22 REGULATORY TREATMENT OF NON-SAFETY SYSTEMS

22.1 Introduction

Unlike the current generation of light-water reactors or the evolutionary advanced light-water reactors (ALWRs), the AP1000 plant design, like AP600, uses passive safety systems that rely almost exclusively on natural forces, such as density differences, gravity, and stored energy, to supply safety injection water and provide core and containment cooling. These passive systems do not include pumps. The passive systems include some active valves, but all the safety-related active valves either require only dc safety-related electric power (supplied by means of batteries), are air operated (and fail safe on loss of air), or are check valves. The AP1000 design does not include any safety-related sources of ac power for operation of passive system components. All active systems (i.e., systems requiring ac power to operate) are designated as non-safety-related, except for the instrumentation and control systems which use safety-related ac converted from safety-related dc power.

As the AP1000 relies on passive safety systems to perform the design-basis safety-related functions of reactor coolant makeup and decay heat removal, different portions of the passive systems also provide certain defense-in-depth backup to primary passive features. For example, while the passive residual heat removal (PRHR) system is the primary safety-related heat removal feature in a non-loss-of-coolant transient, the automatic depressurization system (ADS) together with passive safety injection features provide a safety-related defense-in-depth backup.

The ALWR Utility Requirements Document (URD) for passive plants, promulgated by the Electric Power Research Institute (EPRI), includes standards related to the design and operation of active non-safety-related systems. The URD recommends that the plant designer specifically define the active systems relied upon for defense-in-depth that are necessary to meet passive ALWR plant safety and investment protection goals. Another important aspect of these defense-in-depth systems is long-term, postaccident plant capabilities. Passive systems should be able to perform their safety functions, independent of operator action or offsite support for 72 hours after an initiating event. After 72 hours, non-safety or active systems may be required to replenish the passive systems or to perform core and containment heat removal duties directly. The AP1000 includes active systems that provide defense-in-depth (or investment protection) capabilities for reactor coolant system makeup and decay heat removal. These active systems are the first line of defense to reduce challenges to the passive systems in the event of transients or plant upsets. As noted above, most active systems in the AP1000 are designated as non-safety-related.

Examples of non-safety-related systems that provide defense-in-depth capabilities for the AP1000 design include the chemical and volume control system, normal residual heat removal system (RNS), and the startup (backup) feedwater system. For these defense-in-depth systems to operate, the associated systems and structures to support these functions must also

be operable, including non-safety-related standby diesel generators, the component cooling water system, and the service water system. The AP1000 also includes other active systems, also designated as non-safety-related, such as the heating, ventilation, and air conditioning system, that remove heat from the instrumentation and control (I&C) cabinet rooms and the main control room (MCR) and prevent the excessive accumulation of radioactive materials in the control room to limit challenges to the passive safety capabilities for these functions.

In existing plants, and in the evolutionary ALWR designs, many of these active systems are designated as safety-related. However, by virtue of their designation in the AP1000 design as non-safety-related, credit is generally not taken for the active systems in the Chapter 15 licensing design-basis accident analyses (except in certain cases where operation of a non-safety-related system could make an accident worse). In SECY-90-406, "Quarterly Report on Emerging Technical Concerns," dated December 17, 1990, the staff listed the role of these active systems in passive plant designs as an emerging technical issue. In SECY-93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor Designs," dated April 2, 1993, the staff discussed the issue of the regulatory treatment of non-safety systems (RTNSS) and stated that it would propose a process for resolution of this issue in a separate Commission paper. The staff subsequently issued SECY-94-084, "Policy and Technical Issues Associated with the Regulatory Treatment of Non-Safety Systems in Passive Plant Designs," dated March 28, 1994, which discusses that process. SECY-95-132, "Policy and Technical Issues Associated with the Regulatory Treatment of Non-Safety Systems in Passive Plant Designs (SECY-94-084)," dated May 22, 1995, was essentially a revised version of SECY-94-084 issued to respond to Commission comments on that paper and to request Commission approval of certain revised positions. However, the staff's position on RTNSS as discussed in SECY-94-084 was approved by the Commission (Staff Requirements Memorandum dated June 30, 1994), and was unchanged in SECY-95-132.

In SECY-94-084, the staff cited the uncertainties inherent in the use of the passive safety systems, resulting from limited operational experience and relatively low driving forces inherent in these systems. The uncertainties relate to both system performance characteristics (e.g., the possibility that check valves could stick under low-differential-pressure conditions) and thermal-hydraulic phenomena (e.g., critical flow through ADS valves). The system performance issues were addressed in some cases by design enhancements. For example, check valve performance was improved by using biased-open check valves in the core makeup tank (CMT) discharge lines. In addition, the check valves in the in-containment refueling water storage tank (IRWST) injection lines and containment recirculation lines were designed to ensure that the pressure differential across these valves would be small during normal plant operation. The applicant also addressed, to some extent, uncertainties associated with the passive system reliability, and thermal-hydraulic uncertainties by virtue of the design certification test programs. The U.S. Nuclear Regulatory Commission (NRC or staff) has also performed confirmatory integral systems testing and analyses over a broad range of conditions to help determine the thermal-hydraulic "boundaries" within which the plant responds in an acceptable manner for both design-basis events and accidents beyond the licensing design basis. These activities have reduced, but not eliminated, the thermal-hydraulic uncertainties associated with passive system performance.

