

## 17 QUALITY ASSURANCE

### 17.1 Quality Assurance During the Design and Construction Phase

In the AP1000 Design Control Document (DCD), Section 17.5, "Combined License Information Items," Westinghouse Electric Company (Westinghouse or the applicant) states that the Combined License (COL) applicant will address its quality assurance (QA) program for the design phase, as well as its QA program for procurement, fabrication, installation, construction and testing of structures, systems, and components (SSCs) in the facility. When completing the detailed design during the COL design phase, the COL applicant is required to submit its design phase QA program for staff review. This will be in addition to the staff review of the COL applicant's QA program for construction of the facility. This is described as a COL information item in DCD Tier 2 Section 17.5. The NRC staff agrees that this part of the QA program can be the COL applicant's responsibility and that making this a COL item in DCD Tier 2 Section 17.5 is acceptable. This is COL Action Item 17.1-1.

### 17.2 Quality Assurance During the Operations Phase

In DCD Tier 2 Section 17.5, "Combined License Information Items," the applicant states that the COL applicant will address its QA program for operations. This is described as a COL information item in DCD Tier 2 Section 17.5. The NRC staff agrees that this part of the QA program can be the COL applicant's responsibility and that making this a COL item in DCD Tier 2 Section 17.5 is acceptable. This is COL Action Item 17.2-1.

### 17.3 Quality Assurance During the Design Phase

Title 10 of the Code of Federal Regulations (10 CFR) Section 52.47(a)(1)(i) requires, in part, that an application for design certification contain technical information which is required of applicants for construction permits and operating licenses by 10 CFR Part 50 and its appendices. The requirements of 10 CFR 50.34(a)(7) state, in part, that an applicant for a construction permit provide a description of the QA program to be applied to the design of SSCs. Further, the description of the QA program shall include a discussion of how the applicable requirements of 10 CFR Part 50, Appendix B, "Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants," will be satisfied. Therefore, the staff reviewed the QA program used during the AP1000 design phase. Specific guidance for the conduct of this review is contained in NRC technical report designation (NUREG)-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants," Section 17.3, "Quality Assurance Program Description."

### 17.3.1 General

Revision 0 of DCD Tier 2 Section 17.3.1 for the AP1000 design outlines the QA program applicable to the design, procurement, fabrication, inspection, and/or testing of items and services for the AP1000 project. The design for the AP1000 is based upon employing the design of AP600 to the maximum extent possible. As a result, the applicant stated that a continuous QA program spanning the AP600 design as well as the AP1000 design has been used. Prior to March 31, 1996, activities for the AP600/AP1000 design program were performed in accordance with Topical Report WCAP-8370, "Westinghouse Energy Systems Business Unit/Power Generation Business Unit Quality Assurance Plan." Since March 31, 1996, activities affecting the quality of items and services for the AP1000 project during design, procurement, fabrication, inspection, and/or testing have been performed in accordance with the quality plan described in "Westinghouse Energy Systems Business Unit - Quality Management System." Since that time, the quality management system (QMS) has been maintained as the quality plan for the AP1000 program and subsequent revisions have been submitted to and accepted by the NRC staff, as meeting the requirements of 10 CFR Part 50, Appendix B. The latest revision to the Westinghouse QMS was implemented on October 1, 2002, after the NRC staff found that QMS, Revision 5, continued to meet the requirements of 10 CFR Part 50, Appendix B, as documented in an NRC evaluation letter dated September 13, 2002, from W. Ruland to H. Sepp (ADAMS Accession No. ML022540895).

### 17.3.2 Evaluation

During the review of the AP1000 design QA program, the staff identified five areas where additional information was required to complete the QA program description review: (1) QA controls for non-safety related risk significant SSCs identified by the regulatory treatment of non-safety systems (RTNSS) process defined in SECY 95-132, (2) implementation of QA controls for AP1000 design testing, (3) implementation of the Westinghouse QMS for AP1000 design activities, (4) basis for certain exceptions to quality related regulatory guides, and (5) missing QA related information in DCD Tier 2 Section 17.6, "References." By letters dated September 19, 2002, and April 16, 2003, the staff requested additional information to complete this review. The status and pending resolution of each of these five areas is discussed below.

- QA Controls for SSCs Identified by the RTNSS Process

The NRC staff performed a review of AP1000 DCD Tier 2 Section 17.3, "Quality Assurance During Design, Procurement, Fabrication, Inspection and/or Testing of Nuclear Power Plant Items." The NRC found that the applicant revised DCD Tier 2 Section 17.3 to remove SSCs identified by the RTNSS process from the scope of non-safety related quality control requirements outlined in DCD Tier 2 Table 17-1. Although the NRC concluded that the Table 17-1 quality controls were adequate for risk-significant non-safety related SSCs, the staff determined that not including RTNSS related SSCs within the scope of DCD Tier 2 Section 17.1 and Section 17.3 of the AP1000 design was not acceptable.

