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. However, they do include some active valves, but all the safety-related active valves required either dc safety-related electric power (supplied by 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 alternating current (ac) power for the 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 (I&C) systems which use safety-related ac power 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 the 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, provides a safety-related, defense-in-depth backup.

The ALWR Utility Requirements Document (URD) for passive plants, issued 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 and necessary to meet passive ALWR plant safety and investment protection goals. Defense-in-depth systems provide long-term, post-accident 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 in reducing 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 I&C cabinet rooms and the main control room (MCR).

These systems also 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, as well as 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 licensing design-basis accident analyses described in DCD Tier 2, Chapter 15 (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 (SRM) 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 passive safety systems resulting from limited operational experience and the relatively low driving forces (e.g., density differences and gravity) 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). In some cases, the system performance issues were addressed 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 are designed to ensure that the pressure differential across these valves would be small during normal plant operation. The applicant also addressed uncertainties associated with the passive system reliability, as well as 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 to 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 they are 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 make up the process:

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

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

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

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

(5) The design certification rule does not explicitly state the R/A missions for risk-significant SSCs. Instead, the rule includes deterministic requirements for both safety-related and non-safety-related design features.

The following two sections discuss the steps of the RTNSS process to address the five key elements described above.

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 uses the following five criteria to determine those SSC functions:

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

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

(3) 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 $1x10^{-4}$ each reactor year, and a large release frequency (LRF) of less than $1x10^{-6}$ each reactor year

(4) 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. 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 AP1000 design, combined with the regulatory oversight for identified SSCs, has maintained an acceptable balance between core damage prevention and mitigation. However, it was not used as a criterion for establishing the availability requirements for non-safety-related, defense-in-depth systems.

(5) SSC functions relied upon to prevent significant adverse systems interactions

22.3 Specific Steps in the RTNSS Process

The following specific steps were established for design certification applicants 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. The process also includes adequate treatment of R/A uncertainties, long-term safety operation, and

containment performance. A margins approach is used to evaluate seismic events. In addressing containment performance, the PRA considers the sensitivities and uncertainties in accident progression, as well as inclusion of severe accident phenomena, including explicit treatment of containment bypass. In the PRA, mean values are used to determine the availability of passive systems and the frequencies of core damage and large releases. The process estimates the magnitude of potential variations in these parameters and identifies significant contributors to these variations using appropriate uncertainty and sensitivity analyses. Finally, the RTNSS process calls for an adverse systems interaction study to be performed and its results to be considered in the PRA. Chapter 19 of this report discusses the AP1000 baseline PRA.

22.3.2 Search for Adverse Systems Interactions

The RTNSS process includes systematic evaluation of adverse interactions between the active and passive systems. The results of this analysis are used to initiate design improvements to minimize adverse systems interactions and are considered in developing 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 of this report). The focused PRA results are used in several ways to determine the R/A missions of non-safety-related, risk-significant SSCs.

First, the focused PRA maintains the same scope of initiating events and their frequencies as identified 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 commensurate with their R/A missions.

Second, following an initiating event, the event tree logic of the comprehensive, Level-3 focused PRA will not include the effects of non-safety-related standby SSCs. At a minimum, these event trees will not include the defense-in-depth functions and their support, such as onsite ac power. This will allow the COL applicant 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 $1x10^{-4}$ each reactor year and an LRF of $1x10^{-6}$ each reactor year. The applicant will also evaluate the containment performance, including bypass, during a severe accident. If the applicant determines that non-safety-related SSCs must be added to the focused PRA model to meet the safety goals, these SSCs will be subject to regulatory oversight based on their risk significance.

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

directly impact 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 identification of any combination of non-safety-related SSCs that are necessary to meet NRC regulations, safety goal guidelines, and the containment performance goal objectives. These combinations are based on criteria 1 and 5 in Section 22.2 of this report, for which NRC regulations are the bases for consideration, and criteria 3 and 4 in Section 22.2 of this report, for 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, the applicant will use PRA insights, sensitivity studies, and deterministic methods 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), resolve the long-term safety and seismic issues (criterion 2), and prevent significant adverse systems interactions (criterion 5) are subject to regulatory oversight.

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

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

(2) Add the necessary success paths (an event sequence in the PRA event tree which results in no core damage) with non-safety-related systems and functions to the focused PRA to meet safety goal guidelines, containment performance goal objectives, and NRC regulations. Choose the systems by considering the factors for optimizing the design effects and benefits.