The residual uncertainties associated with passive safety system performance increase the importance of active systems in providing defense-in-depth functions that back up the passive systems. Recognizing this, the NRC and EPRI developed a process to identify important active systems and to maintain appropriate regulatory oversight of those systems. This process does not require that the active systems brought under regulatory oversight meet all safety-related criteria, but rather that these controls provide a high level of confidence that active systems having a significant safety role are available when challenged.

The ALWR URD specifies standards concerning design and performance of active systems and equipment that perform non-safety-related, defense-in-depth functions. These standards include radiation shielding to permit access after an accident, redundancy for the more probable single active failures, availability of non-safety-related electric power, and protection against more probable hazards. The standards also address realistic safety margin analysis and testing to demonstrate the systems' capabilities to satisfy their non-safety-related, defense-in-depth functions. However, the ALWR URD does not include specific quantitative standards for the reliability of these systems.

SECY-94-084 and SECY-95-132 describe the scope, criteria, and process used to determine regulatory treatment of non-safety systems in the passive plant designs.

The following five key elements made up the process:

- The ALWR URD describes the process to be used by the designer for specifying the reliability/availability (R/A) missions of risk-significant structures, systems, and components (SSCs) needed to meet regulatory requirements and to allow comparisons with NRC safety goals. An R/A mission is the set of requirements related to performance, reliability, and availability for a SSC function that adequately ensures its task, as defined by the focused probabilistic risk assessment (PRA) or deterministic analysis, is accomplished.

- The designer applies the process to the design to establish R/A missions for the risk-significant SSCs.

- If active systems are determined to be risk-significant, the NRC reviews the R/A missions to determine if they are adequate, and if the operational reliability assurance process or simple technical specifications (TS) and limiting conditions for operation are adequate to give reasonable assurance that the missions can be met during operation.

- If active systems are relied upon to meet the R/A missions, the designer imposes design requirements commensurate with risk significance on those elements involved.

- R/A missions are not included in the design certification rule. Instead, NRC includes deterministic requirements on both safety-related and non-safety-related design features in the design certification rule.

The steps of this RTNSS process to address these key elements are discussed in the following two sections.

22.2 Scope and Criteria for the RTNSS Process

The RTNSS process applies broadly to those non-safety-related SSCs that perform risk significant functions, and therefore, are candidates for regulatory oversight. The RTNSS process applies the following five criteria to determine those SSC functions:

- SSC functions relied upon to meet deterministic NRC performance requirements such as Title 10 of the Code of Federal Regulations (CFR) 50.62 for mitigation of anticipated transients without scram (ATWS) and 10 CFR 50.63 for station blackout (SBO)

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

- SSC functions relied upon under power-operating and shutdown conditions to meet the Commission's safety goal guidelines of a core damage frequency (CDF) of less than 1.0E-04 each reactor year and a large release frequency (LRF) of less than 1.0E-06 each reactor year

- SSC functions needed to meet the containment performance goal, including containment bypass, during severe accidents. This issue was discussed in detail in SECY-93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs," dated April 2, 1993. For the AP1000, this criterion for assessing containment performance is the degree to which the design comports with the Commission's probabilistic containment performance goal of 0.1 conditional containment failure probability (CCFP) when no credit is provided for the performance of the non-safety-related "defense-in-depth" systems for which there will be no regulatory oversight. The CCFP is a containment performance measure that provides perspectives on the degree to which the design has achieved a balance between core damage prevention and core damage mitigation. CCFP was used in a qualitative manner to confirm that the design, combined with the regulatory oversight for identified SSCs, has maintained an acceptable balance between core damage prevention and mitigation, but was not used as a criterion for establishing the availability requirements for non-safety-related "defense-in-depth" systems.

- SSC functions relied upon to prevent significant adverse systems interactions

22.3 Specific Steps in the RTNSS Process

The following specific steps were established to implement the process described above.

22.3.1 Comprehensive Baseline Probabilistic Risk Assessment

The RTNSS process starts with a comprehensive Level-3 baseline PRA, which includes all appropriate internal and external events for both power and shutdown operations. Adequate treatment of R/A uncertainties, long-term safety operation, and containment performance are included. Seismic events are evaluated using a margins approach. Containment performance is addressed with consideration of sensitivities and uncertainties in accident progression and inclusion of severe accident phenomena, including explicit treatment of containment bypass. Mean values are used to determine the availability of passive systems and the frequencies of core damage and large releases. Appropriate uncertainty and sensitivity analyses are used to estimate the magnitude of potential variations in these parameters and to identify significant contributors to these variations. Also an adverse systems interaction study is performed, and its results are considered in the PRA. The AP1000 baseline PRA is discussed in Chapter 19 of this report.

22.3.2 Search for Adverse Systems Interactions

The RTNSS process includes systematic evaluation of adverse systems interactions between the active and passive systems. The results of this analysis are used for design improvements to minimize adverse systems interactions and are considered in making PRA models, as noted above.

22.3.3 Focused PRA

The focused PRA is a sensitivity study, which includes the passive systems and only those active systems necessary to meet the safety goal guidelines approved by the Commission in SECY-94-084 (see criterion (3) in Section 22.2 above). The focused PRA results are used to determine the R/A missions of non-safety-related SSCs which are risk-significant as follows.

First, the scope of initiating events and their frequencies are maintained in the focused PRA as in the baseline PRA. As a result, non-safety-related SSCs used to prevent the occurrence of initiating events will be subject to regulatory oversight applied commensurate with their R/A missions for prevention.