In Request for Additional Information (RAI) 260.001, the NRC requested the applicant to either justify removal of SSCs identified by the RTNSS process from DCD Tier 2 Section 17.3 or maintain the SSCs identified by the RTNSS process within the scope of the non-safety related QA controls outlined in Table 17-1. In Revision 3 to DCD Tier 2 Section 17.3, the applicant placed SSCs identified by the RTNSS process within the scope of Table 17-1, "QA Controls". The NRC staff found that this meets the guidance in SECY 95-132 and standard review plan (SRP) Section 17.3 and is acceptable.

- QA Issues Associated with AP1000 Design Testing

The NRC staff plans to perform a QA test control implementation inspection to determine if additional testing activities performed at the test facility associated with the AP1000 design are accomplished, in accordance with the Westinghouse 10 CFR Part 50, Appendix B, QA program as described in Chapter 17 of the AP1000. The NRC will review QA provisions applicable to the identified test facility as described in the applicable AP1000 test project quality plan and test procedures. In particular, the team plans to examine the areas covered by the QA program to confirm that the test activities were accomplished under suitably controlled conditions by properly trained personnel and that pertinent test data, used to furnish documentary evidence of activities, affecting quality were properly recorded and maintained. For additional details, see Chapter 21 of this report. This is Open Item 17.3.2-1.

- Implementation of QA Program for AP1000 Design

Westinghouse stated that a project-specific quality control plan was used to implement the requirements of the Westinghouse QMS program. The staff plans to conduct an inspection of the implementation of the project-specific quality plan to verify that design activities conducted for the AP1000 project complied with the Westinghouse QMS and the requirements of 10 CFR Part 50, Appendix B. As discussed in this report Chapter 20, "Generic Issues," the NRC staff will also address the implementation of QA requirements 10 CFR 50.34(f)(3) and NUREG-0933, Item I.F.2, during this inspection. This is DSER Open Item 17.3.2-2.

- Compliance with QA Related RGs

The NRC staff reviewed DCD Tier 2 Section 1, Appendix 1A, "Conformance with Regulatory Guides," and noted that the applicant has taken exceptions to regulatory positions contained in several QA related regulatory guides (RGs). Specifically, the applicant identified exceptions to quality control guidance contained in the following five RGs:

- (1) RG 1.28, "Quality Assurance Program Requirements (Design and Construction),"
- (2) RG 1.37, "Quality Assurance Requirements for Cleaning of Fluid Systems and Associated Components of Water Cooled Nuclear Power Plants,"

- (3) RG 1.38, "Quality Assurance Requirements for Packaging, Shipping, Receiving, Storage and Handling of Items for Water-Cooled Nuclear Power Plants,"
- (4) RG 1.39, "Housekeeping Requirements for Water-Cooled Nuclear Power Plants," and
- (5) RG 1.54, "Quality Assurance Requirements for Protective Coatings Applied to Water Cooled Nuclear Power Reactors."

The evaluation of the exceptions to each of these RGs is discussed below.

Exception to RG 1.28: As noted previously in this chapter, in DCD Tier 2 Section 1, Appendix 1A, the applicant took exception to record retention recommendations in RG 1.28. Specifically, RG 1.28, Regulatory Position C.2, Quality Assurance Records, states, in part, that programmatic nonpermanent records should be retained for at least 3 years. For programmatic nonpermanent records, the retention period should be considered to begin upon completion of the activity. In addition, RG 1.28 states that product and programmatic nonpermanent records should be retained at least until the date of issuance of the full power operating license of the unit. Under 10 CFR Part 52, issuance of a COL is comparable to issuance of a full power operating license under 10 CFR Part 50. The applicant stated that because a definitive schedule for obtaining a full power operating license does not exist, the records retention plan is keyed to the final design approval. The applicant stated that a 3 year programmatic records retention period will be initiated starting on the date that NRC issues an AP1000 final design approval. The NRC staff determined that this exception to RG 1.28 may not be acceptable since programmatic nonpermanent records could be discarded 3 years after issuance of a final design approval; therefore, these records may not be available to a future COL applicant. The NRC staff requested additional information to assess the basis for not retaining nonpermanent records until a COL is issued. The applicant should provide a list of the specific records types that they are proposing to discard after 3 years. The applicant should also provide additional justification for discarding each of these record types after final design approval. This information was requested from the applicant through RAI 260.007. This is DSER Open Item 17.3.2-3.

Exceptions to RGs 1.37, 1.38, and 1.39: RG 1.37, 1.38, and 1.39 reference use of American National Standards Institute (ANSI) standards N45.2-1, N45.2-2, and N45.2-3. However, the applicant referenced the requirements contained in American Society of Mechanical Engineers (ASME) quality standards NQA-1 and NQA-2 rather than these ANSI standards. The requirements in ANSI N45.2-1, N45.2-2, and N45.2-3 have been updated and incorporated into ASME quality standards NQA-1 and NQA-2. Because the staff considered incorporation of these ANSI standards into the guidance contained in ASME NQA-1 and NQA-2 to be enhancements, the NRC staff determined that these RG exceptions are acceptable. The staff also noted that these three RGs are associated with COL activities. Therefore, the staff requested the applicant to annotate the discussion of RG 1.37 and RG 1.38 in DCD Tier 2 Appendix 1A to indicate the need for a COL applicant to address implementation of these RGs similar to the annotation

used for RG 1.39. Specifically, the applicant should add the following statement in DCD Appendix 1A to the exceptions taken in RGs 1.37 and 1.38: "See Section 17.5 for COL Information items." In Revision 4 of DCD Tier 2 Appendix 1A, the applicant added the reference to the COL information in DCD Tier 2 Section 17.5. The NRC staff finds that the exceptions to RGs 1.37, 1.38 and 1.39 are acceptable.

