

GE-Hitachi Nuclear Energy Americas LLC

James C. Kinsey  
Project Manager, ESBWR Licensing

PO Box 780 A55  
Wilmington, NC 28402-0780  
USA

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

MFN 07-373

Docket No. 52-010

July 15, 2007

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

**Subject:** Draft DCD ESBWR Appendix 19A Regulatory Treatment Of Non-Safety Systems (RTNSS).

Enclosure 1 contains GEH's draft revision to DCD Chapter 19 "Probabilistic Risk Assessment showing changes to Appendix 19A REGULATORY TREATMENT OF NON-SAFETY SYSTEMS (RTNSS).

The attached text shows changes that were made to clarify the meaning of the Appendix. These changes will be included in Revision 4 of the DCD.

Sincerely,



James C. Kinsey  
Project Manager, ESBWR Licensing

DC68

Enclosures:

1. ESBWR Design Control Document Tier 2 Chapter 19 *Probabilistic Risk Assessment and Severe Accidents. Appendix 19A REGULATORY TREATMENT OF NON-SAFETY SYSTEMS (RTNSS)*. Draft Unverified for Information Only.

cc:   AE Cabbage            USNRC (with enclosures)  
      George Stramback    GHE/San Jose (with enclosures)  
      RE Brown             GHE/Wilmington (with enclosures)

eDRF Section 0000-0070-2559

Enclosure 1

MFN 07-373

ESBWR Design Control Document Tier 2 Chapter 19  
Probabilistic Risk Assessment and Severe Accidents.

Appendix 19A

REGULATORY TREATMENT OF NONSAFETY  
SYSTEMS (RTNSS).

Draft Unverified for Information Only.

Related to ESBWR Design Certification Application  
ESBWR Probabilistic Risk Assessment

ESBWR

Draft Unverified for Information Only

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

### 19A.1 INTRODUCTION

The purpose of this Section is to demonstrate that the ESBWR design adequately addresses Regulatory Treatment of Non-Safety Systems (RTNSS) issues. A systematic process is used in the ESBWR design process to identify regulatory guidance and assess it relative to specified ESBWR design features to determine if additional regulatory treatment is warranted for structures, systems, or components (SSCs) that perform a significant safety, special event, or post-accident recovery function.

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

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

- (1) Determine whether regulatory oversight for certain nonsafety-related systems is needed.
- (2) Identify risk important SSCs for regulatory oversight (if it is determined that regulatory oversight is needed).
- (3) Decide on an appropriate level of regulatory oversight for the various identified SSCs commensurate with their risk importance.

The following SECY-94-084 criteria are applied to the ESBWR design to determine the systems that are candidates for consideration of regulatory oversight:

- ⊖A) SSC functions relied upon to meet beyond design basis deterministic NRC performance requirements such as 10 CFR 50.62 for anticipated transient without scram (ATWS) mitigation and 10 CFR 50.63 for station blackout (SBO).
- ⊖B) SSC functions relied upon to resolve long-term safety (beyond 72 hours) and to address seismic events. Criterion B is divided into two groupings:
  - Criterion B1 addresses those functions that provide defense in depth for key safety functions (core cooling, decay heat removal and control room habitability) that are designed to Seismic Category II standards so there is reasonable assurance that they can perform their functions following a seismic event.
  - Criterion B2 addresses components that provide additional information for operators to diagnose plant conditions, (post-accident monitoring) and thus have a less direct effect on the success of key safety functions. Reasonable assurance for long-term functionality of monitoring components is provided by other augmented seismic design criteria, as discussed below.

## ESBWR

**Draft Unverified for Information Only**

- ⊖C) SSC functions relied upon under power-operating and shutdown conditions to meet the NRC's safety goal guidelines of a core damage frequency (CDF) of less than  $1.0E-4$  per reactor year and large release frequency (LRF) of less than  $1.0E-6$  per reactor year.
- ⊖D) SSC functions needed to meet the containment performance goal (SECY-93-087, Issue I.J), including containment bypass (SECY-93-087, Issue II.G), during severe accidents.
- ⊖E) SSC functions relied upon to prevent significant adverse systems interactions.

Upon the identification of candidates for RTNSS consideration, the ESBWR design process evaluates each candidate to determine if RTNSS designation is made. Following selection of all RTNSS equipment, a risk evaluation is performed to determine the appropriate regulatory controls.

**19A.1.1 Selection of Important Non-Safety Systems**

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

Criteria A, B, D and E are assessed using deterministic methods, including an assessment of containment performance. Criterion C is assessed probabilistically, by quantitative and qualitative methods based on information derived from the baseline PRA and also a focused PRA sensitivity study. The baseline PRA, described in DCD Tier 2 Chapter 19 is a comprehensive analysis that is performed in conjunction with the design phase of the ESBWR. It is an integrated assessment of the ESBWR design as it applies to transient and accident conditions. It identifies areas where further improvement can reduce risk in the design and operational phases and it quantifies the risk estimates to assess the capability of the ESBWR design to meet the NRC safety goals of CDF less than  $1.0 E-4$  per year and LRF less than  $1.0 E-6$  per year. The focused PRA sensitivity study evaluates whether the existing passive systems are solely adequate to meet the NRC safety goals, that is, without the benefit of the available nonsafety-related active systems.

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

**19A.2 CRITERION A: BEYOND DESIGN BASIS EVENTS ASSESSMENT****19A.2.1 ATWS Assessment**

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

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

- Automatic feedwater runback under conditions indicative of an ATWS; and

## ESBWR

## Draft Unverified for Information Only

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

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

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

~~The ESBWR design includes an ARI system with sensors and logic that are independent and diverse of the RPS.~~

~~Most of SLCS is safety related and therefore has sufficient regulatory oversight. However, there is an ATWS actuation logic performed by the Diverse Protection System (DPS), which is a non-safety related system. The logic includes an isolation of RWCU/SDC~~

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

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

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

### 19A.2.2 Station Blackout Assessment

The ESBWR is designed to cope with a station blackout (SBO) event for 72 hours. The analysis in DCD Tier 2, Subsection 15.5.5 demonstrates that reactor water level is maintained above the top of active fuel by operation of the Isolation Condenser System (ICS), which is safety-related. With operation of the Passive Containment Cooling System (PCCS), the containment and suppression pool pressures and temperatures are maintained within their design limits. Therefore, the integrity for containment is maintained. The ESBWR is designed to successfully mitigate an SBO event to meet the requirements of 10 CFR 50.63. There are no RTNSS candidates for SBO based on Criterion A.

### 19A.3 CRITERION B: LONG-TERM SAFETY ASSESSMENT

#### 19A.3.1 Actions Required Beyond 72 Hours

The safety functions that are required to be maintained in the long term are:

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

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

##### 19A.3.1.1 *Core Cooling*

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

There are no RTNSS systems associated with this safety function.

##### 19A.3.1.2 *Decay Heat Removal*

The safety function is to remove reactor decay heat from the core, containment, and spent fuel pool. The passive systems that provide this function for the core and containment are the safety-related ICS and the safety-related Passive Containment Cooling System (PCCS). These systems are capable of removing decay heat for at least 72 hours without the need for active systems or operator actions. After 72 hours, makeup water is needed to replenish the boil-off from the upper containment and spent fuel pools. The ESBWR design includes permanently installed piping in the Fuel and Auxiliary Pools Cooling System (FAPCS) that connects directly to a diesel-driven makeup pump system. This connection enables the upper containment pools and spent fuel pools to be filled with water from the Fire Protection System (FPS), which

**Draft Unverified for Information Only**

provides on-site makeup water to extend the cooling period from 72 hours to 7 days. The dedicated FPS equipment for providing makeup water and the flow paths to the pools are classified as nonsafety-related. Some of the piping that interfaces between FPS, FAPCS, and the pools is safety-related, as described in Tier 2 Subsection 9.1.3. The spent fuel pool is normally cooled by FAPCS. However, on a complete loss of FAPCS cooling under the condition of maximum heat load, a sufficient quantity of water is available in the spent fuel pool to allow boiling for 72 hours and still provide acceptable ~~minimum~~ fuel coverage in the pool. A dedicated external connection to the FAPCS line allows for manual hook-up of external water sources, if needed, at 7 days for either upper containment pool replenishment and for spent fuel pool makeup. These functions are manually actuated from the yard area and can be performed without any support systems.

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

**19A.3.1.3 Control Room Habitability**

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

This generator is included within the scope of RTNSS.

**19A.3.1.4 Post-Accident Monitoring**

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

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

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

The standby diesel generators and the PIP buses provide power for Q-DCIS. Portions of the HVAC systems in the Reactor Building, Electrical Building, Fuel Building, Control Building, and some areas of the Turbine Building perform component and area cooling. In addition,

ESBWR

**Draft Unverified for Information Only**

support for these nonsafety-related functions is required from Reactor Component Cooling Water, Plant Service Water, and the Chilled Water System.

**19A.3.2 Seismic Assessment**

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

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

~~The seismic requirements for Criterion B RTNSS equipment can be divided into two classes:~~

~~B1 These are the RTNSS systems required for continued core cooling, decay heat removal, and control room habitability. These systems are designed as Seismic Category II.~~

~~B2 These are the RTNSS systems required for post accident monitoring, as described in 19A.3.1.4. These systems are designed to International Building Code Category 4 requirements for seismic ruggedness.~~

**19A.4 CRITERION C: PRA MITIGATING SYSTEMS ASSESSMENT**

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

**19A.4.1 Focused PRA Sensitivity Study**

A focused PRA sensitivity study evaluates whether passive systems alone are adequate to meet the NRC safety goals of CDF less than 1.0 E-4 per year and LRF less than 1.0 E-6 per year. The focused PRA retains the same initiating event frequencies as the baseline PRA, and sets the status of nonsafety-related systems to failed, while safety-related systems remain unchanged in the model. The focused PRA model is evaluated using only the safety-related systems and RTNSS systems determined from criteria A or B. Additional nonsafety-related systems are included only if they are required to meet the CDF or LRF goals. The additional nonsafety-related systems required to meet the CDF and LRF goals are candidates for RTNSS.

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

Insights from the shutdown model results indicate that the dominant risk contributor is a LOCA in an instrument or drain line connected to the vessel 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 candidates for regulatory oversight.

## ESBWR

## Draft Unverified for Information Only

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

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

**19A.4.2.1 Fire**

The Fire PRA is a bounding analysis that incorporates several conservative assumptions. The fire analysis does not account for the amount of combustible material present, or for the distance between fire sources and targets. The analysis assumes that a fire ignition in any fire area 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:

- The basic layout and safety design features of the ESBWR make it inherently capable of mitigating internal fires. Safety system redundancy and physical separation by fire barriers ensure that, in all cases, a single fire limits damage to a single safety system division. Fire propagation to neighboring areas presents a relatively minor risk contribution due to fire barriers.
- A fire in the control room is assumed to affect the execution of human actions. A fire in the control room does not affect the automatic actuations of the safety systems. Additionally, the existence of remote shutdown panels allows the detection of failed automatic actuations and the performance of compensatory manual actuations.

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

**19A.4.2.2 Flood**

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

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

## ESBWR

**Draft Unverified for Information Only**

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

**19A.4.2.3 Wind**

The conclusion from the ESBWR 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 results is bounded by a loss of offsite power with the plant safety systems available, and is thus negligible with respect to CDF and LRF.