Second, following an initiating event, the comprehensive Level-3 focused PRA event-tree logic will not include the effect of non-safety-related standby SSCs. As a minimum, these event trees will not include the defense-in-depth functions and their support, such as onsite ac power, to determine if the passive safety systems, when challenged, can provide sufficient capability without non-safety-related backup to meet the NRC safety goal guidelines for a CDF of 1E-04 each year and an LRF of 1E-06 each reactor year. The applicant evaluates the containment performance, including bypass, during a severe accident. If it is determined that non-safety-related SSCs are needed to be added to the focused PRA model to meet the safety goals, these SSCs are subject to regulatory oversight on the basis of their risk significance.

Although not discussed explicitly in these steps, an important aspect of the focused PRA is the evaluation of uncertainties, particularly those uncertainties inherent in the use of passive safety

systems. Because of limited data and experience with the passive systems, thermal-hydraulic uncertainties could impact the PRA results. Specifically, thermal-hydraulic uncertainties can have a direct impact on the determination of success criteria for accident sequences in the PRA. As noted above, this was one of the primary reasons for the development of the RTNSS process.

22.3.4 Selection of Important Non-Safety-Related Systems

The RTNSS process includes the determination of any combinations of non-safety-related SSCs that are necessary to meet NRC regulations, safety goal guidelines, and the containment performance goal objectives. These combinations consist of criteria (1) and (5) in Section 22.2 of this report, in which NRC regulations are the bases for consideration, and criteria (3) and (4) in Section 22.2 of this report, in which PRA methods are the bases for consideration. To address the long-term safety issue in criterion (2) of Section 22.2 of this report, PRA insights, sensitivity studies, and deterministic methods are used to establish the ability of the design to maintain core cooling and containment integrity beyond 72 hours. Non-safety-related SSCs required to meet deterministic regulatory requirements (criterion (1)), to resolve the long-term safety and seismic issues (criterion (2)), and to prevent significant adverse systems interactions (criterion (5)) are subject to regulatory oversight.

The staff expects regulatory oversight for all non-safety-related SSCs in the focused PRA model needed to meet NRC requirements, the safety goal guidelines, and containment performance goals. Using the focused PRA to determine the non-safety-related SSCs important to risk involves the following steps:

- Determine those non-safety-related SSCs needed to maintain the initiating event frequencies at the comprehensive baseline PRA levels.

- Add the necessary success paths with non-safety-related systems and functions in the focused PRA to meet the safety goal guidelines, containment performance goal objectives, and NRC regulations. Choose the systems by considering the factors for optimizing the design effect and benefit of particular systems. Perform PRA importance studies to assist in determining the importance of these SSCs.

22.3.5 Non-Safety-Related System Reliability/Availability Missions

Upon completion of the selection step above, the applicant determines and documents the functional R/A missions of active systems needed to meet the safety goal guidelines, containment performance goals, and NRC performance requirements, and proposes regulatory oversights as discussed in Section 22.3.6 below. The steps described in Sections 22.3.4, 22.3.5, and 22.3.6 are repeated to ensure that the most appropriate active systems and their R/A missions are selected.

As part of this step, the applicant establishes graded safety classifications and graded requirements for I&C systems on the basis of the importance to safety of their functional R/A missions.

22.3.6 Regulatory Oversight Evaluation

Upon completing the steps detailed in the previous five sections, the applicant conducts the following activities to determine the means of appropriate regulatory oversight for the RTNSS-important non-safety systems:

- review the DCD Tier 2 Information and the PRA, and audit plant performance calculations to determine that the design of these risk-significant, non-safety-related SSCs satisfies the performance capabilities and R/A missions.

- review the DCD Tier 2 Information to determine that it includes the proper design information for the reliability assurance program, including the design information for implementing the maintenance rule.

- review the DCD Tier 2 Information to determine that it includes proper short-term availability control mechanisms, if required for safety and determined by risk significance, such as simple TS.

22.4 Other Issues Related to RTNSS Resolution

In SECY-94-084, several other issues were discussed, related overall to passive plant performance or performance of specific passive safety systems. Resolution of these issues was tied by the staff to an acceptable resolution of the RTNSS issue. On the basis of the defense-in-depth equipment availability administrative controls discussed in Section 22.5.9 of this report, the staff was able to reach acceptable conclusions regarding the AP1000 design related to (1) safe shutdown requirements as discussed in Section 6.3.1.4; (2) station blackout as discussed in Section 8.6.2.1; and (3) electrical distribution as discussed in Section 8.2.4 of this report.

22.5 NRC Review of Westinghouse's Evaluation of Systems for Inclusion in RTNSS

Westinghouse Topical Report WCAP-15985, Revision 1, "AP1000 Implementation of the Regulatory Treatment of Nonsafety-Related Systems Process," dated April 2003, describes the applicant's implementation of RTNSS process for the AP1000 for the determination of which non-safety-related systems in the AP1000 should be subject to regulatory treatment, and under what conditions that treatment should apply. The AP1000 RTNSS implementation followed the scope, criteria, and specific steps described in SECY-94-084 and SECY-95-132, which are discussed in Sections 22.2 and 22.3 of this report. The criteria used by the applicant to determine which systems required regulatory oversight were based on probabilistic assessments of passive system performance (focused PRA) and on an initiating event frequency study. In addition, containment performance challenges and seismic considerations, deterministic assessments of the design response to events such as ATWS and SBO, long-term cooling (post-72 hour), and adverse systems interactions were evaluated.

