

**CHAPTER 17****QUALITY ASSURANCE****17.1 Quality Assurance During the Design and Construction Phases**

See Section 17.5.

**17.2 Quality Assurance During the Operations Phase**

See Section 17.5.

**17.3 Quality Assurance During Design, Procurement, Fabrication, Inspection and/or Testing of Nuclear Power Plant Items and Services**

This section outlines the quality assurance program applicable to the design, procurement, fabrication, inspection, and/or testing of items and services for the AP600 Project.

Effective March 31, 1996, activities affecting the quality of items and services for the AP600 Project during design, procurement, fabrication, inspection, and/or testing are being performed in accordance with the quality plan described in "Westinghouse Electric Corporation - Energy Systems Business Unit, Quality Management Systems," Revision 1 (Reference 1).

Activities performed prior to March 31, 1996 were performed in accordance with the quality plan described in topical report WCAP-8370, "Energy Systems Business Unit - Power Generation Business Unit, Quality Assurance Plan," Revision 12a (Reference 2). Activities performed prior to November 30, 1992 were performed in accordance with the quality plan described in topical report WCAP-8370/7800, "Energy Systems Business Unit - Nuclear Fuel Business Unit, Quality Assurance Plan," Revision 11A/7A (Reference 3).

A project-specific quality plan was issued to supplement the quality management system document and the topical reports for design activities affecting the quality of structures, systems, and components for the AP600 project (Reference 4). This plan addresses the NQA-1-1989 edition through NQA-1b-1991 addenda.

Quality Assurance requirements for systems, structures, and components will be graded based on the safety classification as indicated in Section 3.2. Safety-related systems are classified as Equipment Classes A, B and C, and will meet the requirements of 10 CFR 50, Appendix B. For systems, structures, and components included in the regulatory treatment of nonsafety systems (RTNSS), the quality requirements are identified in Table 17-1. See Section 16.3 for systems that should be considered for designation of systems and components included in the regulatory treatment of nonsafety systems.

While Westinghouse retains the overall responsibility for the AP600 design, portions of the design are developed by external organizations. Each organization maintains a quality assurance program that meets the NQA-1 criteria that apply to its work scope. In accordance

with QMS Revision 1 (Reference 1), Westinghouse performs an initial evaluation of these programs and monitors their continued effective implementation through audits, surveillance, and evaluation of the performance of external organizations.

## **17.4 Design Reliability Assurance Program**

This subsection presents the AP600 Design Reliability Assurance Program (D-RAP).

### **17.4.1 Introduction**

The AP600 D-RAP is implemented as an integral part of the AP600 design process to provide confidence that reliability is designed into the plant and that the important reliability assumptions made as part of the AP600 probabilistic risk assessment (PRA) (Reference 5) will remain valid throughout plant life. The PRA quantifies plant response to a spectrum of initiating events to demonstrate the low probability of core damage and resultant risk to the public. PRA input includes specific values for the reliability of the various structures, systems, and components (SSCs) in the plant that are used to respond to postulated initiating events.

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 AP600 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 the 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 Combined License applicant.

Finally, Figure 17.4-1 shows the Operational Reliability Assurance Process (O-RAP). This phase, which is implemented by the Combined License applicant, provides confidence that the operations and maintenance activities performed by the operating plant support should maintain the reliability assumptions made in the plant PRA.

### **17.4.2 Scope**

The D-RAP includes a design evaluation of the AP600 and identifies the aspects of plant operation, 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.

### **17.4.3 Design Considerations**

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.

#### **17.4.4 Relationship to Other Administrative Programs**

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.

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 O-RAP. The Combined License applicant will be responsible for the submittal of an O-RAP to the NRC. The NRC will review this process as part of the plant's maintenance program, Quality Assurance program, or other existing program.

#### **17.4.5 The AP600 Design Organization**

The AP600 organization of Section 1.4 formulates and implements the AP600 D-RAP.

The AP600 management staff is responsible for the AP600 design and licensing.

The AP600 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 AP600 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 INPO and EPRI.

The Risk and Reliability organization is responsible for developing the D-RAP and has direct access to the AP600 staff. Risk and Reliability is responsible for keeping the AP600 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 to the design process. Additionally, a cognizant representative of Risk and Reliability is present at design 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.

#### 17.4.6 Objective

The objective of the D-RAP is to design reliability into the plant and to maintain the AP600 reliability consistent with the NRC-established PRA safety goals.

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

- Provide reasonable assurance that
  - The AP600 is designed, procured, constructed, maintained and operated in a manner consistent with the assumptions and risk insights in the AP600 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 AP600 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 AP600 design
- Provide a mechanism for establishing baseline reliability values for SSCs consistent with the regulatory treatment of nonsafety systems (RTNSS) process (Reference 6)
- 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

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 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 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 the deterministic licensing design bases.