**19A.4.2.4 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). 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 (~~Seismic Category II~~). Piping and components completely separate from FAPCS pool cooling piping provide flow paths for post-accident make-up water transfer to the IC/PCC pools and spent fuel pool. This piping and components are designed to meet Quality Group C and Seismic Category II requirements. Therefore, there are no seismic-related candidates for RTNSS consideration.

**19A.4.3 Assessment of Uncertainties**

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

Passive system T-H uncertainties manifest themselves in the PRA model within failure probabilities and success criteria. Passive components that must rely on natural forces, such as gravity, have lower driving forces than conventional pumped systems so additional margin is incorporated into the design. Some passive functions are based on new engineering design, with limited operating experience to establish confidence in the failure rate estimates. The PRA models the effectiveness of passive safety functions in the failure rate estimated and success criteria that are factored into the event trees. Therefore, assessing the event tree success criteria in the PRA model identifies T-H uncertainties.

There are also uncertainties associated with the manual alignment and operation of long-term decay heat removal systems identified under RTNSS Criterion B. These uncertainties can influence the results such that there is a challenge to the CDF and LRF goals in transient sequences. This is not an issue for low frequency scenarios, such as large LOCA or seismic events.

In order to address these uncertainties, the FAPCS system is added as a RTNSS candidate. This system has the capability to provide a core injection function and to provide a decay heat removal function. The support systems needed to use this system are RCCWS, diesel generators,

ESBWR

**Draft Unverified for Information Only**

PIP buses, Fuel Building HVAC, and PSWS. These are all considered to be covered by RTNSS for Criterion C.

The function of FAPCS is provided as a two train system. The trains are physically and electrically separated such that no single active component failure can fail the function. This provides the CDF and LRF reduction needed to address the PRA uncertainty concerns.

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

#### **19A.4.4 PRA Initiating Events Assessment**

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

- ~~Could these~~ Are non-safety related SSCs ~~significantly contribute to~~ considered in the calculation of the ~~occurrence of an~~ initiating event frequency?
- Does the unavailability of these non-safety-related SSCs ~~have a~~ significantly affect the calculation of ~~impact on~~ the initiating event frequency?
- Does the initiating event significantly affect CDF or LRF for the baseline PRA?

If the answer to all three of these questions is “Yes”, then the non-safety SSC is a RTNSS candidate. The results are discussed below.

##### **19A.4.4.1 At-Power Generic Transients**

Initiating events that are considered Generic Transients are described in subsection 19.2.3.1. Because several initiating events in this group are caused by the failures of non-safety-related SSCs, screening questions 1, 2, and 3 ~~in Table 19.A-1~~ are answered “Yes.” However, this category of transient initiating events includes various failures of components or operator errors. No specific non-safety-related systems have a significant effect on risk, and there are no RTNSS candidates from this category.

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

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

##### **19A.4.4.3 At-Power Transient with Loss of Feedwater**

The initiating events in this group begin with a prompt and total loss of feedwater and require the success of other mitigating systems for reactor vessel level control. The SSCs related to

## ESBWR

**Draft Unverified for Information Only**

feedwater and condensate are nonsafety-related, and thus Questions 1, 2, and 3 are answered "Yes." The loss of feedwater is a significant contributor to CDF, so the feedwater and condensate systems are RTNSS candidates. However, several features in the advanced design of the new generation feedwater level control system add significant reliability and, thus, a lower failure probability for loss of feedwater initiating events. The feedwater level control system is implemented on a triplicate, fault-tolerant digital controller. Therefore, a control failure is much less likely to occur in the ESBWR than in the design of current generation of reactors.

The dominant contributors to a total loss of feedwater are a loss of control power to the feedwater controllers and loss of AC power to the pumps. Only a total and immediate loss of all feedwater flow is included in the Loss of Feedwater initiating event category. A controller failure that results in reduced feedwater flow is considered a transient, which is much less significant than a complete loss of feedwater.

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

**19A.4.4.4 At-Power Loss of Preferred Power**

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

~~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." Loss of preferred power is a significant contributor to CDF and LRF for at power and shutdown risk. However, the 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 weather related faults. These are outside the scope of the certified design. The other SSCs that prevent a loss of offsite power, such as substations, breakers, and motor control centers, protective relays, etc. are much less risk significant and below the threshold for RTNSS consideration. Therefore, the SSCs within the ESBWR design scope for preventing a loss of offsite power initiating event are not risk significant and do not warrant additional regulatory oversight.~~

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

ESBWR

Draft Unverified for Information Only

**19A.4.4.5 At-Power LOCA**

Loss of coolant accidents are initiated by piping leaks, valve leaks, or breaks. LOCAs are postulated to initiate in systems, such as RWCU/SDC and Main Steam. However, general design considerations require that all piping and components within the reactor coolant pressure boundary be safety-related. The RWCU/SDC and Main Steam piping have redundant safety-related isolation valves that automatically close on a LOCA signal. ~~re-are no~~ Questions 1, 2, and 3 are answered "No."

In addition, Safety/Relief Valves are safety-related. Therefore, there are no RTNSS candidates from this category.

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

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

**19A.4.4.7 Loss of Shutdown Cooling**

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

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

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

There are no RTNSS candidates for regulatory oversight.

**19A.4.4.8 Shutdown LOCA**

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

Breaks outside containment can be originated only in ICS, RWCU/SDC or FAPCS piping, or instrument lines, because these are the only systems that remove reactor coolant from the containment during shutdown. The rest of the RPV vessel piping is isolated. The RWCU/SDC and FAPCS containment penetrations have redundant and automatic power-operated safety-related containment isolation valves that close on signals from the leak detection and isolation system and the reactor protection system. The ICS lines have redundant power operated safety-related isolation valves inside containment to terminate a loss of inventory in the event of an ICS line break outside of containment. Questions 1, 2, and 3 are answered "No."

There are no RTNSS candidates from this category, although availability controls on the lower drywell hatches are provided (see 19.A.4.2.2).

ESBWR

Draft Unverified for Information Only

#### 19A.4.5 Summary of RTNSS Candidates from Criterion C

The focused PRA sensitivity study requires certain portions of DPS being designated as RTNSS. The portions that provide capability for a manual backup of safety-related automatic actuation of ECCS provides the level of protection necessary to meet both the CDF and LRF goals.

The assessment of uncertainties concludes that the defense-in-depth role of FAPCS in providing a backup source of low pressure injection and suppression pool cooling is within the requirements for RTNSS.

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

#### 19A.5 CRITERION D: CONTAINMENT PERFORMANCE ASSESSMENT

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

The containment bypass issue from SECY-93-087, Issue II.G, during severe accidents is concerned with potential sources of steam bypassing the suppression pool and failure of heat exchanger tubes in passive containment cooling systems. These concerns are addressed in the Design Control Document. Tier 2 Subsection 6.2.1.1.5 addresses the steam bypass of the suppression pool. Tier 2 Subsection 6.2.2.3 addresses the design of the Passive Containment Cooling Heat Exchanger tubes. The Criterion D safety concerns are addressed in the ESBWR design, and no RTNSS candidates are identified.

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

The concerns about adverse system interactions have been addressed for currently operating reactors as NRC Unresolved Safety Issue, Item A-17: SYSTEMS INTERACTIONS IN NUCLEAR POWER PLANTS. Item A-17 acknowledges that systems interactions are usually well recognized and, therefore, are accounted for in the evaluation of plant safety by designers and in plant safety assessments. The concern is the potential for unrecognized subtle dependencies among SSCs to be unidentified and possibly lead to safety-significant events. The term used to describe these unrecognized, subtle dependencies is adverse systems interactions (ASIs). The NRC recommends that 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.

##### 19A.6.1 Systematic Approach

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

## ESBWR

**Draft Unverified for Information Only**

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

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

**19A.6.1.1 Gravity Driven Cooling System (GDCS)****19A.6.1.1.1 Design Features**

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

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

**19A.6.1.1.2 System Interfaces**

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

**19A.6.1.1.3 Analysis of Potential Adverse System Interactions**

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

The following GDCS indications are reported in the control room:

- Status of the locked-open maintenance valves,
- Status of the squib-actuated valves,
- GDCS pools and suppression pool level indication,
- Position of each GDCS check valve,
- Suppression pool high and low level alarm,
- GDCS pools high and low level alarms, and
- Squib valve continuity alarms.

ESBWR

**Draft Unverified for Information Only**

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

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

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

**19A.6.1.2 Automatic Depressurization System (ADS)****19A.6.1.2.1 Design Features**

The depressurization function is accomplished through the use of safety/relief valves (SRVs) and depressurization valves (DPVs). Supporting systems for ADS include the instrumentation, logic, control and motive power sources. The instrumentation and logic power is obtained from corresponding safety-related divisional uninterruptible and 120 VAC power sources. Either source can support ADS operation. The actual SRV solenoid and DPV squib initiator power is supplied by the corresponding safety-related divisional batteries. The motive power for the electrically operated pneumatic pilot solenoid valves on the SRVs is provided by the SRV accumulators that are charged during normal operations by the nonsafety-related High Pressure Nitrogen Supply System. Failure of the HPNSS does not result in a loss of SRV function.

**19A.6.1.2.2 System Interfaces**

Main Steam, Containment, Suppression Pool, DC Power

**19A.6.1.2.3 Analysis of Potential Adverse System Interactions**

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

ESBWR

**Draft Unverified for Information Only**

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

**19A.6.1.3 Isolation Condenser System (ICS)****19A.6.1.3.1 Design Features**

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

Each IC is located in a subcompartment of the Isolation Condenser/Passive Containment Cooling (IC/PCC) pool, and all pool subcompartments communicate at their lower ends to enable full utilization of the collective water inventory, independent of the operational status of any given IC train. A valve is provided at the bottom of each IC/PCC pool subcompartment that can be closed so the subcompartment can be emptied of water to allow IC maintenance. Pool water can heat up to about 101°C (214°F); steam that is formed, being non-radioactive and having a slight positive pressure relative to station ambient, vents from the steam space above each IC segment where it is released to the atmosphere through large-diameter discharge vents. A moisture separator is installed at the entrance to the discharge vent lines to preclude excessive moisture carryover. IC/PCC pool makeup clean water supply for replenishing level during normal plant operation is provided from FAPCS. A nonsafety-related independent FAPCS makeup line is provided to provide emergency makeup water into the IC/PCC pool from the fire protection system and from piping connections located in the reactor yard.

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

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

**19A.6.1.3.2 System Interfaces**

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

**19A.6.1.3.3 Analysis of Potential Adverse System Interactions**

The ICS and PCCS pools (IC/PCC) have two local panel-mounted, safety-related level transmitters. Both transmitter signals are indicated on the safety-related displays and sent through the gateways for nonsafety-related display and alarms. Both signals are validated and

ESBWR

**Draft Unverified for Information Only**

used to control the valve in the makeup water supply line to the IC/PCCS pool. The FAPCS IC/PCC pools cooling and cleanup subsystem pump is automatically tripped on low water level in IC/PCC pools. Water level in the skimmer surge tanks is maintained by automatic open/closure of the makeup water supply isolation valve. Water level in the IC/PCC pools is maintained by automatic open/closure of the makeup water supply isolation valve.