(3) 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 steps described in the previous section of this report, the applicant should determine and documents the functional R/A missions of those active systems needed to meet safety goal guidelines, containment performance goals, and NRC performance requirements. The applicant should also propose regulatory oversights as discussed in Section 22.3.6 of this report. The applicant should repeat the steps described in Sections 22.3.4, 22.3.5, and 22.3.6 of this report to ensure that it selects the most appropriate active systems and associated R/A missions.

As part of this process, the applicant should establish graded safety classifications and graded requirements for based on 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 should conduct the following activities to determine the means of appropriate regulatory oversight for the RTNSS-important non-safety systems:

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

- Review the DCD Tier 2 information to determine whether 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 whether it includes proper short-term availability control mechanisms if required for safety and determined by risk significance.

22.4 Other Issues Related to RTNSS Resolution

SECY-94-084 discussed several other issues related to overall passive plant performance or the performance of specific passive safety systems. The staff tied resolution of these issues to an acceptable resolution of the RTNSS issue. On the basis of the availability of short-term administrative controls for defense-in-depth equipment, as 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 8.5.2.1, and (3) part exemption from GDC 17 for ac offsite power sources as discussed in Section 8.2.3.2 of this report.

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

Westinghouse Commercial Atomic Power (WCAP)-15985, Revision 2, "AP1000 Implementation of the Regulatory Treatment of Nonsafety-Related Systems Process," dated August 2003, describes the applicant's implementation of the RTNSS process for the AP1000. The applicant used this process to determine which non-safety-related systems in the AP1000 should be subject to regulatory treatment and under what conditions that treatment should apply. The implementation of the RTNSS process for the AP1000 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 a study of initiating event frequency. In addition, the applicant evaluated 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.

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 Westinghouse AP1000 PRA report, APP-GW-GL-022, "AP1000 Probabilistic Risk Assessment," provides the detailed results of the focused PRA. The focused PRA evaluation in WCAP-15985, Revision 2, is based on the results from the AP1000 PRA report. Section 19.1.7, "PRA Input to the Regulatory Treatment of Non-Safety-Related Systems (RTNSS) Process," of this report summarizes the staff's evaluation of the focused PRA results. The draft safety evaluation report (DSER) specified that the evaluation described in the following sections is subject to satisfactory closure of Open Item 19.1.10.1-3. Open Item 19.1.10.1-3 identified the need for the applicant to provide all steps in the RTNSS process of using PRA results to identify non-safety-related systems for regulatory oversight as well as the type and level of such oversight. This open item has since been resolved.

22.5.1.1 PRA Event Mitigation Evaluation

Section 2 of WCAP-15985, Revision 2, describes the focused PRA sensitivity studies performed by the applicant 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 function is relied upon in the focused PRA sensitivity studies to allow the calculated CDF and LRF to 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 and during shutdown operation. Similar sensitivity studies are not required for external events because the associated risks were assessed conservatively without credit for non-safety systems to mitigate accidents.

The focused PRA sensitivity studies are 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 2, lists the safety-related systems and functions credited in the focused PRA sensitivity study, as well as the non-safety-related systems and functions that were assumed to fail. Table 2-2 in WCAP-15985, Revision 2, provides a comparison of the summary results for the baseline and focused PRA sensitivity studies assuming (1) failure of all non-safety-related systems, and (2) failure of all non-safety systems, except for the manual diverse actuation system (DAS) controls for the following functions:

- reactor trip
- passive residual heat removal system heat exchanger and in-containment refueling water storage tank gutter valves (air operated)
- core makeup tank isolation valves (air operated)
- automatic depressurization system stages 1, 2, 3 valves (motor operated), and stage 4 valves (squib)

- in-containment refueling water storage tank injection isolation valves (squib)
- containment recirculation isolation valves (squib)
- passive containment cooling system water drain valves (air and motor operated)
- containment isolation valves (air operated)
- hydrogen igniters

Chapter 50 of the AP1000 PRA report describes the detailed focused PRA sensitivity studies. Based on the summary results provided in Table 2-2 of WCAP-15985, Revision 2, case 1 of the focused PRA (assumes failure of all non-safety system mitigation functions) results in an LRF above the safety goal guideline of $1x10^{-6}$. However, case 2 of the focused PRA (assumes taking credit of the DAS manual controls) results in both the CDF and the LRF meeting the safety goal guidelines of $1x10^{-4}$ and $1x10^{-6}$, respectively.