#### **17.4.7 D-RAP, Phase I**

Phase I, the definition portion of the D-RAP, includes the initial identification of SSCs to be included in the program, implementation of the aspects applicable to design efforts, and definition of the scope, requirements, and implementation options to be included in the later phases.

##### **17.4.7.1 SSCs Identification and Prioritization**

The initial task of the D-RAP is identification of risk-significant SSCs to be included within the scope of the program. As shown in Figure 17.4-1, the AP600 PRA is used to identify those SSCs, consistent with the criteria of Reference 7 for risk achievement worth (RAW), risk reduction worth (RRW), and Fussel-Vesely Worth (FVW). The review of light water reactor industry experience and industry notices (such as licensee event reports) support the process. An expert panel is also employed in the selection process.

PRA-based measurements provide information that contributes to the identification and prioritization of SSCs. A component's RAW is the factor by which the plant's core damage frequency increases if the component reliability is assigned the value 0.0. Components with risk achievement worth values of 2 or greater are considered for inclusion in the D-RAP.

RRW is used in the selection process. A component's risk reduction worth is the amount by which the plant's core damage frequency decreases if the component's reliability is assigned the value 1.0. A threshold measure of 1.005 or greater is used as the cutoff. Components with RRW of 1.005 or greater are considered for inclusion in the D-RAP.

FVW is also used in the screening process. This is a measure of an event's contribution to the overall plant core damage frequency. Components with Fussel-Vesely worth of 0.5 percent or greater are considered for inclusion in the D-RAP.

Deterministic considerations are also instrumental in identifying risk-significant SSCs. The deterministic identification of risk-significant SSCs encompasses the following guidelines and considerations:

- ATWS rule (10 CFR 50.62)
- Loss of all ac power (10 CFR 50.63)
- Post-72-hour actions
- Containment performance
- Adverse interactions with the AP600 safety-related systems
- Seismic considerations

Nonsafety-related systems identified as risk-significant are considered in the scope of the D-RAP:

- Diverse actuation system
- Non-Class 1E dc and uninterruptible power supply system
- Offsite power, main ac power, and onsite standby power systems
- Normal residual heat removal system
- Component cooling water system
- Service water system

Finally, risk-significant SSCs are selected using industry experience, regulations, and engineering judgment.

#### **17.4.7.1.1 Level 1 PRA and Shutdown Analysis**

The Level 1 PRA evaluates accident sequences from initiating events and failures of safety functions to core damage events. The probability of core damage and the identification of dominant contributors to that state are also determined in this analysis.

A low-power and shutdown assessment is conducted to address concerns about risk of operations during shutdown conditions. It encompasses operation when the reactor is in a subcritical state or is in a transition between subcriticality and power operation up to 5 percent of rated power. It consists of a Level 1 PRA and an evaluation of release frequencies and magnitudes.

Included in the D-RAP are events that meet the threshold risk achievement worth, risk reduction worth, or Fussel-Vesely worth values defined in subsection 17.4.7.1.

#### **17.4.7.1.2 Level 2 Analysis**

The Level 2 analysis predicts the plant response to severe accidents and offsite fission product releases. Specifically, the analysis includes the following sections:

- Evaluating severe accident phenomena and fission product source terms
- Modeling the containment event tree

- Analyzing hydrogen burn, mixing, and igniter placement
- Modeling the AP600 utilizing the MAAP4 code

Equipment used in the prevention of severe accidents and severe post-accident boundary conditions is credited in the Level 1 and Level 2 PRA analyses. An example of this preventive equipment is the reactor coolant system automatic depressurization system (ADS). Successful depressurization leads to core cooling, and in the event that injection fails, results in a low pressure core damage sequence that has fewer uncertainties and can be more easily mitigated than high pressure core damage.

The containment event tree used in the AP600 Level 2 PRA examines the operation of equipment which mitigates the threat to the containment from severe accident phenomena. The systems credited for the mitigation of large fission product releases are containment isolation, passive containment cooling water (PCS), and operator action to flood the cavity by opening the recirculation valves and energizing the hydrogen igniters.

#### 17.4.7.1.3 External Event Analyses

These analyses consider the events whose cause is external to all the systems associated with normal and emergency operations situations. They include the following:

- Internal flood
- Seismic margins analysis
- External events evaluations (such as high winds and tornados, external floods, and transportation accidents)
- Fire

The internal flood analysis identifies, analyzes, and quantifies the core damage risk contribution as a result of internal flooding during at-power and shutdown conditions. The analysis models potential flood vulnerabilities in conjunction with random failures modeled as part of the internal events PRA.

The seismic margins analysis identifies potential vulnerabilities and demonstrates seismic margin beyond the safe shutdown earthquake. The capacity of those components required to bring the plant to a safe, stable shutdown is evaluated.