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

Four sets of differential pressure instrumentation are located on the IC steam line and another four sets on the condensate return line inside the drywell. Detection of excessive flow beyond operational flow rates in the steam supply line or in the condensate return line (2/4 signals) results in alarms to the operator, plus automatic isolation of both steam supply and condensate return lines.

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

**19A.6.1.4 Standby Liquid Control System (SLCS)****19A.6.1.4.1 Design Features**

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

**19A.6.1.4.2 System Interfaces**

Control Building, Containment, DC Power

**19A.6.1.4.3 Analysis of Potential Adverse System Interactions**

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

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

**19A.6.1.5 Passive Containment Cooling System (PCCS)****19A.6.1.5.1 Design Features**

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

**19A.6.1.5.2 System Interfaces**

Containment, FAPCS, ICS, Suppression Pool

**19A.6.1.5.3 Analysis of Potential Adverse System Interactions**

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

**19A.6.1.5.4 Monitoring Instrumentation**

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

### 19A.7 SELECTION OF IMPORTANT NON-SAFETY SYSTEMS

The selection of RTNSS systems considers nonsafety-related SSCs that are necessary to meet NRC regulations, safety goal guidelines, and containment performance goal objectives. RTNSS systems needed to meet the NRC regulations specified in Criteria A, B, D and E are based on deterministic analyses. RTNSS systems needed to meet Criteria C and ~~D~~ are based on PRA insights.

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

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

## 19A.8 PROPOSED REGULATORY OVERSIGHT

### 19A.8.1 Regulatory Oversight

Regulatory oversight is applied to each system designated as RTNSS to ensure that it has sufficient reliability and availability to perform its RTNSS function, as defined by the focused PRA, or deterministic criteria. The extent of oversight is commensurate with the safety significance of the RTNSS function, and is categorized as either High Regulatory Oversight (HRO), or Low Regulatory Oversight (LRO), or Support.

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

LRO - If a RTNSS system is not significant, as described above, then the proposed level of regulatory oversight is Low Regulatory Oversight (LRO), which is addressed in regulatory availability specifications, which are described in the Availability Control Manual.

Support – These systems have low risk significance and they provide support (generally component and room cooling) for RTNSS systems that provide active mitigation functions. Treatment of support systems relative to the systems they support is described in the Availability Control Manual. ~~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. This is applicable to the Criterion B deterministic systems. Those classified as B1 are relied upon to perform core cooling, decay heat removal, and control room habitability, and must be protected from external events at a higher level. Those in B2 are for defense in depth and the external event protection is defined at a lower level.~~

~~Fire events are sufficiently addressed with the current regulatory standards, so no additional controls are applied.~~

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

~~If a RTNSS system is not significant, as described above, then the proposed level of regulatory oversight should be in regulatory availability specifications, which are described in the Availability Control Manual.~~

### 19A.8.2 Reliability Assurance

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

ESBWR

Draft Unverified for Information Only

### 19A.8.3 Augmented Design Standards

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

A RTNSS system classified as B1 or B2 that is required to function following a seismic event requires an augmented seismic design criterion. For B1 SSCs, the design is performed in accordance with Seismic Category II. B2 SSCs are designed for seismic requirements in consistent with the International Building Code (IBC) – 2003 by International Code Council, Inc. (300-214-4321). The building structures are classified as Category IV (Power Generating Stations) with an Occupancy Importance Factor of 1.5. Either of the methods permitted by the IBC, simplified analysis or dynamic analysis, is acceptable for determination of seismic loads on NS structures and equipment including those designated as RTNSS. Because these systems are designated to perform their function post 72 hours, the equipment does not need to be able to perform their functions during the seismic event, but must be available following the event.

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

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

Systems that meet RTNSS Criteria ~~A, C, D, or E 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.

### 19A.8.4 Regulatory Treatment

The proposed regulatory treatment of RTNSS systems is presented below, and is summarized in Table 19A-2. ~~Availability controls for each of these functions are contained in NEDO-33331, "ESBWR Availability Controls Manual".~~

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

This function is RTNSS based on the requirements of Criterion A relative to the ATWS Rule, 10 CFR 50.62. The ARI function does not have a high risk significance due to the redundancy and

ESBWR

**Draft Unverified for Information Only**

diversity of the reactor protection system. The proposed level of regulatory oversight for this function should be in the Availability Control Manual.

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

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

**19A.8.4.3 Feedwater Runback Logic**

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

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

The diesel-driven makeup pump is considered for RTNSS in accordance with Criterion B1, long-term actions required beyond 72 hours to ensure safe shutdown conditions. The pump and the FPS piping and valves are classified as nonsafety-related but are designed so that portions of the system remain available following a seismic event to keep equipment required for safe shutdown free from fire damage during a safe shutdown earthquake. In conjunction with the diesel-driven pump, the dedicated connection for FPS makeup includes the Fire 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 IC/PCC pools is a candidate for regulatory oversight in accordance with Criterion B1, actions that are required beyond 72 hours to ensure safe shutdown conditions. When consideration is given to all safety-related and RTNSS equipment, loss of this function does not challenge the CDF or LRF goals. Therefore, the proposed level of regulatory oversight for this function is in the Availability Control Manual.

**19A.8.4.5 Diverse Protection System**

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

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

The BiMAC function has been developed to a conceptual level, with several design details that are not yet finalized. These details are needed to justify the target failure probability of less than 1.0 E-3. BiMAC plays an important role in mitigating core melt scenarios. Therefore, it is a

ESBWR

**Draft Unverified for Information Only**

candidate for RTNSS consideration. The BiMAC device functions during severe accidents, and thus has no effect on the level 1 PRA. The inclusion of the BiMAC device in the ESBWR design provides an engineered method to assure heat transfer between the debris bed and cooling water. By flooding the lower drywell after the introduction of core material, the potential for energetic fuel-coolant interaction is minimized. Covering core debris with water provides scrubbing of fission products released from the debris and cools the corium, limiting potential core-concrete interaction (CCI). The BiMAC device provides additional assurance of debris bed cooling by providing engineered pathways for water flow through the debris bed. BiMAC failure can occur if no water is supplied. Other failure mechanisms include manufacturing defects, unforeseen phenomenology problems or a broken GDCS line that would divert flow. In these instances, the situation becomes similar to flooding the debris bed without the engineered flow through the corium. Thus, BiMAC failure to function can be conservatively modeled as failure to supply water from the GDCS deluge line.

Loss of the BiMAC function does not pose a challenge to the LRF goals when other safety-related and RTNSS systems are taken into account. The proposed level of regulatory oversight for the BiMAC function is in the Availability Control Manual.

**19A.8.4.7 Distributed Control and Instrumentation System**

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

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

Based on a review of the original PRA results, FAPCS can supply core cooling and containment heat removal in certain non-seismic PRA sequences in a backup capacity (that is, two 100% capacity trains.) Due to its expected importance in providing redundancy to core cooling and containment heat removal, FAPCS and its supporting functions (e.g., AC power and component cooling) are therefore RTNSS systems. The loss of any train of FAPCS does not challenge the goals for CDF or LRF, so the proposed level of regulatory oversight for these functions is in the Availability Control Manual.

**19A.8.4.9 AC Power System**

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

ESBWR

Draft Unverified for Information Only

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

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

**19A.8.4.11 Long-Term Containment Integrity**

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

**19A.8.4.12 Lower Drywell Hatches**

An equipment hatch for removal of equipment during maintenance and an air lock for entry of personnel are provided in the lower drywell. These access openings are sealed under normal plant operation but may be opened when the plant is shut down. Closure of both hatches is required for the shutdown Loss-of-Coolant Accident (LOCA) below top of active fuel (TAF) initiators during MODES 5 and 6. Due to the low frequency of occurrence, this function is not risk-significant and the proposed regulatory oversight is in the Availability Control Manual.

**~~19A.8.4.12–19A.8.4.13 Control Room Habitability – Long-Term Battery Charging Ventilation~~**

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

**~~19A.9 REFERENCES~~**

~~19A-1 — GEEN NEDO 33331, “ESBWR, Availability Controls Manual”~~

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

**Table 19A-2  
 RTNSS Systems**

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

**Table 19A-2  
 RTNSS Systems**

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

<sup>1</sup> Note: LRO = Low Regulatory Oversight, HRO = High Regulatory Oversight

TABLE OF CONTENTS / REVISION SUMMARY

**19A.9 AVAILABILITY CONTROLS MANUAL**

USE AND APPLICATION

1.1 Definitions.....  
1.2 Logical Connectors.....  
1.3 Completion Times .....  
1.4 Frequency .....

2.0 Not Used

3.0 LIMITING CONDITION FOR OPERATION (LCO) APPLICABILITY.....  
3.0 SURVEILLANCE REQUIREMENT (SR) APPLICABILITY.....

3.1 Not Used

3.2 Not Used

3.3 INSTRUMENTATION

3.3.1 Alternate Rod Insertion (ARI) .....  
3.3.2 Anticipated Transient Without Scram (ATWS) / Standby Liquid Control (SLC)  
System Actuation.....  
3.3.3 Feedwater Runback (FWRB) .....  
3.3.4 Post Accident Monitoring (PAM) Instrumentation.....

3.4 Not Used

3.5 EMERGENCY CORE COOLING SYSTEMS (ECCS)

3.5.1 Gravity-Driven Cooling System (GDCCS) Deluge Function .....

3.6 CONTAINMENT SYSTEMS

3.6.1 Containment Oxygen  
3.6.2 Lower Drywell Hatches.....

3.7 PLANT SYSTEMS

3.7.1 Emergency Makeup Water .....  
3.7.2 Fuel and Auxiliary Pools Cooling System (FAPCS) .....  
3.7.3 Spent Fuel pool (SFP) Water Level.....

3.8 ELECTRICAL POWER SYSTEMS

3.8.1 Standby Diesel Generators .....  
3.8.2 Control Room Habitability Area (CRHA) Heating, Ventilation, and  
Air Conditioning (HVAC) Subsystem (CRHAVS) Portable  
Generator .....

4.0 DESIGN FEATURES

4.1 Basemat-Internal Melt Arrest and Coolability (BiMAC) Device .....

ACM 1.0 USE AND APPLICATION

ACM 1.1 Definitions

---

---

- NOTES -

1. Definitions are defined in Section 1.1 of the Technical Specifications (TS) and are applicable throughout the Availability Controls Manual (ACM) and ACM Bases. Only definitions specific to the ACM will be defined in this section.
2. The defined terms of this section and the TS appear in capitalized type and are applicable throughout the ACM and the ACM Bases.
3. When a term is defined in both the TS and the ACM, the ACM definition takes precedence within the ACM and the ACM Bases.

---

---

<u>Term</u>	<u>Definition</u>
ACTIONS	ACTIONS shall be that part of an Availability Control that prescribes Required Actions to be taken under designated Conditions within specified Completion Times.
AVAILABLE— AVAILABILITY	A system, subsystem, train, division, component, or device shall be AVAILABLE or have AVAILABILITY when it is capable of performing its specified risk informed function(s) and when all necessary attendant instrumentation, controls, normal or emergency electrical power, cooling and seal water, lubrication, and other auxiliary equipment that are required for the system, subsystem, train, division, component, or device to perform its specified risk informed function(s) are also capable of performing their related support function(s).