Since the manual controls of the DAS are credited to meet the LRF safety goal, these controls are identified as RTNSS-important and subject to regulatory oversight. In accordance with 10 CFR 50.36(c)(2)(ii)(D), Criterion 4, limiting conditions for operation must be established in the plant's TS for an SSC which 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 limiting condition for operation, actions and surveillance requirements on the manual controls of the DAS. In addition, the AP1000 design reliability assurance program (D-RAP) in DCD Tier 2, Table 17.4-1, as well as the AP1000 inspections, tests, analyses, and acceptance criteria (ITAAC) in Tier 1, Section 2.5.1, includes the DAS. The quality assurance guidance in Generic Letter (GL) 85-06, "Quality Assurance Guidance for ATWS Equipment That is Not Safety-Related," is applicable to the non-safety-related equipment encompassed by the ATWS rule. Section 4.1 of WCAP-15985, Revision 2, states that certain DAS functions and the associated DAS power supplies are needed to meet the requirements of the ATWS rule. In the DSER, the staff stated that the evaluation of the quality assurance (QA) associated with the power supplies to DAS was subject to the resolution of DSER Open Item 20.7-2, which stated that the applicant did not clearly describe that the QA controls guidance of GL 85-06 applied to the DAS power supplies. As discussed in the staff's evaluation of GL 85-06 in Section 20.7 of this report, Open Item 20.7-2 is resolved based on the fact that Sections 10.3-1 and 10.3.3, respectively, of WCAP-15985, Revision 2, state that the QA guidance of GL 85-06 is applicable to DAS and the non-Class 1E dc and UPS systems because of the ATWS mitigation functions.

Section 2.3 of WCAP-15985, Revision 2, 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), the importance of non-safety-related SSCs in an initiating event frequency, and the uncertainties associated with hydrogen standing flames. This PRA uncertainty evaluation determines which non-safety-related SSCs should be identified as RTNSS-important to add margin to compensate for the PRA uncertainties. In certain situations, no non-safety-related SSCs can directly compensate for the PRA uncertainties. In

these cases, margin is provided in the PRA by adding regulatory oversight on those non-safety-related SSCs that have been identified as being able to improve the results of the PRA sensitivity studies for other sequences. As a result of this evaluation, the following non-safety-related SSCs are designated as 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 protection and safety monitoring system software uncertainty)

- injection capability of the normal residual heat removal system and onsite power supplies (provides margin for ADS/IRWST injection/containment recirculation valve reliability uncertainty and long-term cooling thermal-hydraulic uncertainty)

- hydrogen igniters (provides margin for uncertainty in hydrogen burn consequences)

Section 22.5.9 of this report 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, Revision 2, describes the evaluation performed by the applicant 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. The following 11 categories of initiating events were identified for at-power and shutdown conditions.

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 unavailability of non-safety-related SSCs to the initiating event frequencies is based on the following three criteria:

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

(2) Does the unavailability of the non-safety-related SSCs significantly affect the calculation of the initiating event frequency?

(3) Does the initiating event significantly affect the CDF and the 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 that occur at power. In WCAP-15985, Revision 2, the applicant states that the results of probabilistic evaluations indicate 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 a non-loss-of-coolant accident transient associated with the main feedwater flow (turbine trip, spurious reactor trip), which had a CDF of 1.4 percent and a LRF of 7.5 percent. Therefore, the non-safety-related SSCs required for normal at-power operation are important with respect to the effect of this initiating event. These non-safety-related secondary plant systems associated with this event include the following:

- 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 would be subject to regulatory oversight through investment protection short-term availability controls. However, rather than proposing short-term availability control for these systems, the applicant considered design improvements of various AP1000 design features that affect the operation of these systems with increased reliability so as to reduce initiating event frequency. As discussed in Section 10.3.2 of WCAP-15985, Revision 2, the design improvements include the improvements in the main feedwater system, the use of a digital steam generator water level system, and the use of a digital turbine electro-hydraulic control system. 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 resulting in increased reliability would reduce the initiating event frequencies.

