C.IV.10. Regulatory Treatment of Non-Safety Systems

COL applicants that do not reference a certified design and are proposing a design that includes passive safety systems should define the active systems relied upon for defense-in-depth and necessary to meet passive advanced light water reactor (ALWR) plant safety and investment protection goals. This process is referred to as regulatory treatment of non-safety systems (RTNSS). The background and the implementation of the RTNSS process is provided below. The RTNSS process is considered for advance reactor designs on a case-by-case basis.

For COL applicants that reference a certified design, the certification will have addressed the implementation of the RTNSS process.

This information is based on NUREG-1793, Volume 3, "Final Safety Evaluation Report Related to Certification of the AP1000 Standard Plant Design," issued in September 2004.

C.IV.10.1 *Background*

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. These active systems are the first line of defense in reducing challenges to the passive systems in the event of transients or plant upsets.

In 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 passive plant design as non-safety related, credit is generally not taken for the active systems in the licensing design-basis accident analyses that are described in Chapter 15 of the generic design control document for the certified designs (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 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 because of 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 were designed to ensure that the pressure differential across these valves would be small during normal plant operation. The design certification 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 NRC 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.

C.IV.10.2 ***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[1]

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

[1] This issue was discussed in detail in SECY-93-087. 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.

C.IV.10.3 *Specific Steps in the RTNSS Process*

The following specific steps were established for design certification applicants to implement the process described above. These steps would be applicable to COL applicants not referencing a certified design.

C.IV.10.3.1 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.

C.IV.10.3.2 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.

C.IV.10.3.3 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 C.IV.10.2 of this guide). 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 1×10^{-4} each reactor year and an LRF of 1×10^{-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.

C.IV.10.3.4 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 C.IV.10.2 of this guide, for which NRC regulations are the bases for consideration, and criteria 3 and 4 in Section C.IV.10.2 of this guide, for which PRA methods are the bases for consideration. To address the long-term safety issue in criterion 2 of Section C.IV.10.2 of this guide, the applicant should 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.

C.IV.10.3.5 Non-Safety-Related System Reliability/Availability Missions

Upon completion of the selection steps described in the previous section of this guide, 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 C.IV.10.3.6 of this guide. The applicant should repeat the steps described in Sections C.IV.10.3.4, C.IV.10.3.5, and C.IV.10.3.6 of this guide 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 based on the importance to safety of their functional R/A missions.

C.IV.10.3.6 Regulatory Oversight Evaluation

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

- Review the final safety analysis report (FSAR), 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 FSAR 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 FSAR information to determine whether it includes proper short-term availability control mechanisms if required for safety and determined by risk significance.

C.IV.10.4 *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 COL applicant not referencing a certified design should address these issues as applicable.