---

---

ACM 1.0 USE AND APPLICATION

ACM 1.2 Logical Connectors

---

Logical Connectors are discussed in Section 1.2 of the Technical Specifications and are applicable throughout the Availability Controls Manual and Bases.

---

ACM 1.0 USE AND APPLICATION

ACM 1.3 Completion Times

---

Completion Times are discussed in Section 1.3 of the Technical Specifications and are applicable throughout the Availability Controls Manual and Bases.

---

ACM 1.0 USE AND APPLICATION

ACM 1.4 Frequency

---

---

Frequency is discussed in Section 1.4 of the Technical Specifications and is applicable throughout the Availability Controls Manual and Bases.

---

---

ACM 3.0 AVAILABILITY CONTROL LIMITING CONDITION FOR OPERATION (ACLCO)  
APPLICABILITY

---

ACLCO 3.0.1      ACLCOs shall be met during the MODES or other specified conditions in the Applicability, except as provided in ACLCO 3.0.2.

---

ACLCO 3.0.2      Upon discovery of a failure to meet an ACLCO, the Required Actions of the associated Conditions shall be met, except as provided in ACLCO 3.0.5 and ACLCO 3.0.6.

If the ACLCO is met or is no longer applicable prior to expiration of the specified Completion Time(s), completion of the Required Action(s) is not required, unless otherwise stated.

---

ACLCO 3.0.3      When an ACLCO is not met and the associated ACTIONS are not met, an associated ACTION is not provided, or if directed by the associated ACTIONS, action shall be initiated to:

- a.    Restore compliance with the ACLCO or associated ACTIONS; and

-----  
- NOTE -

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

- b.    Enter the circumstances into the Corrective Action Program.

Exceptions to this ACLCO are stated in the individual ACLCOs.

---

ACLCO 3.0.4      When an ACLCO is not met, entry into a MODE or other specified condition in the Applicability shall only be made:

- a.    When the associated ACTIONS to be entered permit continued operation in the MODE or other specified condition in the Applicability for an unlimited period of time;
- b.    After performance of a risk assessment addressing unavailable systems and components, consideration of the results, determination of the acceptability of entering the MODE or other specified condition in the Applicability, and establishment of risk management actions, if appropriate; exceptions to this ACLCO are stated in the individual ACLCOs; or

ACLCO Applicability

---

ACLCO 3.0.4 (continued)

- c. When an allowance is stated in the individual value, parameter, or other ACLCO.

This ACLCO shall not prevent changes in MODES or other specified conditions in the Applicability that are required to comply with TS or ACM ACTIONS or that are part of a shutdown of the unit.

---

ACLCO 3.0.5      Equipment removed from service or declared unavailable to comply with ACTIONS may be returned to service under administrative control solely to perform testing required to demonstrate its AVAILABILITY or the AVAILABILITY of other equipment. This is an exception to ACLCO 3.0.2 for the system returned to service under administrative control to perform the testing required to demonstrate AVAILABILITY.

---

ACLCO 3.0.6      When a supported system ACLCO is not met solely due to a support system ACLCO not being met, the Conditions and Required Actions associated with this supported system are not required to be entered. Only the support system ACLCO ACTIONS are required to be entered. This is an exception to ACLCO 3.0.2 for the supported system. In this event, a risk evaluation shall be performed in accordance with the Maintenance Rule Program. If an unacceptable risk is determined to exist, the appropriate Conditions and Required Actions of the ACLCO in which the loss of risk mitigation exists are required to be entered.

When a support system's Required Action directs a supported system to be declared unavailable or directs entry in Conditions and Required Actions for a supported system, the applicable Conditions and Required Actions shall be entered in accordance with ACLCO 3.0.2.

---

---

ACM 3.0 AVAILABILITY CONTROL SURVEILLANCE REQUIREMENT (ACSR)  
APPLICABILITY

---

ACSR 3.0.1            ACSRs shall be met during the MODES or other specified conditions in the Applicability for individual ACLCOs, unless otherwise stated in the ACSR. Failure to meet an ACSR, whether such failure is experienced during the performance of the ACSR or between performances of the ACSR, shall be failure to meet the ACLCO. Failure to perform an ACSR within the specified Frequency shall be failure to meet the ACLCO except as provided in ACSR 3.0.3. ACSRs do not have to be performed on unavailable equipment or variables outside specified limits.

---

ACSR 3.0.2            The specified Frequency for each ACSR is met if the ACSR is performed within 1.25 times the interval specified in the Frequency, as measured from the previous performance or as measured from the time a specified condition of the Frequency is met.

For Frequencies specified as “once,” the above interval extension does not apply.

If a Completion Time requires periodic performance on a “once per . . .” basis, the above Frequency extension applies to each performance after the initial performance.

Exceptions to this ACSR are stated in the individual ACSRs.

---

ACSR 3.0.3            If it is discovered that an ACSR was not performed within its specified Frequency, then compliance with the requirement to declare the ACLCO not met may be delayed, from the time of discovery, up to 24 hours or up to the limit of the specified Frequency, whichever is greater. This delay period is permitted to allow performance of the ACSR. A risk evaluation shall be performed for any ACSR delayed greater than 24 hours and the risk impact shall be managed.

If the ACSR is not performed within the delay period, the ACLCO must immediately be declared not met, and the applicable Condition(s) must be entered.

When the ACSR is performed within the delay period and the ACSR is not met, the ACLCO must immediately be declared not met, and the applicable Conditions must be entered.

---

ACSR Applicability

---

ACSR 3.0.4      Entry into a MODE or other specified condition in the Applicability of an ACLCO shall only be made when the associated ACSRs have been met within their Specified Frequency, except as provided by ACSR 3.0.3. When an ACLCO is not met due to ACSRs not having been met, entry into a MODE or other specified condition in the Applicability shall only be made in accordance with ACLCO 3.0.4.

This provision shall not prevent entry into MODES or other specified conditions in the Applicability that are required to comply with TS or ACM ACTIONS or that are part of a shutdown of the unit.

---

ACM B 3.0 AVAILABILITY CONTROL LIMITING CONDITION FOR OPERATION (ACLCO)  
APPLICABILITY

BASES

---

ACLCOs                      ACLCO 3.0.1 through ACLCO 3.0.5 establish the general requirements applicable to all ACLCOs in Sections 3.1 through 3.8 and apply at all times, unless otherwise stated.

---

ACLCO 3.0.1                ACLCO 3.0.1 establishes the Applicability statement within each individual Requirement as the requirement for when the ACLCO is required to be met (i.e., when the unit is in the MODES or other specified conditions of the Applicability statement of each Control).

---

ACLCO 3.0.2                ACLCO 3.0.2 establishes that upon discovery of a failure to meet an ACLCO, the associated ACTIONS shall be met. The Completion Time of each Required Action for an ACTIONS Condition is applicable from the point in time that an ACTIONS Condition is entered. The Required Actions establish those remedial measures that must be taken within specified Completion Times when the requirements of an ACLCO are not met. This Requirement establishes that:

- a. Completion of the Required Actions within the specified Completion Times constitute compliance with a Control; and
- b. Completion of the Required Actions is not required when an ACLCO is met within the specified Completion Time, unless otherwise specified.

There are two basic types of Required Actions. The first type of Required Action specifies a time limit in which the ACLCO must be met. This time limit is the Completion Time to restore an unavailable system or component to AVAILABLE status or to restore variables to within specified limits. If this type of Required Action is not completed within the specified Completion Time, remedial actions to document the failure to comply with the Availability Controls Manual (ACM) requirements are required. (Whether stated as a Required Action or not, correction of the entered Condition is an action that may always be considered upon entering ACTIONS.) The second type of Required Action specifies the remedial measures that permit continued operation of the unit that is not further restricted by the Completion Time. In this case, compliance with the Required Actions provides an acceptable justification for continued operation.

BASES

---

ACLCO 3.0.2 (continued)

Completing the Required Actions is not required when an ACLCO is met or is no longer applicable, unless otherwise stated in the individual Control.

The nature of some Required Actions of some Conditions necessitates that, once the Condition is entered, the Required Actions must be completed even though the associated Conditions no longer exist. The individual ACLCO ACTIONS specify the Required Actions where this is the case.

The Completion Times of the Required Actions are also applicable when a system or component is removed from service intentionally. The reasons for intentionally relying on the ACTIONS include, but are not limited to, performance of ACSRs, preventive maintenance, corrective maintenance, or investigation of operational problems. Entering ACTIONS for these reasons must be done in a manner that does not compromise safety. Individual Controls may specify a time limit for performing an ACSR when equipment is removed from service or bypassed for testing. In this case, the Completion Times of the Required Actions are applicable when this time limit expires, if the equipment remains removed from service or bypassed.

When a change in MODE or other specified condition is required to comply with Required Actions, the unit may enter a MODE or other specified condition in which another Control becomes applicable. In this case, the Completion Times of the associated Required Actions would apply from the point in time that the new Control becomes applicable and the ACTIONS Condition(s) are entered.

---

ACLCO 3.0.3

ACLCO 3.0.3 establishes the actions that must be implemented when an ACLCO is not met and:

- a. An associated Required Action and Completion Time is not met and no other Condition applies; or
- b. The condition of the unit is not specifically addressed by the associated ACTIONS. This means that no combination of Conditions stated in the ACTIONS can be made that exactly corresponds to the actual condition of the unit. Sometimes, possible combinations of Conditions are such that entering ACLCO 3.0.3 is warranted; in such cases, the ACTIONS specifically state a

BASES

---

ACLCO 3.0.3 (continued)

Condition corresponding to such combinations and also that ACLCO 3.0.3 be entered immediately.

This Requirement requires: a) an Action to initiate efforts to restore compliance with the ACLCO or associated ACTIONS, and b) an Action that requires entering the circumstances into the Corrective Action Program (CAP). These actions ensure that the appropriate resources will continue to be focused on restoring compliance with the ACLCO or associated ACTIONS and that the circumstances concerning failure to comply with the Availability Controls Manual (ACM) requirements will be reviewed. This review will be conducted in accordance with the procedural guidance for CAP notifications.

Exceptions to ACLCO 3.0.3 are addressed in the individual Requirements.

---

ACLCO 3.0.4

ACLCO 3.0.4 establishes limitations on changes in MODES or other specified conditions in the Applicability when an ACLCO is not met. It allows placing the unit in a MODE or other specified condition stated in that Applicability (i.e., the Applicability desired to be entered) when unit conditions are such that the requirements of the ACLCO would not be met, in accordance with ACLCO 3.0.4.a, ACLCO 3.0.4.b, or ACLCO 3.0.4.c.

ACLCO 3.0.4.a allows entry into a MODE or other specified condition in the Applicability with the ACLCO not met when the associated ACTIONS to be entered permit continued operation in the MODE or other specified condition in the Applicability for an unlimited period of time. Compliance with Required Actions that permit continued operation of the unit for an unlimited period of time in a MODE or other specified condition provides an acceptable level of safety for continued operation. This is without regard to the status of the unit before or after the MODE change. Therefore, in such cases, entry into a MODE or other specified condition in the Applicability may be made in accordance with the provisions of the Required Actions.