The 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 challenge the plant's normal operation. Because the regulatory oversight of the RTNSS-important non-safety-related SSCs is intended to ensure the reliability and availability 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 by the DCD design details and by 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, Revision 2, the applicant concludes that the results of probabilistic evaluations demonstrate that 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, for events at shutdown. 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
- normal residual heat removal system
- component cooling water system
- service water system

The availability controls apply only during reduced reactor coolant system inventory operations occurring at 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, Revision 2, 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 an SRM 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 depressurization of the reactor coolant system (RCS), passive safety system injection, containment isolation, passive containment cooling, and ex-vessel coolable geometry. Based on the evaluation of the ability of

non-safety-related SSCs to meet 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 CCFP. The staff also identified that the RV insulation design is required for successful cooling of the external reactor vessel.

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, the applicant 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. The applicant determined that short-term availability control for the RV insulation system is unnecessary because the system is included as a risk-significant SSC in the reliability assurance program. DCD Tier 1, Section 2.2.4 includes the important acceptance criteria associated with the insulation design.

DCD Tier 2, Section 6.2.4 describes the hydrogen igniters. The hydrogen igniters are subject to the AP1000 D-RAP and are included in DCD Tier 1, Section 2.3.9. The hydrogen igniters are also subject to short-term availability controls, as described in DCD Tier 2, 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 that they are acceptable.

22.5.4 Deterministic ATWS and SBO Evaluation

In Sections 4 and 5 of WCAP-15985, Revision 2, the applicant provides deterministic evaluations regarding the 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:

- the diverse actuation system functions of reactor trip, turbine trip, and passive residual heat removal during power operation

- the non-class-1E dc power and uninterruptible power supply system, which provides power to the diverse actuation system

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

In Section 10.2 of WCAP-15985, Revision 2, the applicant summarizes the mission statements of the DAS and the non-class 1E dc power and uninterruptible power supply system for ATWS events. These non-safety-related systems are included in DCD Tier 2, Table 16.3-2, items 1.1 and 3.4, regarding short-term availability controls.

The staff has determined that the applicant 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 the RTNSS process, is acceptable.

22.5.5 Evaluation of Adverse Systems Interactions

In Section 8 of WCAP-15985, Revision 2, the applicant considered potential adverse systems interactions where non-safety-related systems may adversely interact with the safety-related systems. 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. The staff reviewed WCAP-15992, Revision 1, to determine if the applicant acceptably evaluated adverse systems interactions (ASIs) that could occur in the AP1000. The following three types of interactions were considered:

- Functional Interactions - interactions among the passive safety systems, and interactions between passive safety systems and active non-safety-related systems

- Human Commission Errors - interaction resulting from operator errors of commission

- Spatial Interactions - interactions that could occur as a result of equipment location in the plant

An ASI is a system interaction that produces an undesirable result (i.e., when the operation and/or performance of an "initiating" system adversely affects the operation and/or performance of a safety-related "affected" system as it performs its safety function). Section 2 of WCAP-15992, Revision 1, provides a detailed systematic evaluation of the functional interactions ASIs among the passive safety systems, and between the passive safety systems and active non-safety systems. The systematic evaluation includes a matrix of the potential initiating systems and the potential affected systems and components, and an evaluation of the potential interactions for each combination of the systems and features in the matrix. An evaluation is made on important interactions to identify any adverse effects on the critical safety functions, such as safety injection and core cooling, and confirm that the adverse interaction

has been addressed and evaluated as part of the plant design process, through the various design, analysis, and testing mechanisms. These mechanisms include detailed design analyses and evaluation; separate effects tests and integral system tests; design basis safety analyses; PRA success criteria analyses; and supporting emergency response guideline (ERG) analyses. Based on its evaluation, the applicant did not identify any functional-interaction ASIs that have not been evaluated in the design process.

Since the AP1000 plant is designed to minimize the reliance on operator actions to mitigate accident, cognitive operator actions, or human commission errors rather than omission errors, are deemed to be the source of potential adverse systems interactions. Section 3 of WCAP-15992, Revision 1, provides an evaluation of potential human commission errors that may cause ASIs. In its examination, three questions were asked for each candidate ASI:

- Is there an opportunity for a commission error?
- Are there safeguards against a commission error?
- Is the effect of ASI already modeled in the PRA?