22.5.1 Focused Probabilistic Risk Assessment

As discussed above, one of the steps in the RTNSS process is the use of focused PRA results to identify non-safety systems needed to meet the CDF and LRF safety goal guidelines. The detailed focused PRA results are provided in Westinghouse AP1000 PRA report, APP-GW-GL-022, "AP1000 Probabilistic Risk Assessment." The focused PRA evaluation in WCAP-15985 is based on the results from the AP1000 PRA report. The staff's evaluation of the focused PRA results can be found in Section 19.1.7 of the report. The resolution of the open item in Section 19.1.7 could impact the resolution of the RTNSS. Therefore, the evaluation below based on the PRA results is subject to satisfactory closure of Open Item 19.1.10.1-3.

22.5.1.1 PRA Event Mitigation Evaluation

Section 2 of WCAP-15985, Revision 1, describes the focused PRA sensitivity studies performed to quantify the importance of non-safety-related systems in mitigating PRA events. The focused PRA sensitivity studies calculate the CDF and LRF without reliance on non-safety-related SSC mitigation. If a non-safety-related SSC mitigation functions is relied upon in the focused PRA sensitivity studies so that the calculated CDF and LRF meet the safety goal guidelines, it is designated risk important and will be subject to regulatory oversight. The focused PRA sensitivity studies include an evaluation of internal events that occur at-power. The applicant stated that internal fire and flood events are not included in this evaluation because the AP1000 PRA quantification has shown them to have a much lower risk. Seismic margins are used to evaluate seismic events.

The focused PRA sensitivity study is based on the AP1000 baseline PRA by setting the failure probability of each non-safety SSC to 1. The initiating event frequencies remain the same as in the baseline PRA. Table 2-1 in WCAP-15985, Revision 1, lists the safety-related systems and functions credited in the focused PRA sensitivity study, and the non-safety-related systems and functions that were assumed to be failed. Table 2 provides the summary results for the baseline and focused PRA sensitivity study with comparisons between two cases: (1) assuming failure of all non-safety-related systems, and (2) assuming failure of all non-safety systems, except for the manual diverse actuation system (DAS) controls of the following functions:

- reactor trip
- PRHR HX and IRWST gutter valves air operated valves (AOV)
- CMT isolation valves (AOV)
- ADS stages 1, 2, 3 motor operated valves (MOV), and 4 (squib)
- IRWST injection isolation valves (squib)
- containment recirculation isolation valves (squib)
- PCS water drain valves (AOV and MOV)
- containment isolation valves (AOV)
- Hydrogen igniters

The detailed focused PRA sensitivity study is described in Chapter 50 of the AP1000 PRA report. Based on the summary results provided in Table 2-2 of WCAP-15985, Revision 1, the

case 1 focused PRA with the assumed failure of all non-safety system mitigation functions results in the large release frequencies (LRF) above the safety goal guideline of 1.0E-06. However, the Case 2 focused PRA taking credit of the DAS manual controls results in both the CDF and LRF meeting the safety goal guidelines of 1.0E-4 and 1.0E-6, respectively.

Since these DAS manual controls are credited to meet the LRF safety goal, these DAS manual controls are identified as RTNSS-important and subject to regulatory oversight. In accordance with 10 CFR Part 50.36(c)(2)(ii)(D) Criterion 4, limiting conditions for operation must be established in the plant TS for a structure, system, or component with operating experience or probabilistic risk assessment has shown to be significant to public health and safety. Therefore, in DCD Tier 2 Chapter 16, TS 3.3.5, "Diverse Actuation System (DAS) Manual Controls," specifies the LCO and surveillance requirements on the DAS manual controls. In addition, the DAS is included in the AP1000 D-RAP in DCD Tier 2 Table 17.4-1, as well as the AP1000 ITAAC in Tier 1 Information subsection 2.5.1. The quality assurance guidance in Generic Letter 85-06 is applicable to the nonsafety-related equipment encompassed by the ATWS rule. Section 4.1 of WCAP-15985 states that certain DAS functions and the associated DAS power supplies are needed to meet the requirements of the ATWS rule. However, as discussed in DSER Open Item 20.7-1, Westinghouse does not clearly describe the quality assurance controls applied to the DAS power supplies. Therefore, the evaluation of the quality assurance associated with the power supplies to DAS is subject to the resolution of Open Item 20.7-1.

Section 2.3 of WCAP-15985, Rev. 1, also provides an evaluation of potential uncertainties associated with assumptions made in the PRA models of passive systems (e.g., failure rates of IRWST injection line check and squib valves), non-safety-related SSC importance in an initiating event frequency, and hydrogen standing flames uncertainty. The objectives of this PRA uncertainty evaluation is to determine which non-safety-related SSCs should be identified as RTNSS-important to add margin to compensate for the PRA uncertainties. In certain situations, there are no non-safety-related SSCs that can directly compensate for the PRA uncertainties, and therefore, margin is provided in the PRA by adding regulatory oversight on non-safety-related SSCs that improve the PRA sensitivity study results for other sequences. As a result of this evaluation, the following non-safety-related SSCs are designated RTNSS-important to add margin to compensate for potential uncertainties:

- Automatic DAS ATWS and engineered safety feature actuation (provides margin for reactor trip breaker uncertainty, thermal-hydraulic analysis uncertainty and for protection and safety monitoring system (PMS) software uncertainty).

