe accidents is concerned with potential sources of steam bypassing the suppression pool and failure of heat exchanger tubes in passive containment cooling systems. These concerns are addressed in the Design Control Document. Section 6.2.1.1.5 addresses the steam bypass of the suppression pool. 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, and no additional RTNSS related effort is needed.

20.6 CRITERION E: ASSESSMENT OF SIGNIFICANT ADVERSE INTERACTIONS

20.6.1 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 that there was the potential for unrecognized subtle dependencies among SSCs to be unidentified, and that they could possibly lead to safety-significant events. The term used to describe these unrecognized, subtle dependencies is adverse systems interactions (ASIs). The NRC did not recommend that licensees 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.

20.6.2 Systematic Approach

The purpose of this analysis is to systematically evaluate adverse interactions between the active and passive systems in the design phase of the ESBWR certification process. 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 non safety-related systems are analyzed further as RTNSS candidates.

20.6.3 Gravity Driven Cooling System (GDCS)

20.6.3.1 Design Features

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

20.6.3.2 System Interfaces

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

20.6.3.3 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.

The Fuel and Auxiliary Pools Cooling System (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 independent 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 cleaner water in other pools. The power operated 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. In this case, the Deluge squib valves and actuation logic are safety-related, and the probability of an inadvertent actuation is extremely low.

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

20.6.4 Automatic Depressurization System (ADS)

20.6.4.1 Design Features

The depressurization function is accomplished through the use of safety/relief valves (SRVs) and depressurization valves (DPVs). Supporting systems for ADS include the instrumentation, logic, control and motive power sources. The instrumentation and logic power is obtained from corresponding 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 divisional 250 VDC batteries. The motive power for the electrically operated pneumatic pilot solenoid valves on the SRVs is from accumulators located near the SRVs, which are supplied with nitrogen by the High Pressure Nitrogen Supply System.

20.6.4.2 System Interfaces

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

20.6.4.3 Analysis of Potential Adverse System Interactions

DC Power supplies the SRV solenoids and the DPV squib valves. Two squibs singly or jointly, actuate a booster, which actuates the shearing plunger. The squibs are initiated by either one or both of 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.

Nitrogen accumulators provide driving force for the pneumatic pilot solenoid ADS valves. The High Pressure Nitrogen Supply System (HPNSS) 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.

20.6.5 Isolation Condenser System (ICS)

20.6.5.1 Design Features

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

Each IC is located in a subcompartment of the Isolation Condenser/Passive Containment Cooling (IC/PCC) pool, and all pool subcompartments communicate at their lower ends to enable full utilization of the collective water inventory, independent of the operational status of any given IC train. A valve is provided at the bottom of each IC/PCC pool subcompartment that can be closed so the subcompartment can be emptied of water to allow IC maintenance. Pool water can heat up to about 101°C (214°F); steam that is formed, being non-radioactive and having a slight positive pressure relative to station ambient, vents from the steam space above each IC segment where it is released to the atmosphere through large-diameter discharge vents. A moisture separator is installed at the entrance to the discharge vent lines to preclude excessive moisture carryover. IC/PCC pool makeup clean water supply for replenishing level during normal plant operation is provided from FAPCS. A 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 be 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 (motor operated, fail as-is), and, (2) a condensate return bypass valve (nitrogen piston operated, 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 motor-operated 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 nitrogen piston-operated condensate return bypass valve opens if the DC power is lost.

20.6.5.2 System Interfaces

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

20.6.5.3 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 non safety-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.

20.6.6 Standby Liquid Control System (SLCS)

20.6.6.1 Design Features

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

20.6.6.2 System Interfaces

Control Building, Containment, DC Power

20.6.6.3 Analysis of Potential Adverse System Interactions

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

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

20.6.7 Passive Containment Cooling System (PCCS)

20.6.7.1 Design Features

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

20.6.7.2 System Interfaces

Containment, FAPCS, ICS, Suppression Pool

20.6.7.3 Analysis of Potential Adverse System Interactions

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

20.6.8 Adverse Systems Interactions Summary

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

20.7 SELECTION OF IMPORTANT NON-SAFETY SYSTEMS

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

20.7.1 Fire Protection Makeup to Upper Containment Pools

The FPS makeup to the upper containment pools should be considered for regulatory oversight in accordance with Criterion B, long-term actions, i.e., actions required beyond 72 hours to ensure safe shutdown conditions. The FPS is classified as non-safety related but is designed so that portions of the system remain operable following a seismic event. These portions include the diesel driven pump in the Fire Protection Enclosure (FPE), the water supply, the suction pipe from the water supply to the pump, one of the supply pipes from the FPE to the Reactor Building, and the connections to the FAPCS.