ACLCO 3.0.4.b allows entry into a MODE or other specified condition in the Applicability with the ACLCO not met after performance of a risk assessment addressing unavailable systems and components, consideration of the results, determination of the acceptability of entering the MODE or other specified condition in the Applicability, and establishment of risk management actions, if appropriate.

## BASES

---

### ACLCO 3.0.4 (continued)

The risk assessment may use quantitative, qualitative, or blended approaches, and the risk assessment will be conducted using the plant program, procedures, and criteria in place to implement 10 CFR 50.65(a)(4), which requires that risk impacts of maintenance activities be assessed and managed. The risk assessment, for the purposes of ACLCO 3.0.4.b, must take into account all inoperable Technical Specification equipment regardless of whether the equipment is included in the normal 10 CFR 50.65(a)(4) risk assessment scope. The risk assessments will be conducted using the procedures and guidance endorsed by Regulatory Guide 1.182, "Assessing and Managing Risk Before Maintenance Activities at Nuclear Power Plants." Regulatory Guide 1.182 endorses the guidance in Section 11 of NUMARC 93-01, "Industry Guideline for Monitoring the Effectiveness of Maintenance at Nuclear Power Plants." These documents address general guidance for conduct of the risk assessment, quantitative and qualitative guidelines for establishing risk management actions, and example risk management actions. These include actions to plan and conduct other activities in a manner that controls overall risk, actions to increase risk awareness by shift and management personnel, actions to reduce the duration of the condition, actions to minimize the magnitude of risk increases (establishment of backup success paths or compensatory measures), and a determination that the proposed MODE change is acceptable. Consideration should also be given to the probability of completing restoration such that the requirements of the ACLCO would be met prior to the expiration of ACTIONS Completion Times that would require exiting the Applicability.

ACLCO 3.0.4.b may be used with single or multiple systems and components unavailable. NUMARC 93-01 provides guidance relative to consideration of simultaneous unavailability of multiple systems and components.

The results of the risk assessment shall be considered in determining the acceptability of entering the MODE or other specified condition in the Applicability, and any corresponding risk management actions. The ACLCO 3.0.4.b risk assessments do not have to be documented.

The ACLCOs allow continued operation with equipment unavailable in MODE 1 for the duration of the Completion Time. Since this is allowable, and since in general the risk impact in that particular MODE bounds the risk of transitioning into and through the applicable MODES or other specified conditions in the Applicability of the ACLCO, the use of the

## BASES

---

### ACLCO 3.0.4 (continued)

ACLCO 3.0.4.b allowance should be generally acceptable, as long as the risk is assessed and managed as stated above.

ACLCO 3.0.4.c allows entry into a MODE or other specified condition in the Applicability with the ACLCO not met based on a Note in the Control which states ACLCO 3.0.4.c is applicable. These specific allowances permit entry into MODES or other specified conditions in the Applicability when the associated ACTIONS to be entered do not provide for continued operation for an unlimited period of time and a risk assessment has not been performed. This allowance may apply to all the ACTIONS or to a specific Required Action of a Control. The risk assessments performed to justify the use of ACLCO 3.0.4.b usually only consider systems and components. For this reason, ACLCO 3.0.4.c is typically applied to Controls which describe values and parameters.

The provisions of this Control should not be interpreted as endorsing the failure to exercise the good practice of restoring systems or components to AVAILABLE status before entering an associated MODE or other specified condition in the Applicability.

---

### ACLCO 3.0.5

ACLCO 3.0.5 establishes the allowance for restoring equipment to service under administrative controls when it has been removed from service or declared unavailable to comply with ACTIONS. The sole purpose of this Control is to provide an exception to ACLCO 3.0.2 (e.g., to not comply with the applicable Required Action(s)) to allow the performance of required testing to demonstrate:

- a. The AVAILABILITY of the equipment being returned to service; or
- b. The AVAILABILITY of other equipment.

The administrative controls ensure the time the equipment is returned to service in conflict with the requirements of the ACTIONS is limited to the time absolutely necessary to perform the required testing to demonstrate AVAILABILITY. This Control does not provide time to perform any other preventive or corrective maintenance.

---

BASES

---

ACLCO 3.0.6

ACLCO 3.0.6 establishes an exception to ACLCO 3.0.2 for supported systems that have a support system ACLCO specified in the ACM. This exception is provided because ACLCO 3.0.2 would require that the Conditions and Required Actions of the associated unavailable supported system ACLCO be entered solely due to the unavailability of the support system. This exception is justified because the actions that are required to ensure the plant risk is appropriately controlled are specified in the support system ACLCO Required Actions. These Required Actions may include entering the supported system Conditions and Required Actions or may specify other Required Actions.

When a support system is unavailable and there is an ACLCO specified for it in the ACM, the supported system(s) are required to be declared unavailable if determined to be unavailable as a result of the support system unavailability. However, it is not necessary to enter into the supported system Conditions and Required Actions unless directed to do so by the support system Required Actions. The potential confusion and inconsistency of requirements related to the entry into multiple support and supported system ACLCO Conditions and Required Actions are eliminated by providing all the actions that are necessary to ensure the plant is maintained in a safe condition in the support system Required Actions.

However, there are instances where a support system Required Action may either direct a supported system to be declared unavailable or direct entry into Conditions and Required Actions for the supported system. This may occur immediately or after some specified delay to perform some other Required Action. Regardless of whether it is immediate or after some delay, when a support system Required Action directs a supported system to be declared unavailable or directs entry into Conditions and Required Actions for a supported system, the applicable Conditions and Required Actions shall be entered in accordance with ACLCO 3.0.2.

The Maintenance Rule Program ensures unacceptable risk is detected and appropriate actions are taken. Upon entry into ACLCO 3.0.6, an evaluation shall be made to determine if unacceptable risk exists. Additionally, other limitations, remedial actions, or compensatory actions may be identified as a result of the support system unavailability and corresponding exception to entering supported system Conditions and Required Actions. The Maintenance Rule Program implements the requirements of ACLCO 3.0.6.

---

ACM B 3.0 AVAILABILITY CONTROL SURVEILLANCE REQUIREMENT (ACSR)  
APPLICABILITY

BASES

---

ACSRs                      ACSR 3.0.1 through ACSR 3.0.4 establish the general requirements applicable to all ACSR in Sections 3.1 through 3.10 and apply at all times, unless otherwise stated.

---

ACSR 3.0.1                ACSR 3.0.1 establishes the requirement that ACSR must be met during the MODES or other specified conditions in the Applicability for which the requirements of the ACLCOs apply, unless otherwise specified in the individual ACSR. This ACSR is to ensure that ACSR are performed to verify the AVAILABILITY of systems and components, and that variables are within specified limits. Failure to meet an ACSR within the specified Frequency, in accordance with ACSR 3.0.2, constitutes a failure to meet an ACLCO.

Systems and components are assumed to be AVAILABLE when the associated ACSR have been met. Nothing in this ACSR, however, is to be construed as implying that systems or components are AVAILABLE when:

- a.    The systems or components are known to be unavailable, although still meeting the ACSR; or
- b.    The requirements of the ACSR(s) are known to be not met between required ACSR performances.

ACSRs do not have to be performed when the unit is in a MODE or other specified condition for which the requirements of the associated ACLCO are not applicable, unless otherwise specified.

Unplanned events may satisfy the requirements (including applicable acceptance criteria) for a given ACSR. In this case, the unplanned event may be credited as fulfilling the performance of the ACSR. ACSR, including ACSR invoked by Required Actions, do not have to be performed on unavailable equipment because the ACTIONS define the remedial measures that apply. ACSR have to be met and performed in accordance with ACSR 3.0.2, prior to returning equipment to AVAILABLE status.

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

BASES

---

ACSR 3.0.1 (continued)

applicable ACSRs are not failed and their most recent performance is in accordance with ACSR 3.0.2. Post maintenance testing may not be possible in the current MODE or other specified conditions in the Applicability due to the necessary unit parameters not having been established. In these situations, the equipment may be considered AVAILABLE provided testing has been satisfactorily completed to the extent possible and the equipment is not otherwise believed to be incapable of performing its function. This will allow operation to proceed to a MODE or other specified condition where other necessary post maintenance testing can be completed.

---

ACSR 3.0.2

ACSR 3.0.2 establishes the requirements for meeting the specified Frequency for ACSRs and any Required Action with a Completion Time that requires the periodic performance of the Required Action on a "once per . . ." interval.

ACSR 3.0.2 permits a 25% extension of the interval specified in the Frequency. This extension facilitates ACSR scheduling and considers plant operating conditions that may not be suitable for conducting the ACSR (e.g., transient conditions or other ongoing ACSR or maintenance activities).

The 25% extension does not significantly degrade the reliability that results from performing the ACSR at its specified Frequency. This is based on the recognition that the most probable result of any particular ACSR being performed is the verification of conformance with the ACSR. The exception to ACSR 3.0.2 are those ACSRs for which the 25% extension of the interval specified in the Frequency does not apply. These exceptions are stated in the individual ACSRs. The requirements of regulations take precedence over the ACM. The ACM cannot in and of itself extend a test interval specified in the regulations.

As stated in ACSR 3.0.2, the 25% extension also does not apply to the initial portion of a periodic Completion Time that requires performance on a "once per . . ." basis. The 25% extension applies to each performance after the initial performance. The initial performance of the Required Action, whether it is a particular ACSR or some other remedial action, is considered a single action with a single Completion Time. One reason for not allowing the 25% extension to this Completion Time is that such an action usually verifies that no loss of function has occurred by checking

BASES

---

ACSR 3.0.2 (continued)

the status of redundant or diverse components or accomplishes the function of the unavailable equipment in an alternative manner.

The provisions of ACSR 3.0.2 are not intended to be used repeatedly merely as an operational convenience to extend ACSR intervals (other than those consistent with refueling intervals) or periodic Completion Time intervals beyond those specified.

---

ACSR 3.0.3

ACSR 3.0.3 establishes the flexibility to defer declaring affected equipment unavailable or an affected variable outside the specified limits when an ACSR has not been completed within the specified Frequency. A delay period of up to 24 hours or up to the limit of the specified Frequency, whichever is greater, applies from the point in time it is discovered that the ACSR has not been performed in accordance with ACSR 3.0.2, and not at the time that the specified frequency was not met.

This delay period provides adequate time to complete ACSRs that have been missed. This delay period permits the completion of an ACSR before complying with Required Actions or other remedial measures that might preclude completion of the ACSR.

The basis for this delay period includes consideration of unit conditions, adequate planning, availability of personnel, the time required to perform the ACSR, the safety significance of the delay in completing the required ACSR, and the recognition that the most probable result of any particular ACSR being performed is the verification of conformance with the requirements. When an ACSR with a Frequency based not on time intervals, but upon specified unit conditions or operational situations (e.g., prior to entering MODE 1 after each fueling loading), is discovered not to have been performed when specified, ACSR 3.0.3 allows the full delay period of up to the specified frequency to perform the ACSR. However, since there is not a time interval specified, the missed ACSR should be performed at the first reasonable opportunity.

ACSR 3.0.3 provides a time limit for, and allowances for, the performance of ACSRs that become applicable as a consequence of MODE changes imposed by Required Actions.