Exception to RG 1.54, Revision 1: The NRC staff found that the applicant took exception to RG 1.54, Revision 1. As described in DSER Section 6.1.2.1, "Protective Coatings," the staff determined that the applicant met the QA requirements of 10 CFR Part 50, Appendix B, for safety related protective coatings inside containment. However, some coatings inside containment are non-safety related in the AP1000 design. The applicant addressed this exception to RG 1.54 in their response to RAI 281.001. See Section 6.1.2.1, "Protective Coatings," of this report, for additional details. The NRC staff found that this exception to RG 1.54 is acceptable.

- Missing QA Related Information in DCD Tier 2 Section 17.6, References

The NRC staff also noted that in DCD Tier 2 Section 17.6, "References," the applicant did not reference the following documents discussed in DCD Tier 2 Section 17.3:

Westinghouse Electric Company Quality Management System (QMS),  
Revision 5, dated October 1, 2002.

WCAP-15985, "AP1000 Implementation of the Regulatory Treatment of  
Nonsafety-Related Systems Process," Revision 1, dated April 2003

Westinghouse should add these references to DCD Tier 2 Section 17.6. In addition, there is no reference to a project specific quality plan for the AP1000 design similar to Reference 4, WCAP-12600, "AP600 Advanced Light Water Reactor Design Quality Assurance Program Plan," Revision 4 dated January 1998. This information was requested from Westinghouse in RAI 261.008. This is DSER Open Item 17.3.2-4.

### 17.3.3 Conclusions

The staff determined that Westinghouse maintained an NRC reviewed and approved QA program that complied with the requirements of 10 CFR Part 50, Appendix B. Additionally, Westinghouse specified appropriate QA controls for risk-significant non-safety related SSCs identified by the RTNSS process. The staff identified two DSER open items associated with the inspection of Westinghouse's QA program implementation for design and testing activities, one open item on an exception to a QA related RG, and one open item on clarifications to references in DCD Tier 2 Section 17.6, "References."

### 17.4 Reliability Assurance Program During the Design Phase

The requirements for a design certification reliability assurance program (RAP) are outlined in SECY-95-132, "Policy and Technical Issues Associated with the Regulatory Treatment of

Non-Safety Systems (RTNSS) in Passive Plant Designs," dated May 22, 1995. In the June 28, 1995, staff requirements memorandum to SECY 95-132, the Commission approved incorporation of the design-specific RAP requirements into the design certification rulemaking for the associated design. The purposes of the RAP are to provide reasonable assurance that (1) an advanced reactor is designed, constructed, and operated in a manner that is consistent with the assumptions and risk insights for risk significant SSCs; (2) the risk-significant SSCs do not degrade to an unacceptable level during plant operations; (3) the frequency of transients that challenge advanced reactor SSCs are minimized; and (4) risk-significant SSCs function reliably when challenged.

The RAP for advanced reactors is implemented in two stages. The first stage, the design RAP (D-RAP) applies before the initial fuel load while the second stage, the operational RAP (O-RAP), applies to reliability assurance activities for the operations phase of the plant life cycle. The NRC staff reviews the D-RAP during design certification, while the O-RAP is reviewed during the COL stage.

The NRC staff drafted SRP Section 17.4, "Reliability Assurance Program," dated April 1996, to provide review guidance for the review of reliability assurance programs. The NRC staff's evaluation of the Westinghouse AP1000 RAP is based on the staff positions discussed in SECY 95-132 and the guidance contained in Draft SRP Section 17.4. An application for advanced reactor design certification or a combined operating license must contain the following:

- (1) the description of the RAP used during the design that includes scope, purpose, objectives and essential elements of the D-RAP;
- (2) the process used to evaluate and prioritize the structures, systems, and components in the design based on their degree of risk significance;
- (3) a list of the structures, systems, and components designated as risk-significant; and,
- (4) for those structures, systems, and components designated as risk significant: (i) a process to determine dominant failure modes that considered industry experience, analytical models, and applicable requirements; and (ii) key assumptions and risk insights from probabilistic, deterministic, or other methods that considered operations, maintenance, and monitoring activities.

The NRC staff reviewed the proposed D-RAP for the AP1000 design using the guidance contained in draft SRP Section 17.4 and SECY 95-132. The NRC staff also reviewed information from the AP1000 probabilistic risk assessment (PRA) Chapter 50, "Importance and Sensitivity Analysis," deterministic methods and expert judgement from all chapters of the DCD to evaluate whether all risk significant SSCs had been identified for inclusion in the D-RAP for the AP1000 design.