20.7.2 Basemat-Internal Melt Arrest and Coolability System (BiMAC)

The BiMAC function has been developed to a conceptual level, with several design details that are not yet finalized. These details are needed to justify the target failure probability of 1 E-3. BiMAC plays an important role in mitigating core melt scenarios, therefore, it is a candidate for RTNSS consideration.

20.7.3 Feedwater and Condensate Systems

These systems were found to 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. It is single failure proof, and thus, a controller failure is much less likely to occur in the ESBWR than in current generation reactors. In addition, there is added protection not available in the current reactors, such as 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 (Level 8), and trip of the FW pumps on reactor water Level 9.

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.

20.7.4 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 utility, but they would be maintained by an internal 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. In summary, 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.

20.8 PROPOSED REGULATORY OVERSIGHT

Section 20.7 summarizes the candidates for RTNSS consideration that were identified in the preceding analysis. In this section, each RTNSS candidate is evaluated to determine its relative risk significance, whether regulatory oversight is prudent, and a proposed method of regulatory oversight.

20.8.1 Risk Significance

The Level 1 PRA results consist of minimal cutsets leading to core damage, as well as importance measures of those components and systems represented as basic events in the models (i.e., internal events, external events, and shutdown models.) The Level 2 PRA results are measured relative to the large release frequency. These results provide the basis for a systematic review to identify important features and capabilities. In most cases, cutsets and importance measures identify functions at the component level. By reviewing the accident sequences resulting from this detailed evaluation, it is possible to identify those systems, features and functions which are most important in assuring that the ESBWR CDF and LRF are very low.

In addition, some qualitative assessment is necessary to prioritize candidate issues dealing with seismic events, and long-term actions, i.e., beyond the 24-hour success cutoff for normal CDF calculations.

If the quantitative and qualitative analyses determine an RTNSS candidate to be significant to public health and safety (i.e., if needed 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.

If a candidate is less significant, then reliability and availability controls should be assigned in accordance with the Reliability Assurance Program.

20.8.2 Fire Protection Makeup to Upper Containment Pools

FPS makeup to the upper containment 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 relative risk significance is low.

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

20.8.3 Basemat-Internal Melt Arrest and Coolability System (BiMAC)

BiMAC functions during severe accidents, and thus has no effect on the level 1 PRA. The inclusion of the BiMAC in the ESBWR design provides an engineered method to assure good heat transfer between a debris bed and cooling water. By flooding the lower drywell after the introduction of core material, the potential for energetic fuel-coolant interaction is minimized. Covering core debris with water provides scrubbing of fission products released from the debris and cools the corium, thus limiting potential core-concrete interaction (CCI). The BiMAC provides additional assurance of debris bed cooling by providing engineered pathways for water flow through the debris bed. BiMAC failure could occur if there were no water supplied. Other

failure mechanisms include manufacturing defects, unforeseen phenomenology problems or a broken GDCS line that would divert flow. In these instances, the situation becomes similar to flooding the debris bed without the engineered flow through the corium. Thus, BiMAC failure to function can be conservatively modeled as failure to supply water from the GDCS deluge line.

The 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, but 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 is to include the BiMAC function and related components within the Reliability Assurance Program.

Table 20.4-1

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 20.4-2

Initiating Events Assessment for RTNSS

Dominant Initiating Events	Are There Non-Safety SSCs That Prevent Initiator Occurrence?	Do the Non-Safety SSCs Significantly Affect CDF or LRF?
At-Power Initiating Events		
Generic Transients	Yes	No
Transient with Loss of Feedwater	Yes	Yes
Loss of Preferred Power	Yes	Yes
LOCA	No	N/A
Shutdown Initiating Events		
Shutdown Loss of Preferred Power	Yes	Yes
Loss of Shutdown Cooling	No	No
Shutdown LOCA	No	N/A