Failure to comply with specified Frequencies for ACSRs is expected to be an infrequent occurrence. Use of the delay period established by ACSR 3.0.3 is a flexibility which is not intended to be used as an

BASES

---

ACSR 3.0.3 (continued)

operational convenience to extend ACSR intervals. While up to 24 hours or the limit of the specified Frequency is provided to perform the missed ACSR, it is expected that the missed ACSR will be performed at the first reasonable opportunity. The determination of the first reasonable opportunity should include consideration of the impact on unit risk (from delaying the ACSR as well as any unit configuration changes required or shutting the unit down to perform the ACSR) and impact on any analysis assumptions, in addition to unit conditions, planning, availability of personnel, and the time required to perform the ACSR. This risk impact should be managed through the program in place to implement 10 CFR 50.65(a)(4) and its implementation guidance Regulatory Guide 1.182, "Assessing and Managing Risk Before Maintenance Activities at Nuclear Power Plants." This Regulatory Guide addresses consideration of temporary and aggregate risk impacts, determination of risk management action thresholds, and risk management action up to and including plant shutdown. The missed ACSR should be treated as an emergent condition as discussed in the Regulatory Guide. The risk evaluation may use quantitative, qualitative, or blended methods. The degree of depth and rigor of the evaluation should be commensurate with the importance of the component. Missed ACSRs for important components should be analyzed quantitatively. If the results of the risk evaluation determine the risk increase is significant this evaluation should be used to determine the safest course of action. All missed ACSRs will be placed in the licensee Corrective Action Program.

If an ACSR is not completed within the allowed delay period, the equipment is considered unavailable or the variable is considered outside the specified limits and the Completion Times of the Required Actions for the applicable ACLCO Conditions begin immediately upon expiration of the delay period. If an ACSR is failed within the delay period, then the equipment is unavailable, or the variable is outside the specified limits and the Completion Times of the Required Actions for the applicable ACLCO Conditions begin immediately upon the failure of the ACSR.

Completion of the ACSR within the delay period allowed by this ACSR, or within the Completion Time of the ACTIONS, restores compliance with ACSR 3.0.1.

---

BASES

---

ACSR 3.0.4            ACSR 3.0.4 establishes the requirement that all applicable ACSRs must be met before entry into a MODE or other specified condition in the Applicability.

This ACSR ensures that system and component AVAILABILITY requirements and variable limits are met before entry into MODES or other specified conditions in the Applicability for which these system and components ensure safe operation of the unit. The provisions of this ACSR should not be interpreted as endorsing the failure to exercise the good practice of restoring systems or components to AVAILABLE status before entering an associated MODE or other specified condition in the Applicability.

A provision is included to allow entry into a MODE or other specified Condition in the Applicability when an ACLCO is not met due to an ACSR not being met in accordance with ACLCO 3.0.4. However, in certain circumstances, failing to meet an ACSR will not result in ACSR 3.0.4 restricting a MODE change or other specified condition change. When a system, subsystem, division, component, device, or variable is unavailable or outside its specified limits, the associated ACSR(s) are not required to be performed, per ACSR 3.0.1, which states that ACSRs do not have to be performed on unavailable equipment. When equipment is unavailable, ACSR 3.0.4 does not apply to the associated ACSR(s) since the requirement for the ACSR(s) to be performed is removed. Therefore, failing to perform the ACSRs within the specified Frequency does not result in an ACSR 3.0.4 restriction to changing MODES or other specified conditions of the Applicability. However, since the ACLCO is not met in this instance, ACLCO 3.0.4 will govern any restrictions that may (or may not) apply to MODE or other specified condition changes. ACSRS 3.0.4 does not restrict changing MODES or other specified conditions of the Applicability when an ACSR has not been performed within the specified Frequency, provided the requirement to declare the ACLCO not met has been delayed in accordance with ACSR 3.0.3.

The provisions of ACSR 3.0.4 shall not prevent changes in MODES or other specified conditions in the Applicability that are required to comply with ACTIONS. In addition, the provisions of ACSR 3.0.4 shall not prevent changes in MODES or other specified conditions in the Applicability that result from any unit shutdown. In this context, a unit shutdown is defined as a change in MODE or other specified condition in the Applicability associated with transitioning from MODE 1 to MODE 2, MODE 2 to MODE 3, and MODE 3 to MODE 4.

BASES

---

ACSR 3.0.4 (continued)

The precise requirements for performance of ACSRs are specified such that exceptions to ACSR 3.0.4 are not necessary. The specific time frames and conditions necessary for meeting the ACSRs are specified in the Frequency, in the ACSR, or both. This allows performance of ACSRs when the prerequisite condition(s) specified in an ACSR procedure require entry into the MODE or other specified condition in the Applicability of the associated ACLCO prior to the performance or completion of an ACSR. An ACSR that could not be performed until after entering the ACLCO Applicability would have its Frequency specified such that it is not "due" until the specific conditions needed are met.

Alternately, the ACSR may be stated in the form of a Note as not required (to be met or performed) until a particular event, condition, or time has been reached. Further discussion of the specific formats of ACSR annotation is found in Section 1.4, "Frequency."

---

ACLCO 3.3.1 The ARI function of the air header dump valves in the Control Rod Drive (CRD) System shall be AVAILABLE.

APPLICABILITY: MODES 1 and 2.

**ACTIONS**

CONDITION	REQUIRED ACTION	COMPLETION TIME
A. The ARI function of one or more CRD System air header dump valves unavailable.	A.1 Restore CRD System air header dump valves to AVAILABLE Status.	7 days
B. Required Action and associated Completion Time not met.	B.1 Enter ACLCO 3.0.3.	Immediately

**SURVEILLANCE REQUIREMENTS**

SURVEILLANCE	FREQUENCY
ACSR 3.3.1.1 ----- <p style="text-align: center;"><b>- NOTE -</b>            Only required to be met in MODE 1.</p> -----  MODE 2 Surveillance Requirements of Technical Specification (TS) 3.3.1.4, "Nuclear Monitoring System (NMS) Instrumentation," Table 3.3.1.4-1, for Functions 1.a, 1.b, and 1.c are applicable.	In accordance with applicable SRs

SURVEILLANCE		FREQUENCY
ACSR 3.3.1.2	Verify each CRD System air header dump valve vents on receipt of an actual or simulated actuation signal.	24 months on a STAGGERED TEST BASIS for each solenoid
ACSR 3.3.1.3	Perform LOGIC SYSTEM FUNCTIONAL TEST for each required ARI Function automatic actuation division.	24 months on a STAGGERED TEST BASIS

### ACM B 3.3.1 INSTRUMENTATION

#### AC B 3.3.1 Alternate Rod Insertion (ARI)

##### BASES

---

This Availability Control (AC) addresses AVAILABILITY of the Alternate Rod Insertion (ARI) function of the air header dump valves in the Control Rod Drive (CRD) system. The ARI function of the Control Rod Drive (CRD) system provides an alternate means for actuating hydraulic scram that is diverse and independent from the Reactor Protection System (RPS). The ARI function of the Anticipated Transient Without Scram (ATWS) mitigation logic is implemented as nonsafety-related logic that is processed by the Diverse Protection System (DPS). The DPS generates the signal; to open the ARI (air header dump) valves in the CRD system on any of the following signals: persistent high power with a Selected Control Rod Run-in (SCRRI) command issued; persistent high power following an RPS scram demand; high reactor dome pressure; low reactor vessel water Level 2; or manual operator action. Following receipt of any of these signals, solenoid operated valves on the scram air header actuate to depressurize the header, allowing the Hydraulic Control Unit (HCU) scram valves to open. The control rod drives then insert the control rods hydraulically.

The ARI function is a nonsafety-related function that satisfies the significance criteria for Regulatory Treatment of Non-Safety Systems, and therefore requires regulatory oversight. The short-term availability controls for this function, which are specified as Completion Times, are acceptable to ensure that the availability of this function is consistent with the functional unavailability in the ESBWR PRA. The surveillance requirements also provide an adequate level of support to ensure that component performance is consistent with the functional reliability in the ESBWR PRA.

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

---

ACM 3.3 INSTRUMENTATION

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

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

APPLICABILITY: MODES 1 and 2.

ACTIONS

CONDITION	REQUIRED ACTION	COMPLETION TIME
A. SLC actuation function of the ATWS/SLC logic unavailable.	A.1 Restore SLC actuation function of the ATWS/SLC logic to AVAILABLE status.	7 days
B. Required Action and associated Completion Time not met.	B.1 Enter ACLCO 3.0.3.	Immediately

SURVEILLANCE REQUIREMENTS

SURVEILLANCE	FREQUENCY
ACSR 3.3.2.1 Verify SLC actuation on receipt of an actual or simulated actuation signal.	24 months
ACSR 3.3.2.2 Perform LOGIC SYSTEM FUNCTIONAL TEST for each required SLC actuation function of the ATWS/SLC automatic actuation division.	24 months on a STAGGERED TEST BASIS

## ACM B 3.3 INSTRUMENTATION

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

#### BASES

---

The Standby Liquid Control (SLC) System provides a diverse backup capability for reactor shutdown, independent of normal reactor shutdown with control rods. It also provides makeup water to the reactor pressure vessel (RPV) to mitigate the consequences of a LOCA. Operability of the SLC System, including the squib-actuated valves, is addressed in Technical Specification (TS) 3.1.7, "Standby Liquid Control (SLC) System." Operability of the instrumentation sensors is addressed in TS 3.3.1.1, "Reactor Protection System (RPS) Instrumentation." This Availability Control addresses only the actuation logic associated with the ATWS/SLC actuation of SLC for diverse backup reactor shutdown, and includes isolation of RWCU/SDC on ATWS/SLC initiation.

There is an ATWS logic processor in each of four divisional Reactor Trip and Isolation Function (RTIF) cabinets. The ATWS logic processors are separate and diverse from RPS circuitry. Each ATWS logic processor uses discrete programmable logic devices for ATWS mitigation logic processing. The programmable logic devices provide voting logic, control logic, and time delays for evaluating the plant conditions for automatic initiation of SLC boron injection.

Automatic initiation of the ATWS/SLC occurs on High RPV dome pressure and a Startup Range Neutron Monitor (SRNM) ATWS permissive, or Low RPV water level (L2) and a SRNM ATWS permissive for 3 minutes or greater.

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

The ATWS/SLC actuation function is a nonsafety-related function that satisfies the significance criteria for Regulatory Treatment of Non-Safety Systems, and therefore requires regulatory oversight. The short-term availability controls for this function, which are specified as Completion Times, are acceptable to ensure that the availability of this function is consistent with the functional unavailability in the ESBWR PRA. The surveillance requirements also provide an adequate level of support to ensure that component performance is consistent with the functional reliability in the ESBWR PRA.

---

ACM 3.3 INSTRUMENTATION

AC 3.3.3 Feedwater Runback (FWRB)

ACLCO 3.3.3 The FWRB function shall be AVAILABLE.