### 17.4.1 General

In Revision 4 of DCD Section 17.4.1, Westinghouse stated that the D-RAP, as shown in Figure 17.4-1, is implemented in three phases. The first phase, the Design Certification phase, defines the overall structure of the AP1000 D-RAP, and implements those aspects of the program which are applicable to the design process. During this phase, risk-significant structures, systems, and components (SSCs) are identified for inclusion in the program using probabilistic, deterministic, and other methods. Phase II, the post-design certification process, develops component maintenance recommendations for the plant's operations and maintenance activities for identified SSCs. The third phase is the site-specific phase, which introduces the plant's site-specific SSCs to the D-RAP process. Phase I is performed by the designer. Phases II and III are the responsibility of the COL applicant.

The NRC staff determined that the general description of RAP phases in DCD Tier 2 Section 17.4-1 meets the intent of the guidance in SECY 95-132 and the acceptance criteria in Draft SRP, Section 17.4, "Reliability Assurance Program." Therefore, the general description of the D-RAP phases is acceptable.

### 17.4.2 Scope

In DCD Tier 2 Section 17.4.2, Westinghouse states:

The D-RAP includes a design evaluation of the AP1000 and identifies the aspects of plant operations, maintenance, and performance monitoring pertinent to risk-significant SSCs. In addition to the PRA, deterministic tools, industry sources, and expert opinion are utilized to identify and prioritize those risk significant SSCs.

The staff reviewed the AP1000 scope, purpose, objectives, and essential elements of the D-RAP in accordance with SECY 95-132 and draft SRP Section 17.4.

The NRC staff also reviewed the scope of SSCs under the D-RAP for the AP600 design and the scope of SSCs under the D-RAP for the AP1000 design to evaluate their differences. The NRC staff found that the scope of SSCs within the D-RAP for the two designs are very similar. However, the D-RAP for the AP1000 design added the following risk significant component functions:

- Compressed and Instrument Air System (CAS) Air Compressor Transmitter
- Passive Containment Cooling System Diverse (3<sup>rd</sup>) Motor Operated Drain Isolation Valve function
- In-Containment Refueling Water Storage Tank (IRWST) Vents
- Normal Residual Heat Removal Valve V055 function
- Feedwater Isolation Valves

The D-RAP for the AP1000 design also removed Passive Core Cooling condensate sump recirculation valve automatic open function and normal valve position and revised the instrumentation and control (I&C) terminology for some I&C systems (e.g., the plant protection

subsystem replaces reactor trip and engineered safety features (ESF) subsystems). The scope of SSCs within the RAP for the AP1000 design is discussed in the resolution of RAIs 260.002 and 260.003. For additional details, see Section 17.4.7 of this report. The NRC staff finds that DCD Tier 2 Section 17.4.2 is consistent with the provisions used to determine the scope of risk significant SSCs in the D-RAP in SECY 95-132 and the acceptance criteria in draft SRP Section 17.4, RAP; therefore, the scope of the D-RAP for the AP1000 design is acceptable.

### 17.4.3 Design Considerations

In DCD Section 17.4.3, Design Considerations, Westinghouse states:

As part of the design process, risk-significant components are evaluated to determine their dominant failure modes and the effects associated with those failure modes. For most components, a substantial operating history is available which defines the significant failure modes and their likely causes.

The identification and prioritization of the various possible failure modes for each component lead to suggestions for failure prevention or mitigation. This information is provided as input to the Combined License applicant's O-RAP.

The design reflects the reliability values assumed in the design and PRA as part of procurement specifications. When an alternative design is proposed to improve performance in either area, the revised design is first reviewed to provide confidence that the current assumptions in the other areas are not violated. When a potential conflict exists between safety goals and other goals, safety goals take precedence.

The NRC staff finds that these design considerations in DCD Section 17.4.3 are an essential element for identifying risk significant SSCs and their failure modes and is consistent with their description in SECY-95-132 and the acceptance criteria in Draft SRP Section 17.4, RAP; therefore, these design considerations are acceptable.

### 17.4.4 Relationship to Other Administrative Programs

In DCD Tier 2 Section 17.4.4, "Relationship to Other Administration Programs," Westinghouse states that the D-RAP manifests itself in other administrative and operational programs. The technical specifications provide surveillance and testing frequencies for certain risk-significant SSCs, providing confidence that the reliability values assumed for them in the PRA will be maintained during plant operations. Risk-significant systems that provide defense-in-depth or result in significant improvement in the PRA evaluations are included in the scope of the D-RAP.

Westinghouse also states that the O-RAP can be implemented through the plant's existing programs for maintenance or quality assurance. For example, the plant's implementation of the Maintenance Rule, 10 CFR 50.65, can provide coverage of the SSCs that would be included in the O-RAP. The COL applicant will be responsible for the submittal of an O-RAP to the NRC.