#### 17.4.7.1.4 Expert Panel

Meetings were held among Systems Engineering, PRA, and Reliability Engineering to perform the final selection of SSCs that should be included in the D-RAP. As shown in Figure 17.4-1, industry-wide information sources and engineering judgment were employed in considering the addition of SSCs to the D-RAP.

#### 17.4.7.1.5 SSCs to be Included in D-RAP

Table 17.4-1 lists the non-site-specific SSCs included in the D-RAP. In Figure 17.4-1, this list is denoted as "Risk-significant items (non-site-specific)." For each item listed in the "SSC" column, there is a corresponding "Rationale" given. Items whose values exceed the thresholds for RAW or RRW are included and noted as such. Other SSCs are included based upon their significance to Level 2 analysis, external event analyses, or seismic margin analysis. Additional items are included based upon an expert panel review. The "Insights and Assumptions" column provides additional insights into the selection process.

The use of Fussel-Vesely worth resulted in no SSC selections.

#### 17.4.7.2 D-RAP, Phase II

During Phase II of the D-RAP, maintenance assessments and recommendations are developed to enhance the reliability of the plant risk-significant components. These activities are shown in Figure 17.4-1 as "Recommended Plant Maintenance Monitoring Activities." The recommendations can take the form of monitoring activities or preventive, predictive or corrective maintenance, and are dependent upon the types of failure modes that a component may experience. These modes are generally determined by a failure modes, effects and criticality analysis. The maintenance recommendations address the most significant failure modes of the component.

#### 17.4.7.2.1 Information Available to Combined License Applicant

To support the Combined License applicant's D-RAP Phase III and O-RAP, the following information is provided:

- The list of risk-significant SSCs identified during the design phase
- The PRA assumptions for component unavailability and failure data
- The analyses performed for components identified as major contributors to total risk, with the dominant failure modes identified and prioritized. The suggested means for prevention or mitigation of these failure modes forms the basis for the plant surveillance, testing, and maintenance programs.

#### 17.4.7.3 D-RAP, Phase III

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 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.

#### 17.4.7.4 D-RAP Implementation

The following is an example of a system that was reviewed and modified under the D-RAP, Phases I and II. The design and analytical results presented here are intended as an example and do not reflect the current AP600 design.

The automatic depressurization system, which is part of the reactor coolant system, acts in conjunction with the passive core cooling system to mitigate design basis accidents. The automatic depressurization system valves are discussed in subsection 5.4.6 of the DCD.

The earlier automatic depressurization system design contained four depressurization stages, with motor-operated valves in all stages. Preliminary PRA analysis established that fourth stage failure, in certain combination with failures of other stages, was a major contributor to core damage frequency. Thus, it was concluded that the fourth stage valves should be diverse in design from the valves in other stages to reduce common cause failure.

As a result of joint meetings among the AP600 PRA, Design, and staff organizations to discuss core melt frequency improvements, the fourth stage automatic depressurization system was changed from a motor-operated valve to a squib (explosively actuated) valve. The new configuration of the system is shown in the reactor coolant system P&ID (Figure 5.1-5 of the DCD). An example of the analytical results that reflect this change is provided in Table 17.4-2.

As part of the evaluation of the squib valves, a failure modes and effects analysis (FMEA) was prepared to identify subcomponent failures and critical items that could lead to hazardous or abnormal conditions of the automatic depressurization system and the plant. The identification of failure modes facilitated the development of recommended maintenance and in-service testing activities to maximize valve reliability.

The squib valve is a completely static electromechanical assembly. Prior to activation, there are no moving parts. No powered components are needed to hold a stem seat or globe in place by torque, solenoid coils, or friction. The explosive actuator is a simple, passive device that is triggered by an applied voltage.

Because the automatic depressurization system fourth stage valves perform safety-related functions, they will be subject to in-service testing to verify that they are ready to function in an accident. Subsection 3.9.6 of the DCD includes in-service testing requirements for these valves.

Example FMEA results for the fourth stage squib valves and the second and third stage motor-operated valves are included in DCD Table 6.3-5. DCD subsection 3.9.6.3.1 provides testing recommendations for the second and third stage valves.

#### 17.4.8 Glossary of Terms

D-RAP	Design Reliability Assurance Program – performed as part of the AP600 design effort to assure that the reliability assumptions of the PRA remain valid throughout the plant operating lifetime.
FVW	Fussel-Vesely Worth
O-RAP	Operational Reliability Assurance Process
PRA	Probabilistic Risk Assessment
RAW	Risk Achievement Worth
Risk-significant	Any SSC determined in the PRA or by risk-significance analysis (e.g., Level 2 PRA and shutdown risk analysis) to be a major contributor to overall plant risk
RRW	Risk Reduction Worth
RTNSS	Regulatory Treatment of Nonsafety-Related Systems
SSC	Structures, Systems, and Components

#### 17.5 Combined License Information Items

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.