- RNS injection capability and onsite power supplies (provides margin for ADS/IRWST injection/containment recirculation valve reliability uncertainty, and long-term cooling thermal-hydraulic uncertainty)

- Hydrogen igniters (provide margin for uncertainty in hydrogen burn consequences)

Section 22.5.9 below describes the short-term availability control of these RTNSS-important SSCs.

22.5.1.2 PRA Initiating Event Frequency Evaluation

Section 3 of WCAP-15985 describes the evaluation performed to study the importance of the non-safety-related systems to the initiating event frequencies used for at-power and shutdown initiating event frequencies in the AP1000 PRA. A total of 11 categories of initiating events were identified for at-power and shutdown conditions. These initiating events are:

At-power initiating events:

- main steam line stuck open safety valve
- reactor coolant system leak
- loss-of-coolant accidents
- secondary side breaks
- transients
- anticipated transient without scram
- miscellaneous special initiators

Shutdown initiating events:

- shutdown loss-of-coolant accident
- shutdown loss of offsite power
- shutdown loss of decay heat removal
- reactor coolant system overdrain

The evaluation of the importance of the non-safety-related SSC unavailability to the initiating event frequencies is based on three criteria:

- Are non-safety related SSCs considered in the calculation of the initiating event frequency?

- Does the unavailability of the non-safety-related SSCs significantly affect the calculation of the initiating event frequency? and,

- Does the initiating event significantly affect CDF and LRF for the PRA?

Sections 59.3 and 59.4, respectively, of the AP1000 PRA report provides AP1000 PRA results and insights regarding the CDF and LRF from internal initiating events at power. In WCAP-15985, Westinghouse states that the results of probabilistic evaluations indicated that, for most at-power events, non-safety-related SSCs played minimal roles in initiating event frequencies, CDF, and LRF. One exception to these conclusions was found in the evaluation of non-LOCA transient with main feedwater flow, which has a CDF of 1.4 percent and LRF of 7.5 percent. Therefore, the non-safety-related SSCs required for normal at-power operation associated with this event are important with respect to the effect of this initiating event. These non-safety-related secondary plant systems include:

- main steam system
- main feedwater system
- condensate system
- main turbine
- main turbine control and diagnostics system
- plant control system portions that control main steam, main feedwater, condensate, and main turbine whose malfunction can cause a reactor trip

Therefore, these SSCs are subject to regulatory oversight through investment protection short-term availability controls. However, as discussed in Section 10.3.2 of WCAP-15985, no regulatory oversight for these systems are recommended. Rather, they are addressed through the design improvements in various AP1000 design features (such as improvements in the main feedwater system, and use of digital steam generator water level system, and digital turbine electrohydraulic control system) that affect the operation of these systems. It is noted that the AP1000 initiating event frequency calculation is conservative in that the design improvements that could affect the initiating event frequencies are not credited in the PRA initiating event frequency sensitivity studies. These design improvements with increased reliability would reduce the initiating event frequencies. These non-safety-related systems that impact the turbine trip/spurious reactor trip and loss of main feedwater initiating events are required to continuously operate to support normal plant power operation. By providing more fault-tolerant system designs that increase plant reliability and availability, the design improvements also directly increase plant safety by reducing the potential for plant transients or trips that could present challenges to the plant. As the regulatory oversight of the RTNSS-important non-safety-related SSCs is intended to ensure the reliability and availability, when called upon, of those systems that are normally in standby operation, it is not meaningful to consider additional regulatory oversight beyond the existing operational controls for the non-safety-related systems that are required to operate during power operation. The staff agrees with the applicant that additional regulatory oversight for the AP1000 non-safety-related SSCs that impact these two initiating events, beyond that provided via the DCD design details and via existing operational controls on current plants, will not provide significant benefit in reducing either the initiating event frequency, CDF, or LRF. Therefore, the staff has determined that no additional oversight beyond the existing operational controls is needed for the non-safety-related secondary plant systems listed above.

Chapter 54 of the AP1000 PRA report describes the low-power and shutdown risk assessment for the AP1000. In Sections 3.8 through 3.10 of WCAP-15985, Westinghouse concludes that the results of probabilistic evaluations showed that, for events at shutdown, non-safety-related SSCs are important in the scenarios of loss of offsite power and loss of decay heat removal, especially during reduced-inventory operations. Consequently, the applicant proposed "short-term availability recommendations" for the following non-safety-related SSCs:

- Offsite power system
- Main ac power system
- Onsite standby (diesel) power system
- RNS
- Component Cooling Water system

- Service Water system

It is important to note that the availability controls proposed by the applicant applied only during reduced reactor coolant system inventory operations during cold shutdown and refueling (Modes 5 and 6).

22.5.1.3 Focused Probabilistic Risk Assessment Summary

Based on the above discussions, the staff has determined that the applicant has followed the RTNSS process in using the focused PRA results to identify RTNSS-important non-safety-related SSCs. Therefore, this process is acceptable.

22.5.2 Containment Performance Consideration

Section 7 of WCAP-15985 provides an evaluation of the AP1000 design for meeting the following deterministic containment performance goal described in SECY-93-087, and approved by the Commission in a Staff Requirements Memorandum dated July 21, 1993:

> The containment should maintain its role as a reliable, leak-tight barrier by ensuring that containment stresses do not exceed ASME service level C limits for a minimum period of 24 hours following the onset of core damage, and that following this 24-hour period the containment should continue to provide a barrier against the uncontrolled release of fission products.