APPLICABILITY: MODE 1

ACTIONS

CONDITION	REQUIRED ACTION	COMPLETION TIME
A. FWRB function unavailable.	A.1 Restore FWRB function to AVAILABLE status.	7 days
B. Required Action and associated Completion Time not met.	B.1 Enter ACLCO 3.0.3.	Immediately

SURVEILLANCE REQUIREMENTS

SURVEILLANCE	FREQUENCY
ACSR 3.3.3.1 Verify FWRB function actuation on receipt of an actual or simulated actuation signal.	24 months
ACSR 3.3.3.2 Perform LOGIC SYSTEM FUNCTIONAL TEST for each required FWRB function automatic actuation division.	24 months on a STAGGERED TEST BASIS

## ACM B 3.3 INSTRUMENTATION

### AC B 3.3.3 Feedwater Runback (FWRB)

#### BASES

---

The feedwater runback logic provides a quick power reduction in response to Anticipated Transient Without Scram (ATWS) conditions. The Feedwater Control System (FWCS) initiates a runback of feedwater pump feedwater demand to zero and closes the Low Flow Control Valve (LFCV) and Reactor Water Cleanup/Shutdown Cooling (RWCU/SDC) overboard flow control valve upon receipt of an ATWS trip signal from the Anticipated Transient Without Scram/Standby Liquid Control (ATWS/SLC) logic. Operability of the instrumentation sensors is addressed in TS 3.3.1.1, "Reactor Protection System (RPS) Instrumentation." This Availability Control addresses the ATWS/SLC actuation logic and FWCS components associated with the FWRB function.

There is an ATWS logic processor in each of four divisional Reactor Trip and isolation Function (RTIF) cabinets. The ATWS logic processors are separate and diverse from Reactor Protection System (RPS) circuitry. Each ATWS logic processor uses discrete programmable logic devices for ATWS mitigation logic processing. The programmable logic devices provide voting logic, control logic, and time delays for evaluating the plant conditions for automatic initiation of feedwater runback.

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

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

The FWRB function is a nonsafety-related function that satisfies the significance criteria for Regulatory Treatment of Non-Safety Systems, and therefore requires regulatory oversight. The short-term availability controls for this function, which are specified as Completion Times, are acceptable to ensure that the availability of this function is consistent with the functional unavailability in the ESBWR PRA. The surveillance requirements also provide an adequate level of support to ensure that component performance is consistent with the functional reliability in the ESBWR PRA.

---

ACM 3.3 INSTRUMENTATION

AC 3.3.4 Post Accident Monitoring (PAM) Instrumentation

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

APPLICABILITY: MODES 1 and 2.

ACTIONS

- NOTE -

Separate Condition entry is allowed for each critical safety function.

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

**SURVEILLANCE REQUIREMENTS**

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

## ACM B 3.3 INSTRUMENTATION

### AC B 3.3.4 Post-Accident Monitoring (PAM) Instrumentation

#### BASES

---

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

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

The PAM instrumentation function is a nonsafety-related function that satisfies the significance criteria for Regulatory Treatment of Non-Safety Systems, and therefore requires regulatory oversight. The short-term availability controls for this function, which are specified as Completion Times, are acceptable to ensure that the availability of this function is consistent with the functional unavailability in the ESBWR PRA. The surveillance requirements also provide an adequate level of support to ensure that component performance is consistent with the functional reliability in the ESBWR PRA.

---

ACLCO 3.5.1 Two GDCS Deluge valves shall be AVAILABLE.

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

**ACTIONS**

CONDITION	REQUIRED ACTION	COMPLETION TIME
A. Required GDCS Deluge valves unavailable.	A.1 Restore required GDCS Deluge valves to AVAILABLE Status.	7 days
B. Required Action and associated Completion Time not met.	B.1 Enter ACLCO 3.0.3.	Immediately

**SURVEILLANCE REQUIREMENTS**

SURVEILLANCE	FREQUENCY
ACSR 3.5.1.1 ----- <p style="text-align: center;"><b>- NOTE -</b></p> Not required to be met for one squib firing circuit intermittently bypassed under administrative controls. -----  Verify continuity of required firing circuits in squib-actuated valves.	31 days

SURVEILLANCE		FREQUENCY
ACSR 3.5.1.2	<p>-----</p> <p style="text-align: center;"><b>- NOTE -</b></p> <p>Squib actuation may be excluded.</p> <p>-----</p> <p>Verify required GDCS Deluge valves actuate on an actual or simulated automatic initiation signal.</p>	24 months
ACSR 3.5.1.3	Perform LOGIC SYSTEM FUNCTIONAL TEST for each required GDCS Deluge automatic actuation division.	24 months on a STAGGERED TEST BASIS

## ACM B 3.5 EMERGENCY CORE COOLING SYSTEM (ECCS)

### AC B 3.5.1 Gravity-Driven Cooling System (GDCS) Deluge Function

#### BASES

---

The GDCS deluge function provide a means of flooding the lower drywell region and the Basemat Internal Melt Arrest and Coolability (BiMAC) Device with GDCS pool water in the event of a core melt sequence which causes failure of the lower vessel head and allows molten fuel to reach the lower drywell floor. Deluge line flow is initiated by thermocouples, which sense high lower drywell region basemat temperatures indicative of molten fuel on the lower drywell floor. Logic circuits actuate squib-type valves in the deluge lines upon detection of basemat temperatures exceeding setpoint values, provided another set of dedicated thermocouples also sense the drywell temperature to be higher than a preset value. The pyrotechnic material of the squib charge used in the deluge valve is different than what is used in the other GDCS squib valves to prevent common mode failure.

Only two of the deluge valves, and their associated instrumentation sensors and actuation logics, are required to be AVAILABLE to remove decay heat energy and the energy from zirconium-water reaction and allow for quenching of core debris. Three GDCS pools, located above the wetwell, at an elevation above the reactor core, contain the water that supports all four GDCS trains for the injection and deluge subsystems and is assured by Technical Specification LCO 3.5.2, "GDCS - Operating."

The GDCS deluge function is a nonsafety-related function that satisfies the significance criteria for Regulatory Treatment of Non-Safety Systems, and therefore requires regulatory oversight. The short-term availability controls for this function, which are specified as Completion Times, are acceptable to ensure that the availability of this function is consistent with the functional unavailability in the ESBWR PRA. The surveillance requirements also provide an adequate level of support to ensure that component performance is consistent with the functional reliability in the ESBWR PRA.

---

ACM 3.6 CONTAINMENT SYSTEMS

AC 3.6.1 Containment Oxygen

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

APPLICABILITY: MODE 1.

ACTIONS

- NOTE -

ACLCO 3.0.4.c is applicable.

CONDITION	REQUIRED ACTION	COMPLETION TIME
A. Containment oxygen concentration $\geq$ 4 volume percent.	A.1 Restore containment oxygen concentration to < 4 volume percent.	7 days
B. Required Action and associated Completion Time not met.	B.1 Enter ACLCO 3.0.3.	Immediately

SURVEILLANCE REQUIREMENTS

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

## ACM B 3.6 CONTAINMENT SYSTEMS

### AC B 3.6.1 Containment Oxygen

#### BASES

---

For the Design Basis Accident (DBA), the generation of post accident oxygen would not result in a combustible gas condition and a design basis Loss-of-Coolant Accident (LOCA) does not have to be considered in this regard. However, the basis of the severe accident analysis assumes that the containment is inert. Maintaining containment oxygen within the specified limit provides defense-in-depth for beyond design basis events that could result in combustible gas mixtures that could threaten containment integrity and lead to offsite radiological releases.[CWS121]

Intentional Entry into Condition A and the associated Required Action is permitted during the reactor startup and shutdown process.[CWS122]

The Containment Oxygen function is a nonsafety-related function that satisfies the significance criteria for Regulatory Treatment of Non-Safety Systems, and therefore requires regulatory oversight. The short-term availability controls for this function, which are specified as Completion Times, are acceptable to ensure that the availability of this function is consistent with the functional unavailability in the ESBWR PRA. The surveillance requirements also provide an adequate level of support to ensure that component performance is consistent with the functional reliability in the ESBWR PRA.

---

ACM 3.6 CONTAINMENT SYSTEMS

AC 3.6.2 Lower Drywell Hatches

ACLCO 3.6.2 The lower drywell personnel air lock and lower drywell equipment hatch shall be AVAILABLE for closure.

APPLICABILITY: MODES 5 and 6, during operations with a potential for draining the reactor vessel (OPDRVs).

ACTIONS

CONDITION	REQUIRED ACTION	COMPLETION TIME
A. Required Drywell equipment hatch not AVAILABLE for closure.	A.1 Initiate action to suspend OPDRVs.	Immediately
B. Required Action and associated Completion Time not met.	B.1 Enter ACLCO 3.0.3.	Immediately

SURVEILLANCE REQUIREMENTS

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

## ACM B 3.6 CONTAINMENT SYSTEMS

### AC B 3.6.2 Lower Drywell Hatches

#### BASES

---

An equipment hatch for removal of equipment during maintenance and an air lock for entry of personnel are provided in the lower drywell. These access openings are sealed under normal plant operation but may be opened when the plant is shut down. Closure of both hatches is required for the shutdown Loss-of-Coolant Accident (LOCA) below top of active fuel (TAF) initiators during MODES 5 and 6. These LOCAs involve breaks in the RWCU/SDC drain lines and instrument lines and CRD housing/maintenance activities. Once the event has been detected, personnel must correctly diagnose the situation, make the decision to close the hatches, and manually close the equipment hatch and the personnel air lock. Administrative controls assure trained personnel will be continuously located in the area of the doors and appropriate administrative controls are in place to communicate awareness of potential breaches and effect decisions to secure the hatches.

The lower drywell hatch closure function is a nonsafety-related function that satisfies the significance criteria for Regulatory Treatment of Non-Safety Systems, and therefore requires regulatory oversight. The short-term availability controls for this function, which are specified as Completion Times, are acceptable to ensure that the availability of this function is consistent with the functional unavailability in the ESBWR PRA. The surveillance requirements also provide an adequate level of support to ensure that component performance is consistent with the functional reliability in the ESBWR PRA.

---

ACM 3.7 PLANT SYSTEMS

AC 3.7.1 Emergency Makeup Water

ACLCO 3.7.1 The emergency makeup water Functions listed in Table AC 3.7.1-1 shall be AVAILABLE.

APPLICABILITY: According to Table AC 3.7.1-1.