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

Combined License applicant is responsible for integrating the objectives of the O-RAP into the Quality Assurance Program developed to implement 10 CFR 50, Appendix B.

The Combined License applicant will address its Quality Assurance program for operations.

The following activities are represented in Figure 17.4-1 as "Plant Maintenance Program."

The Combined License applicant is responsible for performing the tasks necessary to maintain the reliability of risk-significant SSCs. Reference 8 contains examples of cost-effective maintenance enhancements, such as condition monitoring and shifting time-directed maintenance to condition-directed maintenance.

The Maintenance Rule (10 CFR 50.65) is relevant to the Combined License applicant's maintenance activities in that it prescribes SSC performance-related goals during plant operation.

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 operation, 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.

## 17.6 References

1. "Energy Systems Business Unit - Quality Management System," Revision 2.
2. WCAP-8370 Revision 12a, "Energy Systems Business Unit - Power Generation Business Unit Quality Assurance Plan."
3. WCAP-8370/7800, Revision 11A/7A, "Energy Systems Business Unit - Nuclear Fuel Business Unit Quality Assurance Plan."
4. WCAP-12600 Revision 4, "AP600 Advanced Light Water Reactor Design Quality Assurance Program Plan," January 1998.
5. AP600 Probabilistic Risk Assessment, August 1998.
6. Brockhoff, C. S., Haag, C. L., More, D. G., Sterdis, A. L., "AP600 Implementation of the Regulatory Treatment of Nonsafety-Related Systems Process," WCAP-13856, Revision 1, January 1998.

7. Letter from NRC to Westinghouse, "Criteria for Establishing Risk Significant Structures, Systems, and Components (SSCs) to be Considered for the AP600 Reliability Assurance Program," January 16, 1997.
8. Lofgren, E. V., Cooper, et al, "A Process for Risk-Focused Maintenance," NUREG/CR-5695, March 1991.

Table 17-1

**QUALITY ASSURANCE PROGRAM REQUIREMENTS FOR RTNSS  
SYSTEMS, STRUCTURES, AND COMPONENTS**

The following outlines the quality assurance program requirements for suppliers of systems, structures, or components to which the requirements for the regulatory treatment of nonsafety systems (RTNSS) apply.

**1. Organization**

The normal line organization may verify compliance with the requirements of this table. A separate or dedicated quality assurance organization is not required.

**2. Quality Assurance Program**

It is expected that the existing body of supplier's procedures or practices will describe the quality controls applied to the subject equipment. A new or separate QA program is not required.

**3. Design Control**

Measures shall be established to ensure that contractually established design requirements are included in the design. Applicable design inputs shall be included or correctly translated into design documents, and deviations therefrom shall be controlled. Normal supervisory review of the designer's work is an adequate control measure.

**4. Procurement Document Control**

Applicable design bases and other requirements necessary to assure component performance, including design requirements, shall be included or referenced in documents for procurement of items and services, and deviations therefrom shall be controlled.

**5. Instructions, Procedures, and Drawings**

Activities affecting quality shall be performed in accordance with documented instructions, procedures, or drawings of a type appropriate to the circumstances. This may include such things as written instructions, plant procedures, cautionary notes on drawings, and special instructions on work orders. Any methodology which provides the appropriate degree of guidance to personnel performing activities important to the component functional performance will satisfy this requirement.

**6. Document Control**

The issuance and change of documents that specify quality requirements or prescribe activities affecting quality shall be controlled to assure that correct documents are employed.

Table 17-1 (Cont.)

**QUALITY ASSURANCE PROGRAM REQUIREMENTS FOR RTNSS  
SYSTEMS, STRUCTURES, AND COMPONENTS**

## 7. Control of Purchased Items and Services

Measures are to be established to ensure that all purchased items and services conform to appropriate procurement documents.

## 8. Identification and Control of Purchased Items

Measures shall be established where necessary, to identify purchased items and preserve their RTNSS important functional performance capability. Examples of circumstances requiring such control include the storage of environmentally sensitive equipment or material, and the storage of equipment or material that has a limited shelf-life.

## 9. Control of Special Processes

Measures shall be established to control special processes, including welding, heat treating, and non-destructive testing. Applicable codes, standards, specifications, criteria, and other special requirements may serve as the basis of these controls.

## 10. Inspection

Inspections shall be performed where necessary to verify conformance of an item or activity to specified requirements, or to verify that activities are being satisfactorily accomplished.

Inspections need not be performed by personnel who are independent of the line organization. However, inspections, where necessary, shall be performed by knowledgeable personnel.