The NRC staff will review this process as part of the plant's maintenance program, QA program, or other existing programs.

The NRC staff finds that using quality assurance and maintenance rule programs to implement portions of D-RAP and O-RAP as noted in DCD Section 17.4.4, "Relationship to Other Administrative Programs," is consistent with the essential elements of D-RAP in SECY 95-132 and the acceptance criteria in Draft SRP 17.4, RAP; therefore, these essential elements of the AP1000 D-RAP are acceptable.

#### 17.4.5 The AP1000 Design Organization

In DCD Section 17.4.5, The AP1000 Design Organization, Westinghouse states:

The AP1000 organization of Section 1.4 formulates and implements the AP1000 D-RAP.

The AP1000 management staff is responsible for the AP1000 design and licensing.

The AP1000 staff coordinates the program activities, including those performed within Westinghouse as well as work completed by the architect-engineers and other supporting organizations listed in Section 1.4.

The AP1000 staff is responsible for development of Phase I of the D-RAP and the design, analyses, and risk and reliability engineering required to support development of the program. Westinghouse is responsible for the safety analyses, the reliability analyses, and the PRA.

The reliability analyses are performed using common databases from Westinghouse and from industry sources such as [Institute of Nuclear Power Operations] INPO and [Electrical Power Research Institute] EPRI.

The Risk and Reliability organization is responsible for developing the D-RAP and has direct access to the AP1000 staff. Risk and Reliability is responsible for keeping the AP1000 staff cognizant of the D-RAP risk-significant items, program needs, and status. Risk and Reliability participates in the design change control process for the purpose of providing D-RAP-related inputs in the design process. Additionally, a cognizant representative of Risk and Reliability is present at designs reviews. Through these interfaces, Risk and Reliability can identify interfaces between the performance of risk significant SSCs and the reliability assumptions in the PRA. Meetings between Risk and Reliability and the designer are then held to manage interface issues.

The NRC staff reviewed the description of the AP1000 design organization and finds that DCD Section 17.4.5 is consistent with the description of the organizational structure needed to implement the D-RAP in SECY 95-132 and Draft SRP Section 17.4, RAP; therefore, the AP1000 design organization is acceptable.

#### 17.4.6 Objective

In Revision 4 to DCD Section 17.4.6, Objective, Westinghouse states:

The objective of the D-RAP is to design reliability into the plant and to maintain the AP1000 reliability consistent with the NRC-established PRA safety goals;

The following goals have been established for the D-RAP:

- Provide reasonable assurance that
  - The AP1000 is designed, procured, constructed, maintained and operated in a manner consistent with the assumptions and risk insights in the AP1000 PRA for these risk-significant SSCs
  - The risk-significant SSCs do not degrade to an unacceptable level during plant operations
  - The frequency of transients that challenge the AP1000 risk-significant SSCs are minimized
  - The risk-significant SSCs function reliably when they are challenged
- Provide a mechanism for establishing baseline reliability values for risk-significant SSCs identified by the risk determination methods used to implement the Maintenance Rule (10 CFR 50.65) and consistent with PRA reliability and availability design basis assumptions used for the AP1000 design
- Provide a mechanism for establishing baseline reliability values for SSCs consistent with the defense-in-depth functions to minimize challenges to the safety related systems
- Generate design and operational information to be used by a Combined License applicant for ongoing plant reliability assurance activities

Development of maintenance assessments and recommendations for the D-RAP (Phase II) and the site specific portion of the D-RAP (Phase III) is the responsibility of the Combined License applicant.

The Combined License applicant is responsible for submitting its maintenance recommendations (Phase II) and site specific (Phase III) D-RAP organization description to the NRC.

The goal of the Combined License applicant's O-RAP is to maintain reliability consistent with the overall safety goals and to maintain the capability to perform safety-related functions. Individual component reliability values are expected to change throughout the

course of plant life because of aging and changes in suppliers and technology. Changes in individual component reliability values are acceptable as long as overall plant safety performance is maintained within the NRC-established PRA safety goals and deterministic licensing design basis.

The NRC staff finds that the objectives outlined in DCD Section 17.4.6, are consistent with the objectives described in SECY 95-132 and the acceptance criteria in Draft SRP Section 17.4; therefore, these objectives are acceptable. The COL applicant is responsible for the D-RAP design organization during phase III of the design review. In addition, the COL applicant is responsible for implementing the O-RAP. These are COL Action Items in DCD Section 17.5.

#### 17.4.7 D-RAP Phases

##### 17.4.7.1 D-RAP Phase I - SSC Identification and Prioritization

The staff compared the AP1000 SSC identification and prioritization methodology using the guidance provided in Draft SRP Section 17.4 and SECY 95-132. The staff concluded that the AP1000 SSC identification and prioritization methodology was consistent with these guidance documents. However, the staff noted several areas where the D-RAP results for the AP1000 and the previously reviewed and approved AP600 design differed. By letters to the applicant dated September 19, 2002, and May 20, 2003, the NRC staff requested additional information on the D-RAP SSC identification results for the AP1000 design in order to evaluate these differences. The NRC staff evaluated the results for the AP600 and AP1000 D-RAP programs and concluded that the applicant adequately justified the differences. The details of the applicant's response to RAIs 260.002, 260.003, 260.004, 260.005, and the NRC staff evaluation are presented below.