The containment performance evaluation considers the functions of RCS depressurization, passive safety system injection, containment isolation, passive containment cooling, and ex-vessel coolable geometry. Based on the evaluation of non-safety-related SSCs for meeting the containment performance goal, the applicant identified that the reactor vessel (RV) insulation design is required to support in-vessel retention, and that at least one hydrogen igniter group should be available.

As described in Section 19.1.7 of this report, the staff also assesses the AP1000 design's compliance with the probabilistic containment performance goal of 0.1 conditional containment failure probability (CCFP). The staff also identified that the RV insulation design is required for successful external reactor vessel cooling.

Therefore, both non-safety-related RV insulation design and hydrogen igniters are subject to regulatory oversight. As discussed in Section 22.5.1.1 of this report, Westinghouse also identified the need for regulatory oversight of the hydrogen igniters to provide margin for uncertainty in hydrogen burn consequences. DCD Tier 2 Section 5.3.5 describes the design features of the RV insulation system, and the applicant determined that short-term availability control for the RV insulation system is unnecessary. This is because the system is included as a risk-significant SSC in the reliability assurance program, and the important acceptance criteria associated with the insulation design are included in ITAAC 2.2.3.

The hydrogen igniters are described in DCD Tier 2 subsection 6.2.4. The Hydrogen igniters are subject to AP1000 D-RAP and are included in ITAAC 2.3.9. The hydrogen igniters are also subject to short-term availability controls as described in DCD Tier 2 Section 16.3, Table 16.3-2, Item 2.8.

The staff has determined that the applicant has properly identified the RTNSS-important SSCs to meet the containment performance goals in accordance with the Commission's approved position in SECY-93-087. Therefore, the containment performance evaluation is acceptable.

22.5.3 Seismic Consideration

The seismic margins analysis used to perform the AP1000 seismic evaluation does not credit non-safety-related SSCs. Therefore, no non-safety-related SSC is identified as RTNSS-important. Since the SSCs relied upon to address design basis events are designed in accordance with the AP1000 seismic design criteria provided in DCD Tier 2 Section 3.7, the staff has determined they are acceptable.

22.5.4 Deterministic ATWS and SBO Evaluation

In Sections 4 and 5 of WCAP-15985, Westinghouse provides deterministic evaluations regarding AP1000's compliance with the ATWS and SBO rules set forth in 10 CFR 50.62 and 50.63, respectively. The evaluation concludes that the AP1000 safety-related systems automatically establish and maintain safe shutdown conditions for the plant following design basis events, including an extended loss of ac power sources, and therefore no installed non-safety-related SSCs are relied upon to meet the requirements of 10 CFR 50.63. However, the following non-safety-related system functions are needed to meet ATWS regulatory requirements of 10 CFR 50.62:

- DAS actuation functions of reactor trip, turbine trip, and PRHR during power operation
- the non-Class-1E dc power and uninterruptible power supply (UPS), which provide power to the DAS.

The electrical systems and specified DAS functions were specified for RTNSS controls only during power operation (Modes 1 and 2).

In Section 10.2 of WCAP-15985, Westinghouse summarizes the mission statements of the DAS and non-class 1E dc power and UPS system for ATWS events. These non-safety-related systems are included in DCD Tier 2 Section 16.3, Tables 16.3-2, Items 1.1 and 3.4, for short-term availability controls.

The staff has determined that the applicant has properly identified the RTNSS-important SSCs for compliance with the requirements of 10 CFR 50.62 and 50.63. Therefore, the applicant's evaluation of the ATWS and SBO rule as applied to RTNSS is acceptable.

22.5.5 Evaluation of Adverse Systems Interactions

In Section 8 of WCAP-15985, Westinghouse considers potential adverse systems interactions where non-safety-related systems may adversely interact with the safety-related system. In response to a staff request for additional information (RAI-440-128) the applicant submitted WCAP-15992, Revision 1, "AP1000 Adverse System Interactions Evaluation Report," dated February 2003, which provided a detailed systematic compilation and assessment of potential system interactions in the AP1000. Several different types of interactions are considered in WCAP-15992, including:

- Interactions among the passive safety systems
- Interactions between passive safety systems and active non-safety-related systems
- Interactions resulting from operator errors of commission
- Spatial interactions (i.e., interactions that could occur as a result of equipment location in the plant)

After evaluating the potential adverse systems interactions that could occur in the AP1000, the applicant concluded that there were no non-safety-related SSCs that required RTNSS treatment as a result of this specific issue.

The staff also used the information provided in WCAP-15992, Revision 1, as part of the framework for the evaluation of the applicant's emergency response guidelines, in assessing both operator actions to preclude potential adverse systems interactions and interactions that could arise as a result of human commission errors. As a result of its review, the staff agrees with the applicant's conclusion that there are no adverse systems interactions that require the implementation of RTNSS controls. Accordingly, the staff finds the applicant's treatment of adverse systems interactions as described in WCAP-15992, Revision 1, to be acceptable, and does not require RTNSS treatment of any AP1000 non-safety-related SSCs to address adverse systems interaction issues. The staff's evaluation of adverse systems interactions has also been reflected in the review of Unresolved Safety Issue A-17 in Chapter 20 of this report.

22.5.6 Post-72-Hour Actions and Equipment

The passive safety-related systems in the AP1000 are designed to automatically establish and maintain safety shutdown conditions for the plant following design basis events, assuming the most limiting single failure. These passive safety systems will function, under design-basis conditions, for at least 72 hours without the need for operator action and without both non-safety related onsite and offsite power to supplement or extend their capabilities. After 72 hours, support actions and equipment may be needed.