## 11. Test Control

Measures shall be established, as appropriate, to test equipment prior to installation to demonstrate conformance with design requirements.

Tests shall be performed in accordance with test procedures. Test results shall be recorded and evaluated to ensure that test requirements have been met.

## 12. Control of Measuring and Test Equipment

Measures shall be established to control, calibrate, and adjust measuring and test equipment at specific intervals.

Table 17-1 (Cont.)

**QUALITY ASSURANCE PROGRAM REQUIREMENTS FOR RTNSS  
SYSTEMS, STRUCTURES, AND COMPONENTS**

## 13 Handling, Storage, and Shipping

Handling, storage, cleaning, packaging, shipping, and preservation of items shall be controlled to prevent damage or loss and to minimize deterioration.

## 14. Inspection, Test, and Operating Status

Measures shall be established to identify items that have satisfactorily passed required tests and inspections, and to indicate status of inspection, test, and operability as appropriate.

## 15. Control of Nonconforming Items

Items that do not conform to specified requirements shall be identified and controlled to prevent inadvertent installation or use.

## 16. Corrective Action

Measures shall be established to ensure that failures, malfunctions, deficiencies, deviations, defective components, and nonconformances are properly identified, reported, and corrected.

## 17. Records

Records shall be prepared and maintained to furnish evidence that the above requirements for design, procurement, document control, inspection, and test activities have been met.

## 18. Audits

Audits which are independent of line management are not required, if line management periodically reviews and documents the adequacy of the suppliers process and takes any necessary corrective action. Line management is responsible for determining whether reviews conducted by line management or audits conducted by an organization independent of line management are appropriate. If performed, audits shall be conducted and documents to verify compliance with design and procurement documents, instructions, procedures, drawings, and inspection and test activities.

DCD Table 17.4-1 (Sheet 1 of 10)		
RISK-SIGNIFICANT SSCs WITHIN THE SCOPE OF D-RAP		
System, Structure, or Component (SSC) <sup>(1)</sup>	Rationale <sup>(2)</sup>	Insights and Assumptions
System: Component Cooling Water (CCS)		
CCS Pumps	EP	These pumps provide cooling of the normal residual heat removal system (RNS) and the spent fuel pool heat exchanger. Cooling the RNS heat exchanger is RTNSS-important during shutdown reduced-inventory conditions. CCS valve realignment is not required for reduced-inventory conditions.
System: Containment System (CNS)		
Containment Vessel	EP, L2	The containment vessel provides a barrier to steam and radioactivity released to the atmosphere following accidents.
Hydrogen Igniters	EP, L2, Regulations	The hydrogen igniters provide a means to control H <sub>2</sub> concentration in the containment atmosphere, consistent with the hydrogen control requirements of 10 CFR 50.34f.
System: Chemical and Volume Control System (CVS)		
CVS Makeup Pump Suction and Discharge Check Valves	RAW	These CVS check valves are normally closed and have to open to allow makeup pump operation.
CVS Makeup Pumps	RAW/CCF	These pumps provide makeup to the RCS to accommodate leaks and to provide negative reactivity for shutdowns, steam line breaks, and ATWS.
System: Diverse Actuation System (DAS)		
Turbine Impulse Pressure Transmitters 001 and 002	RAW	These sensors provide signals used as permissives for the DAS automatic reactor trip function.
Containment Isolation Valves Controlled by DAS	EP, L2	These containment isolation valves are important in limiting offsite releases following core melt accidents.

Table 17.4-1 (Sheet 2 of 10)		
<b>RISK-SIGNIFICANT SSCs WITHIN THE SCOPE OF D-RAP</b>		
System, Structure, or Component (SSC) <sup>(1)</sup>	Rationale <sup>(2)</sup>	Insights and Assumptions
DAS Actuation Hardware (sensor input through control output and indication)	RAW	The DAS is diverse from the PMS and provides automatic actuation of selected plant features including control rod insertion, turbine trip, passive residual heat removal (PRHR) heat exchanger actuation, core makeup tank actuation, isolation of critical containment lines, and passive containment cooling system (PCS) actuation.
Control Rod MG Set Field Breakers	RAW	These breakers open on a DAS reactor trip signal demand to de-energize the control rod MG sets and allow the rods to drop.
Distribution Panels EDS1-EA-14 and EDS2-EA-14	RAW	These panels distribute power to the DAS equipment.
<b>System: Main ac Power System (ECS)</b>		
Ancillary Diesel Generators	EP	For post-72 hour actions, these generators are available to provide power for Class 1E monitoring, MCR lighting and for refilling the PCS water storage tank.
<b>System: Main and Startup Feedwater System (FWS)</b>		
Startup Feedwater Pumps	EP	The startup feedwater system pumps provide feedwater to the steam generator. This capability provides an alternate core cooling mechanism to the PRHR heat exchangers for non-loss-of-coolant-accidents or steam generator tube ruptures.
<b>System: General I&amp;C<sup>(4)</sup></b>		
Low Pressure/DP Sensors - IRWST level sensors	RAW/CCF	The in-containment refueling water storage tank (IRWST) level sensors support PMS and DAS functions. They are utilized in automatic actuation and they provide indications to the operator. IRWST level supports IRWST recirculation actions.