- Basis for Identification and Prioritization of Risk Significant SSCs within the Scope of D-RAP for the AP1000

In Revision 3 of DCD Tier 2 Section 17.4, Table 17.4-1, the applicant provided expert panel, engineering judgement, and importance measure information on the rationale for including certain SSCs within the scope of D-RAP. The NRC staff found that the probabilistic, deterministic, and engineering judgment information found in the Table 17.4-1 was comprehensive and complete. However, in RAI 260.002, the NRC staff requested additional information concerning the identification and prioritization of risk significant SSCs within the scope of D-RAP for the AP1000 design.

In the response to RAI 260.002, the applicant provided the NRC staff with a comprehensive list of differences between the risk achievement worth (RAW) and risk reduction worth (RRW) values for the AP600 and AP1000 design. The NRC staff reviewed the list of differences between the RAW and RRW between the two plants and found that it appropriately identified SSCs within the scope of the D-RAP for the AP1000 design. The NRC staff also reviewed information in Revision 1 to the AP1000 PRA, Chapter 50, "Importance and Sensitivity Analysis," which contained all the RAW and

RRW importance measure values for individual SSCs. This PRA information was also used to determine the list of risk-significant SSCs under the scope of D-RAP.

Based on the information noted above, the NRC staff found that the SSCs included in the D-RAP in Revision 3 to DCD Tier 2 Section 17.4.1 are consistent with the description of SSCs included in the D-RAP in SECY 95-132 and Draft SRP Section 17.4; therefore, it is acceptable.

In RAI 260.003, the NRC staff requested additional information on (1) the passive containment cooling and normal heat removal functions that were added to the AP1000 design; (2) changes in I&C terminology in the AP1000 design; and (3) changes in the passive containment cooling system (PCS) re-circulation motor operated valves (MOVs) functions and valve position.

- Addition of PCS and normal residual heat removal (RNS) functions to the AP1000 Design

In Revision 0 to DCD Tier 2 Section 17.4-1, the NRC staff identified two system functions that were added to the AP1000 D-RAP. The two functions that were added include (1) the PCS and MOV drain function for evaporative cooling of the containment shell during design basis accidents; and (2) the RNS function. The NRC staff evaluated the changes in the risk ranking for these two functions and found that inclusion of these functions in the D-RAP for the AP1000 design was consistent with the applicant's D-RAP methodology.

- Changes in I&C Terminology

In the AP600 design, the protection and monitoring system (PMS) actuation hardware, the engineered safety feature (ESF) actuation and protection logic cabinets were in the scope of the D-RAP. For the AP1000 design, the PMS actuation hardware, the ESF actuation and protection logic cabinets were removed from the scope of the D-RAP. The NRC staff requested that the applicant provide additional information stating why these cabinets were removed from the scope of the D-RAP.

In Revision 3 to DCD Tier 2 Section 17.4-1, the applicant added the PMS actuation hardware to incorporate changes in I&C system terminology that were made to the DCD Tier 2 Chapter 7; therefore, the scope of the hardware covered by the AP1000 D-RAP was acceptable.

- Changes in Passive Core Cooling System Containment Recirculation MOVs Function and Normal Valve Position

In the AP600 design, the MOVs in the passive core cooling system recirculation lines have a safety function to automatically open to provide core cooling. Because of the safety significance of this function, these MOVs were within the scope of the D-RAP for the AP600 design.

Although Revision 0 of the DCD Tier 2 Section 6.3.2.1.3, "Safety Injection During Loss of Coolant Accidents," indicated that the MOVs in each passive core cooling recirculation line automatically open to provide core cooling, the NRC staff found that these valves were not within the scope of the D-RAP for the AP1000 design.

In response to RAI 260.003c, the applicant issued Revision 3 to DCD Tier 2 Section 6.3.2.1.3, to clarify that these MOVs are normally open and do not have a safety function to automatically open. Based on this change to the normal position of these valves, the NRC staff concludes that these passive core cooling MOVs do not need to be within scope of the AP1000 D-RAP is acceptable.

- Addition of CAS Air Compressor Transmitter

In Revision 1 to DCD Table 17.4-1, Westinghouse added a CAS air compressor transmitter to the D-RAP for the AP1000 design. A failure of the air compressor transmitter was found to increase the RRW above the threshold for large release frequency in the AP1000 design. Based on this information, the NRC staff found that this change to the D-RAP is acceptable.

- Addition of IRWST Vents

In Revision 3 to DCD Table 17.4-1, Westinghouse added the IRWST vents to the D-RAP for the AP1000 design. The IRWST vents provide a pathway to vent steam from the tank into the containment. The IRWST vents also have a severe accident function to prevent the formation of standing hydrogen flames close to the containment walls. This function is accomplished by designing the vents located further from the containment walls to open with less IRWST internal pressure than the other vents. This function was added due to an increase in the RAW above the threshold for common cause failure. Based on this information, the NRC staff finds that this change to the D-RAP is acceptable.