The responses to these questions allow the ASI to be classified as follows: (1) there is no credible concern for human commission error for this ASI to occur; (2) there is credible way for this human error to occur, but the overall effect is insignificant because there is sufficient time to recover; (3) the error is credible but is already modeled in the PRA or is bounded by other failures or success criteria modeled in the PRA; and (4) the error is credible and is not modeled in the PRA. Based on its evaluation, the applicant identified only one category 4 situation in the spent fuel pool cooling system connection to the fuel transfer canal, which is a normally closed and administratively controlled valve, and a credible maintenance operation error potential can be postulated but was not modeled in the PRA. However, spent fuel pool accidents are not deemed to be risk significant and are not studied in the PRA since their effect would develop slowly with less fission product. Overall the evaluation did not identify any human commission error that might cause significant systems interactions and might be of significant concern to plant risk. The evaluation of the human errors system interactions tied to the applicant's ERG in assessing operator actions to preclude potential ASIs that could arise as a result of human errors.

The spatial interactions are interactions resulting from the presence of two or more systems in proximate locations regarding the effects of fire, flood, pipe break, missile hazard, and seismic events. These spatial interactions are addressed in various sections in DCD Tier 2, Section 3.4, "Water Level (Flood) Design;" Section 3.5, "Missile Protection;" Section 3.6, "Protection Against the Dynamic Effects Associated with the Postulated Rupture of Piping;" Section 3.7, "Seismic Design;" and Section 9.5.1, "Fire Protection System." Safety-related systems are required to be protected from the effects of failures in the safety-related and nonsafety-related systems; and are located within the containment, containment shield building, and auxiliary building. The restricted extent of the safety-related systems and components limits the number of nonsafety-related systems that need to be considered as possible source of adverse interactions. In addition to separation of safety-related and nonsafety-related systems, one of the important features providing protection is the exterior and interior structural walls, floors and roof of the auxiliary building and the structure of the containment shield building.

The staff has reviewed functional interactions, human commission interactions, and spatial interactions described in WCAP-15992, Revision 1, and concluded that there are no ASIs that have not been properly addressed in the design process and therefore require RTNSS controls. The staff's evaluation of ASIs is also reflected in the review of Unresolved Safety Issue A-17, "System Interactions in Nuclear Power Plants," in Section 20.2 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 safe-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 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. In this document, the staff took the position that post-72-hour actions related to all design-basis events must 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 Appendix A to 10 CFR Part 50, General Design Criteria (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, Revision 2, the applicant describes the post-72-hour actions for the AP1000. 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
- post-accident 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 support extended operation of the passive safety systems. These extended supports include the following:

- electrical power to supply the post-accident and spent fuel pool monitoring instrumentation provided by ancillary diesel generators that connect to safety-related electrical connections

- makeup water to the passive containment cooling system water storage tank to maintain external containment cooling water flow and to the spent fuel pool to maintain spent fuel cooling provided by a passive containment cooling system recirculation pump powered by an ancillary diesel generator connected to a safety-related makeup connection

- open doors and ancillary fans to ventilate and cool 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, Revision 2, specifies the short-term availability controls for this 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 equipment required for post-72-hour actions is onsite, the equipment meets the requirements of Appendix A to 10 CFR Part 50, 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 Non-Safety-Related SSCs

According to the RTNSS process, non-safety-related SSCs relied upon to meet the criteria described in Section 22.2 of this report are designated as RTNSS-important and are subject to regulatory oversight. As described in Sections 22.5.1 through 22.5.6 of this report, the applicant has identified the RTNSS-important SSCs. In Section 10 of WCAP-15985, Revision 2, the applicant identifies the missions of these important non-safety systems and recommends regulatory oversight.

Section 10.2 of WCAP-15985, Revision 2, provides mission statements of the important non-safety-related SSCs, which are similar to those identified in Sections 2 through 9 of WCAP-15985, Revision 2, (Sections 22.5.1 through 22.5.6 of this report). The following is a summary of each.

- Manual actuations of the diverse actuation system provide the capability to manually actuate reactor trip and engineered safety feature functions during at-power and shutdown modes. (TS 3.3.5)

- Actuation of the diverse actuation system during anticipated transients without scram provides the capability to automatically (1) actuate reactor and turbine trip and (2) initiate passive residual heat removal under conditions indicative of an ATWS during power operation. (1.1)

- Actuation of the engineered safety features of the diverse actuation system automatically actuates passive safety features during at-power and shutdown modes. (1.2)

- Low-pressure reactor coolant system injection by the normal heat removal system provides means of low-pressure reactor coolant system injection from the cask loading pit following actuation of the automatic depressurization system during at-power and shutdown conditions. (2.1)

- Shutdown cooling by the normal residual heat removal system provides shutdown decay heat removal during open shutdown conditions of the reactor coolant system. (2.2)