Table 17.4-1 (Sheet 3 of 10)

**RISK-SIGNIFICANT SSCs WITHIN THE SCOPE OF D-RAP**

System, Structure, or Component (SSC) <sup>(1)</sup>	Rationale <sup>(2)</sup>	Insights and Assumptions
High Pressure/DP Sensors <ul style="list-style-type: none"> <li>- main feedwater flow</li> <li>- startup feedwater flow</li> <li>- pressurizer pressure and level</li> <li>- steam generator wide- and narrow-range level</li> <li>- RCS hot leg level and steamline pressure</li> </ul>	RAW/CCF	The following sensors are included in this group. These sensors support PMS, DAS and PLS functions. They are utilized in reactor trip and ESF functions, and provide indications to the operator. Main feedwater flow sensors support startup feedwater actuation and startup feedwater flow sensors support PRHR actuation. The hot leg level sensors automatically actuate the IRWST and provide information to the operator for manual actuation of the automatic depressurization system (ADS).
System: Class 1E DC Power and Uninterruptible Power System (IDS)		
125 Vdc Distribution Panels	RAW	These panels distribute power to components in the plant that require 1E dc power support.
125 Vdc 24-hour Batteries, Inverters, and Chargers	RAW/CCF	The batteries provide power for the PMS and safety-related valves. The chargers are the preferred source of power for Class 1E dc loads and are the source of charging for the batteries. The inverters provide uninterruptible ac power to the I&C system.
Fused Transfer Switch Box	RAW	The fused disconnect switches connect the different levels of Class 1E distribution panels.
125 Vac Motor Control Centers	EP	These buses provide power for the PMS and safety-related valve operation.

Table 17.4-1 (Sheet 4 of 10)

## RISK-SIGNIFICANT SSCs WITHIN THE SCOPE OF D-RAP

System, Structure, or Component (SSC) <sup>(1)</sup>	Rationale <sup>(2)</sup>	Insights and Assumptions
Main Control Room (MCR) Displays and System Level Control Mechanisms to Support Operator Actions	RAW/CCF	This includes the Class 1E PMS (QDPS) and DAS displays and controls. It also includes the PLS displays and controls associated with CVS reactor makeup, RNS reactor injection from the IRWST, spent fuel cooling, component cooling of RNS and SFS heat exchangers, service water cooling of CCS heat exchangers, standby diesel generators, and hydrogen igniters. These displays and system level control mechanisms provide important plant indications and variables to allow the operator to monitor and control the plant during normal conditions and during design basis accidents.
Reactor Coolant Pump Circuit Breakers	RAW/CCF	These breakers open automatically to allow core makeup tank operation.
System: Passive Containment Cooling System (PCS)		
PCS Air-Operated Drain Isolation Valves	EP	These valves open automatically to drain water from a water storage tank onto the outside surface of the containment shell. This water provides evaporative cooling of the containment shell following accidents.
PCS Water Storage Tank Recirculation Pumps	EP	These pumps provide the motive force to refill the PCS water storage tank during post-72 hour support actions.
System: Plant Control System (PLS)		
PLS Actuation Hardware	RAW/CCF	This common cause failure event is assumed to disable all logic outputs from the PLS associated with CVS reactor makeup, RNS reactor injection from the IRWST, spent fuel cooling, component cooling of RNS SFS heat exchangers, service water cooling of CCS heat exchangers, standby diesel generators, and hydrogen igniters.
PLS Logic Cabinet Supporting CVS Functions	RAW/CCF	This is the distributed controller that supports the CVS function.

Table 17.4-1 (Sheet 5 of 10)

**RISK-SIGNIFICANT SSCs WITHIN THE SCOPE OF D-RAP**

System, Structure, or Component (SSC) <sup>(1)</sup>	Rationale <sup>(2)</sup>	Insights and Assumptions
System: Protection and Safety Monitoring System (PMS)		
CMT Level Sensors	RAW/CCF	These level sensors provide input for automatic actuation of the ADS. They also provide indications to the operator.
PMS Actuation Software	RAW/CCF	The PMS software modules include field input signal processing, control board signal input processing, actuation logic algorithms and output logic functions.
Reactor Trip Switch Gear	RAW/CCF	These breakers open automatically to allow insertion of the control rods.
PMS Actuation Hardware	RAW/CCF	The PMS hardware includes the following: IPC Reactor Trip Subsystems IPC ESF Subsystems ESF Actuation Cabinets Protection Logic Cabinets Manual Input Multiplexers
System: Passive Core Cooling System (PXS)		
Containment Recirculation Isolation MOVs	EP, L2	<p>The containment recirculation lines provide long-term core cooling following a loss-of-coolant accident (LOCA). The motor-operated valves open automatically to allow containment recirculation when the IRWST level is reduced to about the same level as the containment. The motor-operated valves also allow long-term core cooling to be provided by the RNS pumps.</p> <p>These valves together with the IRWST recirculation squib valves can provide a rapid flooding of the containment to support in-vessel retention during a severe accident.</p>