- Addition of Feedwater Isolation Valves

In Revision 0 to DCD Table 17.4-1, Westinghouse added the feedwater isolation valves to the D-RAP for the AP1000 design. This function was added due to an increase in the RAW above the threshold which then identified these valves as risk significant in the AP1000 design. Based on this information, the NRC staff found that this change to the D-RAP was acceptable.

The NRC staff determined that the changes in the scope of equipment in the D-RAP for the AP1000 design is consistent with implementation of the D-RAP SSC identification and prioritization methodology in SECY 95-132 and Draft SRP Section 17.4; therefore, D-RAP Phase I activities are acceptable.

#### 17.4.7.2 D-RAP Phase II

- Development of Recommended Plant Maintenance and Monitoring Activities

In Revision 0 of DCD Tier 2 Section 17.4.1, the applicant stated that the D-RAP, as shown in Figure 17.4-1, is implemented in three phases. The first phase, the design certification phase, defines the overall structure of the AP1000 D-RAP, and implements those aspects of the program which are applicable to the design process. During this phase, risk-significant SSCs are identified for inclusion in the program using probabilistic, deterministic, and other methods. Phase II, the post-design certification process, develops component maintenance recommendations for the plant's operations and maintenance activities for identified SSCs. The third phase is the site-specific phase, which introduces the plant's site-specific SSCs to the D-RAP process. Phases I and II are performed by the designer. Phase III is the responsibility of the COL applicant.

In Revision 0 of DCD Tier 2 Section 17.4.7.2, D-RAP, Phase II, the applicant states that "during Phase II of the D-RAP, maintenance assessments and recommendations are developed to enhance reliability and the plant risk-significant components."

In RAI 260.004, the NRC found that it is not appropriate for the applicant to complete the Phase II, post-design certification phase process, following issuance of a design certification for the AP1000 design. The applicant should not have post design certification issues in the DCD for the AP1000 design. The applicant should complete this activity as the design certification applicant, or the COL applicant should complete this activity. The applicant should provide additional information to clarify the applicant's and COL applicant's additional responsibilities for completion of Phase II activities.

In Revision 4 of DCD Tier 2 Section 17.4.1, paragraph 2 was revised to state that "Phase I is performed by the designer. Phases II and III are completed by the Combined License applicant." Westinghouse also revised DCD Tier 2 Section 17.4.6, Paragraph 2, to state that "Development of maintenance assessments and recommendations for D-RAP (Phase II) and the site specific portion of the D-RAP (Phase III) are the responsibility of the Combined License applicant. The Combined License applicant is responsible for submitting its maintenance recommendations (Phase II) and site specific (Phase III) D-RAP organization description to the NRC."

On the basis of this approach for maintenance recommendations on risk-significant SSCs, described in DCD Tier 2 Sections 17.4.1 and 17.4.7.2, and in accordance with the guidance in SECY 95-132 and the acceptance criteria in SRP 17.4, the NRC staff finds that the design certification applicant's approach for developing recommended maintenance and monitoring activities is acceptable.

- Dominant Failure Modes and Reliability and Availability Data

In RAI 260.005a, the NRC staff noted that DCD Section 17.4.7.2.1 did not clearly specify where cross references information was located in the design certification application for PRA

assumptions for dominant failure modes, and reliability and availability data. The NRC staff requested that Westinghouse add the cross references in DCD Section 17.4.7.2.1. In Revision 4 of DCD Section 17.4.7.2.1, Westinghouse added the appropriate cross references as noted on each of the three items listed below. In Revision 4 to DCD Section 17.4.7.2.1, Westinghouse states that to support the Combined License applicant's D-RAP Phase II and Phase III and O-RAP, the following information is provided:

- The list of risk-significant SSCs identified during the design phase (Table 17.4-1)
- The PRA assumptions for component unavailability and failure data (Chapter 32 of the AP1000 PRA [Reference 5])
- The analyses performed for components identified as major contributors to total risk, with dominant failure modes identified and prioritized. (Chapter 50 of the AP1000 PRA [Reference 5] identified the major contributors to total risk, and chapters 8 and 28 of the AP1000 PRA describes the analyses of the respective systems and associated components in Table 17.4-1.) The suggested means and prevention or mitigation of these failure modes forms the basis for the plant surveillance, testing, and maintenance programs.

The NRC staff finds that the references noted in DCD Tier 2 Sections 17.4.7.2 and 17.4.7.2.1 for D-RAP Phase II meet the guidance in SECY 95-132 and the acceptance criteria in Draft SRP Section 17.4; therefore, D-RAP Phase II activities are acceptable. This is also a COL Action Item in DSER Section 17.5.