The staff evaluation of post-72 hour actions is based on the position developed during the AP600 review and described in SECY-96-128, "Policy and Key Technical Issues Pertaining to the Westinghouse AP600 Standardized Passive Reactor Design," dated June 12, 1996, which

was approved by the Commission in a memorandum dated January 15, 1997. The staff position is that post-72-hour actions related to all design-basis events be accomplished with onsite equipment and supplies for the long term. After 7 days, replenishment of consumables such as diesel fuel oil from offsite suppliers can be credited. The staff further stated that the equipment needed for post-72-hour support need not be in "automatic standby mode," but must be readily available for connection and protected from natural phenomena, including seismic events, as required by 10 CFR Part 50, Appendix A, General Design Criterion (GDC) 2, "Design Basis for Protection Against Natural Phenomena." In a memorandum to the Commission dated June 23, 1997, the staff also stated that a Combined License (COL) applicant would be required to have appropriate availability controls, consistent with RTNSS requirements, for non-safety-related SSCs for post 72-hour support.

In Section 6 of WCAP-15985, Westinghouse describes the AP1000 post-72 hour actions. WCAP-15985 states that the following safety functions are relied upon 72 hours after an accident:

- core cooling, inventory and reactivity control
- containment cooling and ultimate heat sink
- main control room habitability
- postaccident monitoring
- spent fuel pool cooling.

To support these safety functions, the AP1000 design includes both non-safety-related onsite equipment and safety-related connections for use with transportable equipment and supplies to provide support extended operation of the passive safety systems. These extended supports include the following:

- Provide electrical power to supply the postaccident and spent fuel pool monitoring instrumentation using ancillary diesel generators that connect to safety-related electrical connections.

- Provide makeup water to the PCS water storage tank to maintain external containment cooling water flow and to the spent fuel pool to maintain spent fuel cooling, using a PCS recirculation pump powered by an ancillary diesel generator that connects to a safety-related makeup connection.

- Provide open doors and ancillary fans for ventilation and cooling of the MCR, the instrumentation and control rooms, and the dc equipment rooms.

The onsite non-safety-related equipment that supports these extended operations is subject to short-term availability controls. This onsite equipment includes ancillary diesel generators and an ancillary diesel generator fuel oil storage tank, PCS recirculation pump and ancillary PCS water storage tank, and ancillary fans for the MCR and I&C rooms. Section 10.3 of WCAP-15985 specifies the short-term availability controls for these equipment, and also states that the long-term shutdown equipment should be available following seismic and high wind events that may make procurement of offsite equipment more difficult. In addition, this equipment is located in the auxiliary building, which is a Seismic Category I structure.

Since all required equipment for post-72 hour actions is onsite, the equipment meets 10 CFR Part 50, Appendix A, GDC-2 with respect to protection against natural phenomena, and consumable supplies are sufficient to last at least 7 days, the staff concludes that the post-72 hour actions for AP1000 comply with the staff approved positions as stated in SECY-96-128 and are therefore acceptable.

22.5.7 Mission Statements and Regulatory Oversight of Important Nonsafety-Related SSCs

According to the RTNSS process, non-safety-related SSCs that are relied upon to meet the criteria described in Section 22.2 of this report are RTNSS-important and subject to regulatory oversight. As described in Section 22.5.1 through 22.5.6 above, the applicant has provided its evaluation to identify the RTNSS-important SSCs. In Section 10 of WCAP-15985, Westinghouse identifies the missions of these important non-safety systems, and recommends their regulatory oversights.

Section 10.2 of WCAP-15985 provides mission statements of the important nonsafety-related SSCs, which are a summary of those identified in Sections 2 through 9 of WCAP-15985 (Sections 22.5.1 through 22.5.6 above). They are summarized below:

- DAS manual actuations provide capability to manually actuate reactor trip and ESF functions during at-power and shutdown Modes. (TS 3.3.5)

- DAS (ATWS) Actuation provides the capability to automatically (1) actuate reactor and turbine trip and (2) initiate PRHR under conditions indicative of an ATWS during power operation. (1.1)

- DAS (ESF) Actuation automatically actuate passive safety features during at-power and shutdown Modes. (1.2)

- RNS Low-Pressure RCS Injection provides means of low-pressure RCS injection from cask loading pit following ADS actuation during at-power and shutdown conditions. (2.1)

- RNS Shutdown Cooling provides shutdown decay heat removal during RCS open shutdown conditions. (2.2).

- CCS provides cooling to support RNS shutdown decay heat removal operation during RCS open shutdown conditions. (2.3)

- SWS provides cooling to support CCS shutdown decay heat removal operation during RCS open shutdown conditions. (2.4)

- PCS Water and Spent Fuel Pool Makeup Functions provide the capability to transfer water from the PCS ancillary water storage tank to the PCS water storage tank and the spent fuel pool in all modes of plant operation to support post-72 hour operation of passive safety systems. (2.5)

- MCR ancillary room fans provide cooling of the MCR to support post-72 hour MCR habitability during all modes of plant operation. (2.6)

- Instrumentation Room Fans provide cooling of the 1E instrumentation rooms to support post-72-hour postaccident monitoring during all modes of plant operation. (2.7)

- Hydrogen Igniters prevent combustion of hydrogen that may cause failure of the containment following a core melt in Modes 1, 2, 5 and 6 of plant operation. (2.8)

- Onsite AC Power Supply System provides a backup source of electric power to onsite equipment needed to provide PMS actuation and to support RNS operation during all modes of plant operation following a loss of offsite power. (3.1)

- Offsite AC power system provides electric power to onsite equipment needed to support decay heat removal operation during RCS open shutdown conditions. (3.2)

- Ancillary diesel generators provide power to support post-72 hour operation following at-power and shutdown events. (3.3)

- Non-class 1E DC and UPS system provides electrical power to the DAS and actuation components to actuate reactor and turbine trip and initiate PRHR under conditions indicative of an ATWS during power operation. (3.4)

(Note: The number in the parenthesis after each item indicates the TS number or item number in DCD Tier 2 Table 16.3-2 for short-term availability controls.)