Table 17.4-1 (Sheet 6 of 10)

## RISK-SIGNIFICANT SSCs WITHIN THE SCOPE OF D-RAP

System, Structure, or Component (SSC) <sup>(1)</sup>	Rationale <sup>(2)</sup>	Insights and Assumptions
IRWST Check Valves	RAW/CCF	The containment recirculation lines provide long-term core cooling following a LOCA. These check valves open when the IRWST level is reduced to approximately the same level as the containment level.
IRWST Injection Squib Valves	RAW/CCF	The IRWST injection lines provide long-term core cooling following a LOCA. These squib valves open automatically to allow injection when the RCS pressure is reduced to below the IRWST injection head.
IRWST Screens	RAW/CCF	The IRWST injection lines provide long-term core cooling following a LOCA. These screens are located inside the IRWST and prevent large particles from being injected into the RCS. They are designed so that they will not become obstructed.
Containment Recirculation Squib Valves	RAW/CCF	The containment recirculation lines provide long-term core cooling following a LOCA. These squib valves open automatically to allow containment recirculation when the IRWST level is reduced to about the same level as the containment level. These squib valves can also allow long-term core cooling to be provided by the RNS pumps.  These squib valves together with the containment recirculation motor-operated valves can provide a rapid flooding of the containment to support in-vessel retention during a severe accident.
Containment Recirculation Screens	RAW/CCF	The containment recirculation lines provide long-term core cooling following a LOCA. The screens are located in the containment and prevent large particles from being injected into the RCS. They are designed so that they will not become obstructed.
IRWST Gutter Bypass Isolation Valves	EP	These valves direct water collected in the IRWST gutter to the IRWST. This capability extends PRHR heat exchanger operation.
Accumulator Discharge Check Valves	RAW/CCF	These check valves open when the RCS pressure drops below the accumulator pressure to allow accumulator injection.

Table 17.4-1 (Sheet 7 of 10)

**RISK-SIGNIFICANT SSCs WITHIN THE SCOPE OF D-RAP**

<b>System, Structure, or Component (SSC)<sup>(1)</sup></b>	<b>Rationale<sup>(2)</sup></b>	<b>Insights and Assumptions</b>
CMT Discharge Isolation Valves	RAW/CCF	These air-operated valves automatically open to allow core makeup tank injection.
CMT Discharge Check Valves		These check valves are normally open. They close during rapid accumulator injection.
PRHR Heat Exchanger Control Valves	RAW/CCF	The PRHR heat exchangers provide core cooling following non-LOCAs, steam generator tube ruptures, and anticipated transients without scram. The air-operated valves automatically open to initiate PRHR heat exchanger operation.
<b>System: Reactor Coolant System (RCS)</b>		
ADS Stages 1/2/3 Motor-Operated Valves	EP, L2	The ADS provides a controlled depressurization of the RCS following LOCAs to allow core cooling from the accumulator, IRWST injection, and containment recirculation. The ADS provides "bleed" capability for feed/bleed cooling of the core. The ADS also provides depressurization of the RCS to prevent a high-pressure core melt sequence.
ADS 4th Stage Squib Valves	RAW/CCF	The ADS provides a controlled depressurization of the RCS following LOCAs to allow core cooling from the accumulator, IRWST injection, and containment recirculation. The ADS provides "bleed" capability for feed/bleed cooling of the core. The ADS also provides depressurization of the RCS to prevent a high-pressure core melt sequence.
Pressurizer Safety Valves	EP	These valves provide overpressure protection of the RCS.