#### 17.4.7.3 D-RAP, Phase III

In Revision 0 to DCD Section 17.4.7.3, Westinghouse states that:

Site specific activities of the D-RAP are the responsibility of the combined license applicant. Figure 17.4-1 shows these activities in the Phase III area of the figure. At this stage, the D-RAP package is modified or appended based on considerations specific to the site.

The COL applicant will need to establish the PRA importance measures, the expert panel process, and other deterministic methods to determine the site-specific list of SSCs under the scope of RAP.

The Combined License applicant would benefit from using the Phase I and II processes as a guide during this phase of the program. It is the responsibility of the Combined License applicant to ensure its Expert Panel is composed of personnel knowledgeable in the systems, operations, and maintenance of a plant, and that these personnel should have the breadth of experience necessary to perform the site specific SSC selections and evaluations for the RAP.

Based on the above, the NRC staff agreed that D-RAP Phase III is appropriately identified as a COL applicant activity. This is a COL action item in DSER Section 17.5. This activity also meets the guidance in SECY 95-132 and the Draft SRP Section 17.4; therefore, DCD Tier 2 Section 17.4.7.3 is acceptable.

#### 17.4.7.4 D-RAP Implementation

- D-RAP Implementation Example

In Revision 0 of DCD Tier 2 Section 17.4.7.4, D-RAP Implementation, Westinghouse states:

The following is an example of a system that was reviewed and modified under the D-RAP, Phase I and II. The design and analytical results presented here are intended as an example and do not reflect the current AP1000 design.

In DCD Tier 2 Section 17.4.7.4, Westinghouse provided an example of D-RAP implementation using the automatic depressurization system (ADS) for selection of components that are in the D-RAP for the AP1000 design. In RAI 260.005b, the NRC staff determined that the wording in the 2nd sentence of the 1st paragraph in DCD Tier 2 Section 17.4.7.4 was confusing. In Revision 4 to DCD Tier 2 Section 17.4.7.4, Westinghouse revised the paragraph to state:

The following is an example of a system that was reviewed and modified under the D-RAP, Phase I. The design and analytical results presented here are intended as an example.

The NRC staff finds that this change is acceptable. The NRC staff also finds that the ADS example is appropriate for the AP1000 implementation of the D-RAP; therefore, DCD Tier 2 Section 17.4.7.4 is acceptable.

#### 17.4.8 Glossary of Terms

In Revision 3 to DCD Section 17.4.8, "Glossary of Terms," Westinghouse added the abbreviation RTNSS to the list. The NRC staff determined that this section contained all the necessary and appropriate terms used in the D-RAP; therefore, DCD Section 17.4.8 is acceptable.

#### 17.4.9 Conclusion

On the basis of the NRC staff's review and evaluation of DCD Tier 2 Section 17.4, "Design Reliability Assurance Program," the NRC staff concludes that the D-RAP for design certification of the AP1000 design is consistent with the guidance provided in SECY-95-132 and Draft SRP Section 17.4, therefore, the D-RAP is acceptable.

## 17.5 Combined License Information Items

In DCD Tier 2 Section 17.5, "Combined License Information Items," Westinghouse describes the following COL Action Items: (note that the NRC staff action item number is after each Westinghouse item)

The Combined License applicant will address its design phase Quality Assurance program, as well as its Quality Assurance Program for procurement, fabrication, installation, construction, and testing of structures, systems and components in the facility. The quality assurance program will include provisions for seismic Category II structures, systems and components. This is COL Action Item 17.5-1.

The COL applicant will establish PRA importance measures, the expert panel process, and the other deterministic methods to determine the site-specific list of SSCs under the scope of RAP. This is COL Action Item 17.5-2.

The Combined License applicant is responsible for integrating the objectives of the O-RAP into Quality Assurance Program developed to implement 10 CFR [Part] 50, Appendix B. This is COL Action Item 17.5-3.

The Combined License applicant will address its Quality Assurance program for operations. This is COL Action Item 17.5-4.

The Combined License applicant is responsible for performing the tasks necessary to maintain the reliability of risk-significant SSCs. The Maintenance Rule (10 CFR 50.65) is relevant to the Combined License applicant's maintenance activities in that it describes SSC performance related goals during plant operation. This is COL Action Item 17.5-5.

In addition to performing the specific tasks necessary to maintain SSC reliability at its required level, the O-RAP activities include:

- Reliability data base - Historical data available on equipment performance. The compilation and reduction of this data provides the plant with source of component reliability information.
- Surveillance and testing - In addition to maintaining the performance of the components necessary for plant operations, surveillance and testing provides a high degree of reliability for the safety-related SSCs.
- Maintenance plan - This plan describes the nature and frequency of maintenance activities to be performed on plant equipment. The plan includes the selected SSCs identified in the D-RAP.

This is COL Action Item 17.5-6.

In an effort to ensure that the COL action items in DCD 17.5, associated with D-RAP and O-RAP, are accomplished in a manner consistent with the guidance contained in SECY 95-132,

## Quality Assurance

the applicant should provide a COL action item to reflect conformance with the SECY 95-132 guidance. This is DSER Open Item 17.5-1.