These mission statements encompass a complete list of RTNSS-important non-safety-related SSCs which are the results of the evaluation using the RTNSS process, and are therefore acceptable.

22.5.8 Technical Specifications

Section 10.4 of WCAP-15985 proposes TS 3.3.5 with limiting conditions for operation and surveillance requirements for DAS manual controls.

As discussed in Section 22.5.1.1 of this report, the results of the focused PRA event mitigation evaluation show that with the assumption of failure of the non-safety mitigation functions of the non-safety-related SSCs, the LRF will exceed the safety goal guideline of 1.0E-06 per reactor year. However, by crediting the DAS manual controls in the focused PRA, the CDF and LRF are reduced and meet the safety goal guidelines. Since the DAS manual controls are credited to meet the LRF safety goal, these manual controls are included in the AP1000 TS in accordance with the Criterion 4 of 10 CFR 50.36(c)(2)(ii)(D). The proposed TS for DAS manual controls is described in Section 10.4 of WCAP-15985, and AP1000 TS 3.3.5, “Diverse Actuation System (DAS) Manual Controls.” The staff concludes TS 3.3.5 provides proper regulatory oversights for the DAS manual controls and is acceptable pending completion of the resolution of the open item associated with Section 19.1.7 of this report (Open

Item 19.1.10.1-3) to confirm proper use of PRA results in determining the level of regulatory oversight (e.g., required action completion time and surveillance frequency).

22.5.9 Short-Term Availability Controls

Section 10.3 of WCAP-15985 proposed means for the implementation of RTNSS controls in the form of short-term administrative availability controls for these important SSCs summarized in Section 22.5.7 above, except for the DAS manual controls, which are incorporated in the TS.

The regulatory oversight of these RTNSS-important SSCs as described in Table 10-2, "Investment Protection Short-Term Availability Controls," of WCAP-15985 are incorporated in DCD Tier 2 Section 16.3, Table 16.3-2 of the same title. These short-term availability controls of the RTNSS important SSCs follow the AP600 approach, which had been extensively evaluated and found acceptable during the AP600 design certification application review. The administrative controls are formatted similar to TS, with operability requirements, applicability, actions and completion times (if operability requirements are not met), surveillance requirements, and bases for the availability controls. There are no limiting conditions for operation (i.e., there is no requirement to bring the plant to a safe-shutdown condition when operability requirements are not fulfilled) if the completion times for required actions are not met. However, pending the completion of the resolution of the open item associated with Section 19.1.7 of this report (Open Item 19.1.10.1-3), the staff finds this acceptable since these RTNSS-important non-safety-related systems do not meet the four screening criteria specified in 10 CFR 50.36(c)(2)(ii) for TS LCO, i.e., they are not installed instrumentation used to detect and indicate a significant abnormal degradation of the RCPB (Criterion 1), not a process variable, design feature, or operating restriction that is an initial condition of a design basis accident or transient analysis (Criterion 2), not an SSC that is part of the primary success path and which functions or actuates to mitigate a design basis accident or transient (Criterion 3), and not an SSC which operating experience or PRA has shown to be significant to public health and safety (Criterion 4). In addition, these RTNSS-important SSCs are included in (1) AP1000 design reliability assurance program (D-RAP), as described in DCD Tier 2 Section 17.4, "Design Reliability Assurance Program." and included in DCD Tier 2 Table 17.4-1, "Risk-Significant SSCs Within the Scope of D-RAP," and (2) Inspections, Tests, Analyses, and Acceptance Criteria (ITAAC) as described in DCD Tier 1 information.

Therefore, pending the completion of the resolution of the open item associated with Section 19.1.7 of this report (Open Item 19.1.10.1-3), the staff finds the RTNSS administrative controls in Table 16.3-2 acceptable. In DCD Tier 2 Section 16.3.2, "Combined License Information," the applicant states that COL applicants referencing AP1000 will develop a procedure to control the operability of investment protection SSCs in accordance with Table 16.3-2. The staff identifies this as COL Action Item 22.5.9-1.

22.6 Quality Assurance

AP1000 TS 3.3.5 and DCD Tier 2 Section 16.3 provide regulatory oversights and availability controls for the important non-safety-related systems identified through the RTNSS process. As discussed in Section 22.5.2 above, the reactor vessel insulation system was identified as an

RTNSS item, but not subject to short-term availability control. DCD Tier 2 Section 17.4 describes the D-RAP, and DCD Tier 2 Table 17.4-1 identifies the risk- significant SSCs within the scope of the R-RAP, including those RTNSS-important SSCs listed in Section 22.5.7 above and the RV insulation system. The staff concludes that including the RV insulation system under D-RAP is sufficient regulatory oversight, as discussed in Section 22.5.2 above.