ACTIONS

CONDITION	REQUIRED ACTION	COMPLETION TIME
A. Required diesel-driven firewater pump unavailable.	A.1 Restore required diesel-driven firewater pump to AVAILABLE status.	7 days
B. Firewater source total volume not within limit.	B.1 Restore firewater source total volume to within limit.	7 days
C. One or more emergency makeup water Function(s) unavailable.	C.1 ----- <p style="text-align: center;"><b>- NOTE -</b></p> Separate Condition entry is allowed for each emergency makeup water Function. -----  Restore emergency makeup water Function(s) to AVAILABLE status.	31 days
D. Required Action and associated Completion Time not met.	D.1 Enter ACLCO 3.0.3.	Immediately

**SURVEILLANCE REQUIREMENTS**

SURVEILLANCE		FREQUENCY
ACSR 3.7.1.1	Verify firewater source total volume $\geq 3900 \text{ m}^3$ ( $1.03 \times 10^6$ gallons).	31 days
ACSR 3.7.1.2	Verify that each manual, power-operated, or automatic valve in the flow path that is not locked, sealed, or otherwise secured in its correct position is in the correct position or can be aligned to the correct position.	31 days
ACSR 3.7.1.3	Verify required diesel-driven firewater pump starts on a manual start signal and operates for $\geq 15$ minutes.	92 days

Table AC 3.3.7-1 (page 1 of 1)  
Emergency Makeup Water Sources

FUNCTION	APPLICABLE MODES OR OTHER SPECIFIED CONDITIONS
1. Isolation Condenser / Passive Containment Cooling (IC/PCC) Pools Makeup Water – Emergency Makeup	1,2
2. Spent Fuel Pool (SFP) - Emergency Makeup Water	When spent fuel assemblies are stored in the SFP

## ACM B 3.7 PLANT SYSTEMS

### AC B 3.7.1 Emergency Makeup Water

#### BASES

---

The Fire Protection Water Supply System can function in a backup capacity to provide additional water during the post accident recovery period to provide makeup to the Isolation Condenser / Passive Containment Cooling (IC/PCC) pools to extend the safe shutdown state from 72 hours through 7 days. Post 72-hour inventory makeup is provided via safety-related connections to the Fire Protection System and to offsite water sources. The required volume from 72 hours through 7 days is approximately 3,900 m<sup>3</sup> (138,000 ft<sup>3</sup>), and the maximum required delivery rate is approximately 46 m<sup>3</sup>/hr (200 gpm) at 72 hours.

During a loss of the Fuel and Auxiliary Pools Cooling System (FAPCS) cooling trains, the cooling to the Spent Fuel Pool (SFP) is accomplished by allowing the water to heat and boil off. Sufficient pool capacity exists for pool boiling to continue for at least 72 hours post-accident, at which point emergency makeup water can be provided through safety-related connections to the Fire Protection System. The required volume from 72 hours through 7 days is approximately 1921 m<sup>3</sup> (67,840 ft<sup>3</sup>).

In conjunction with the diesel-driven pump, the dedicated connections for FPS makeup include 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 Fuel and Auxiliary Pools Cooling System (FAPCS). Water is pumped from the firewater storage tanks by the diesel-driven firewater pump in the FPE to the desired flow path. The two firewater storage tanks are required to contain a total volume of  $\geq 3900 \text{ m}^3$  ( $1.03 \times 10^6$  gallons) of water to ensure a sufficient quantity of emergency makeup is available.

The emergency makeup water functions are nonsafety-related functions that satisfy the significance criteria for Regulatory Treatment of Non-Safety Systems, and therefore require regulatory oversight. The short-term availability controls for these functions, which are specified as Completion Times, are acceptable to ensure that the availability of these functions is consistent with the functional unavailability in the ESBWR PRA. The surveillance requirements also provide an adequate level of support to ensure that component performance is consistent with the functional reliability in the ESBWR PRA.

---

ACM 3.7 PLANT SYSTEMS

AC 3.7.2 Fuel and Auxiliary Pools Cooling System (FAPCS)

ACLCO 3.7.2 One Fuel and Auxiliary Pools Cooling System (FAPCS) train shall be AVAILABLE.

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

ACTIONS

CONDITION	REQUIRED ACTION	COMPLETION TIME
A. Required FAPCS train unavailable.	A.1 Restore required FAPCS train to AVAILABLE status.	7 days
B. Required Action and associated Completion Time not met.	B.1 Enter ACLCO 3.0.3.	Immediately

SURVEILLANCE REQUIREMENTS

SURVEILLANCE	FREQUENCY
ACSR 3.7.2.1 Verify that each manual, power-operated, or automatic valve in the flow path that is not locked, sealed, or otherwise secured in its correct position is in the correct position or can be aligned to the correct position.	31 days

## ACM B 3.7 PLANT SYSTEMS

### AC B 3.7.2 Fuel and Auxiliary Pools Cooling System (FAPCS)

#### BASES

---

FAPCS is designed to provide the accident recovery functions of suppression pool cooling and low pressure coolant injection (LPCI) of suppression pool water into the reactor pressure vessel (RPV), in addition to its normal spent fuel cooling function. This AC addresses the suppression pool cooling and LPCI functions of the FAPCS.

In the LPCI mode, the required FAPCS pump takes suction from the suppression pool and pumps it into the RPV via Reactor Water Cleanup/Shutdown Cooling (RWCU/SDC) loop B and then Feedwater loop A. In the suppression pool cooling mode, water is drawn from the suppression pool, cooled by the FAPCS, and returned to the suppression pool. The suppression pool cooling mode may be manually initiated following an accident.

The FAPCS function is a nonsafety-related function that satisfies the significance criteria for Regulatory Treatment of Non-Safety Systems, and therefore requires regulatory oversight. The short-term availability controls for this function, which are specified as Completion Times, are acceptable to ensure that the availability of this function is consistent with the functional unavailability in the ESBWR PRA. The surveillance requirements also provide an adequate level of support to ensure that component performance is consistent with the functional reliability in the ESBWR PRA.

---

ACM 3.7 PLANT SYSTEMS

AC 3.7.3 Spent Fuel Pool (SFP) Water Level

ACLCO 3.7.3 The SFP water level shall be  $\geq 8.5$  m (27.9 ft) over the top of irradiated fuel assemblies seated in the spent fuel storage pool.

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

ACTIONS

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

SURVEILLANCE REQUIREMENTS

SURVEILLANCE	FREQUENCY
ACSR 3.7.3.1 Verify SFP water level within limits.	31 days

ACM B 3.7 PLANT SYSTEMS

AC B 3.7.3 Spent Fuel Pool (SFP) Water Level

---

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

Sufficient reserve capacity is maintained on-site to extend the safe shutdown state from 72 hours through 7 days. Post 72-hour inventory makeup is provided via safety-related connections to the Fire Protection System and to offsite water sources.

This function is a nonsafety-related function that satisfies the significance criteria for Regulatory Treatment of Non-Safety Systems, and therefore requires regulatory oversight. The short-term availability controls for this function, which are specified as Completion Times, are acceptable to ensure that the availability of this function is consistent with the functional unavailability in the ESBWR PRA. The surveillance requirements also provide an adequate level of support to ensure that component performance is consistent with the functional reliability in the ESBWR PRA.

---

ACM 3.8 ELECTRICAL POWER SYSTEMS

AC 3.8.1 Standby Diesel Generators

ACLCO 3.8.1 One standby diesel generator shall be AVAILABLE.

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

ACTIONS

CONDITION	REQUIRED ACTION	COMPLETION TIME
A. Required standby diesel generator unavailable.	A.1 Restore required standby diesel generator to AVAILABLE status.	14 days
B. Required Action and associated Completion Time not met.	B.1 Enter ACLCO 3.0.3.	Immediately

SURVEILLANCE REQUIREMENTS

SURVEILLANCE	FREQUENCY
ACSR 3.8.1.1 Verify that the fuel oil volume in the required standby diesel generator fuel tank is $\geq \{ [ ] \text{ m}^3 \{ [ ] \text{ gal} \}$ .	31 days
ACSR 3.8.1.2 Verify that the required standby diesel generator starts and operates at $\geq [4000]$ kw for $\geq 1$ hour.	92 days

## ACM B 3.8 ELECTRICAL POWER SYSTEMS

### AC B 3.8.1 Standby Diesel Generators

#### BASES

---

The diesel generators (DGs) are required to provide power for recharging batteries to support post-accident monitoring (i.e., [RTNSS] Criterion B), and for Fuel and Auxiliary Pools Cooling System (FAPCS) in non-seismic PRA sequences (i.e., [RTNSS] Criterion C). No DG-derived AC power is required for 72 hours after an abnormal event.

The DG function is a nonsafety-related function that satisfies the significance criteria for Regulatory Treatment of Non-Safety Systems, and therefore requires regulatory oversight. The short-term availability controls for this function, which are specified as Completion Times, are acceptable to ensure that the availability of this function is consistent with the functional unavailability in the ESBWR PRA. The surveillance requirements also provide an adequate level of support to ensure that component performance is consistent with the functional reliability in the ESBWR PRA.

{One DG is required to be OPERABLE during MODES 1, 2, 3, and 4 to support FAPCS and the ability to recharge batteries to support post-accident monitoring.}

DG starts required by ACSR 3.8.1.2 may be preceded by an engine prelube period to minimize wear and tear on the DGs during testing. For the purpose of this testing, the DGs must be started from standby conditions, that is, with the engine coolant and oil being continuously circulated and temperature maintained consistent with manufacturer recommendations. Testing required by ACSR 3.8.1.2 also demonstrates OPERABILITY of the associated fuel oil transfer pump and necessary DG support system function(s).

---

ACM 3.8 ELECTRICAL POWER SYSTEMS

AC 3.8.2 Control Room Habitability Area (CRHA) Heating, Ventilation, and Air Conditioning (HVAC) Subsystem (CRHAVS) Portable Generator

ACLCO 3.8.2 The CRHAVS portable generator shall be AVAILABLE.

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

ACTIONS

CONDITION	REQUIRED ACTION	COMPLETION TIME
A. CRHAVS portable generator unavailable.	A.1 Restore CRHAVS portable generator to AVAILABLE status.	7 days
B. Required Action and associated Completion Time not met.	B.1 Enter ACLCO 3.0.3.	Immediately

SURVEILLANCE REQUIREMENTS

SURVEILLANCE	FREQUENCY
ACSR 3.8.2.1 Verify that the fuel volume of $\geq \{[ ] \text{ m}^3 \{ [ ] \text{ gal} \}$ is AVAILABLE for the required RCHAVS portable generator.	31 days
ACSR 3.8.2.2 Verify that the required CRHAVS portable generator starts and operates at $\geq \{[2] \text{ kw} \}$ for $\geq 1$ hour.	92 days

## ACM B 3.8 ELECTRICAL POWER SYSTEM

### AC B 3.8.2 Control Room Habitability Area (CRHA) Heating, Ventilation, and Air Conditioning (HVAC) Subsystem (CRHAVS) Portable Generator

#### BASES

---

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

The CRHAVS portable generator function is a nonsafety-related function that satisfies the significance criteria for Regulatory Treatment of Non-Safety Systems, and therefore requires regulatory oversight. The short-term availability controls for this function, which are specified as Completion Times, are acceptable to ensure that the availability of this function is consistent with the functional unavailability in the ESBWR PRA. The surveillance requirements also provide an adequate level of support to ensure that component performance is consistent with the functional reliability in the ESBWR PRA.

{CRHAVS portable generator starts required by ACSR 3.8.2.2 may be preceded by an engine prelube period to minimize wear and tear on the generator during testing.}

---

## ACM 4.0 DESIGN FEATURES

---

### AC 4.1 Basemat-Internal Melt Arrest and Coolability (BiMAC) Device

#### AC 4.1.1 Volume

The BiMAC is designed and shall be maintained with an available volume, up to a height of the vertical segments of the BiMAC pipes, sized to contain approximately 400% of the full-core debris.

#### AC 4.1.2 Sacrificial Refractory Layer

The BiMAC is designed and shall be maintained with a refractory material located on top of the BiMAC pipes to protect against melt impingement during the initial corium relocation event.

#### AC 4.1.3 Cover Plate

The BiMAC is designed and shall be maintained with a cover plate providing protection for the BiMAC from CRD housings falling from the vessel.

#### AC 4.1.4 Piping

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

---