- The component cooling water system provides cooling to support shutdown decay heat removal by the normal residual heat removal system during shutdown conditions with the reactor coolant system open. (2.3)

- The service water system provides cooling to support shutdown decay heat removal by the component coolant water system during shutdown conditions with the reactor coolant system open. (2.4)

- Makeup functions of the passive containment cooling system water and spent fuel pool provide the capability to transfer water from the passive containment cooling system ancillary water storage tank to the passive containment cooling water system water storage tank and the spent fuel pool in all modes of plant operation in support of post-72-hour operation of passive safety systems. (2.5)

- Ancillary fans in the main control room provide cooling to support post-72-hour habitability of the main control room during all modes of plant operation. (2.6)

- Instrumentation room fans provide cooling of the 1E instrumentation rooms to support post-72-hour accident 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)

- The onsite ac power supply system provides a backup source of electric power to onsite equipment needed to provide actuation of the protection and monitoring system and to support operation of the normal residual heat removal system during all modes of plant operation following a loss of offsite power. (3.1)

- The offsite ac power system provides electric power to onsite equipment needed to support decay heat removal operation during shutdown conditions with the reactor coolant system open . (3.2)

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

- The non-class 1E dc and uninterruptible power supply system provides electrical power to the diverse actuation system and actuation components to actuate reactor and turbine trip and initiate passive residual heat removal under conditions indicative of an anticipated transient without scram during power operation. (3.4)

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

22.5.8 Technical Specifications

Section 10.4 of WCAP-15985, Revision 2, 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 assuming failure of the non-safety mitigation functions of the non-safety-related SSCs, the LRF will exceed the safety goal guideline of $1x10^{-6}$ per reactor year. However, by crediting the DAS manual controls in the focused PRA, the CDF and LRF are reduced, thereby meeting 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 Criterion 4 of 10 CFR 50.36(c)(2)(ii)(D). Section 10.4 of WCAP-15985, Revision 2, and AP1000 TS 3.3.5, “Diverse Actuation System (DAS) Manual Controls,” describe the proposed TS for DAS manual controls. The staff concludes that TS 3.3.5 provides proper regulatory oversights for the DAS manual controls and is acceptable 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, Revision 2, proposed a means for implementing RTNSS controls in the form of short-term administrative availability controls for the SSCs summarized in Section 22.5.7 of this report, 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, Revision 2, is incorporated in DCD Tier 2, Table 16.3-2 of the same title. These short-term availability controls of the RTNSS-important SSCs resemble the AP600 short-term availability controls format, which had been extensively evaluated and found acceptable during the AP600 design

certification application review. The administrative controls are formatted similar to the 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. 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 limiting condition for operation (i.e., they are not installed instrumentation used to detect and indicate a significant abnormal degradation of the reactor coolant pressure boundary (Criterion 1); they are not a process variable, design feature, or operating restriction that is an initial condition of a design-basis accident or transient analysis (Criterion 2); they are 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 they are not an SSC shown to be significant to public health and safety based on operating experience or a PRA (Criterion 4)). In addition, these RTNSS-important SSCs are included in (1) the AP1000 D-RAP, as described in DCD Tier 2, Section 17.4, "Design Reliability Assurance Program," and DCD Tier 2, Table 17.4-1, "Risk-Significant SSCs Within the Scope of D-RAP," and (2) the ITAAC, as described in DCD Tier 1 Information.

Therefore, the staff finds the RTNSS administrative controls in DCD Tier 2, Table 16.3-2 acceptable. In DCD Tier 2, Section 16.3.2, "Combined License Information," the applicant stated that COL applicants referencing AP1000 will develop a procedure to control the operability of investment protection SSCs in accordance with DCD Tier 2, Table 16.3-2. The staff identifies this as COL Action Item 22.5.9-1.

22.6 Quality Assurance and Reliability Assurance Programs

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 RV insulation system was identified as an RTNSS item, but not subject to short-term availability control. DCD Tier 2, Section 17.3 describes the quality assurance program and DCD Tier 2, Table 17-1 describes the quality assurance program requirements for risk-significant RTNSS SSCs. 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 D-RAP, including those RTNSS-important SSCs listed in Section 22.5.7 of this report and the RV insulation system. The staff concludes that including the RV insulation system under D-RAP will provide sufficient regulatory oversight, as discussed in Section 22.5.2 of this report.