Table 17.4-1 (Sheet 8 of 10)

## RISK-SIGNIFICANT SSCs WITHIN THE SCOPE OF D-RAP

System, Structure, or Component (SSC) <sup>(1)</sup>	Rationale <sup>(2)</sup>	Insights and Assumptions
Reactor Vessel Insulation Water Inlet and Steam Vent Devices	EP	These devices provide an engineered flow path to promote in-vessel retention of the core in a severe accident.
Reactor Cavity Doorway Damper	EP	This device provides a flow path to promote in-vessel retention of the core in a severe accident.
System: Normal Residual Heat Removal System (RNS)		
RNS Pumps	EP	These pumps provide shutdown cooling of the RCS. They also provide an alternate RCS lower pressure injection capability following actuation of the ADS.  The operation of these pumps is RTNSS-important during shutdown reduced-inventory conditions. RNS valve realignment is not required for reduced-inventory conditions.
RNS Motor-Operated Valves	RRW/FVW	These MOVs align a flowpath for nonsafety-related makeup to the RCS following ADS operation.
System: Spent Fuel Cooling System (SFS)		
SFS Pumps	EP	These pumps provide flow to the heat exchangers for removal of the design basis heat load.

Table 17.4-1 (Sheet 9 of 10)

**RISK-SIGNIFICANT SSCs WITHIN THE SCOPE OF D-RAP**

System, Structure, or Component (SSC) <sup>(1)</sup>	Rationale <sup>(2)</sup>	Insights and Assumptions
<b>System: Steam Generator System (SGS)</b>		
Main Steam Isolation Valves	RAW	The steam generator main steam isolation valves provide isolation of the steam generator following secondary line breaks and steam generator tube rupture.
Main Steam Safety Valves	EP	The steam generator main steam safety valves provide overpressure protection of the steam generator. They also provide core cooling by venting steam from the steam generator.
<b>System: Service Water System (SWS)</b>		
Service Water Pumps and Cooling Tower Fans	EP	These pumps and fans provide cooling of the CCS heat exchanger which is RTNSS-important during shutdown reduced-inventory conditions. Service water system valve realignment is not required for reduced-inventory conditions.
<b>System: Nuclear Island Nonradioactive Ventilation System (VBS)</b>		
VBS MCR and I&C Rooms B/C Ancillary Fans	EP	For post-72 hour actions, these fans are available to provide cooling of the MCR and the two I&C rooms (B/C) that provide post-accident monitoring.
<b>System: Chilled Water System (VWS)</b>		
VWS Low Capacity Subsystem	RAW/CCF	This VWS subsystem provides chilled cooling water to the CVS makeup pump room. The motor-driven pumps, chillers and unit cooler fans are important components of the VWS.
<b>System: Onsite Standby Power System (ZOS)</b>		
Nonsafety-related Standby Diesel Generators	EP	These diesels provide ac power to support operation of nonsafety-related equipment such as the startup feedwater pumps, CVS pumps, RNS pumps, CCS pumps, SWS pumps, and the PLS. Providing ac power to the RNS and the equipment necessary to support its operation is RTNSS-important for reduced inventory conditions.

Table 17.4-1 (Sheet 10 of 10)

**RISK-SIGNIFICANT SSCs WITHIN THE SCOPE OF D-RAP**

System, Structure, or Component (SSC) <sup>(1)</sup>	Rationale <sup>(2)</sup>	Insights and Assumptions
Standby Diesels Room Cooling Fans	EP	These fans provide cooling of the rooms containing the standby diesel generators.
Nuclear Fuel	SMA	The nuclear fuel includes the fuel pellets, fuel cladding, and associated support structures. This equipment, which provides a first barrier for release of radioactivity and allows for effective core cooling, had the least margin in the seismic margin analysis.

**Notes:**

1. Only includes equipment at the **component** level. Other parts of the SSC or support systems are not included unless specifically listed.
2. Definition of Rationale Terms:
  - CCF = Common Cause Failure (for the SSCs whose inclusion rationale is RAW/CCF, the RAW is based on common cause failure of two or more of the specified SSCs.
  - EP = Expert Panel
  - RAW = Risk Achievement Worth
  - RRW = Risk Reduction Worth
  - SMA = Seismic Margin Analysis
3. Maintenance/surveillance recommendations for equipments are documented in each appropriate DCD section.
4. This category captures instrumentation and control equipment common cause failures across systems.

Table 17.4-2

**EXAMPLE OF RISK-SIGNIFICANT RANKING OF SSCs FOR THE AUTOMATIC  
DEPRESSURIZATION SYSTEM**

<b>Rank<sup>(1)</sup></b>	<b>Event Code</b>	<b>Description</b>
1	ED3MOD07	EDS3 EA1 distribution panel failure or unavailable due to testing and maintenance
2	AD4MOD07, AD4MOD08, AD4MOD09, AD4MOD10	Hardware failure of 2 of 4 automatic depressurization system Stage 4 lines (includes squib valves)
3	EC1BS001TM, ECBS012TM, EC1BS121TM, EC2BS002TM, EC2BS022TM, EC2BS221TM	Unavailability of bus ECS ES due to unscheduled maintenance
4	AD2MOD01, AD2MOD02, AD2MOD03, AD2MOD04	Hardware failure of automatic depressurization system Stages 2 and 3 of lines 1 and 2 (includes motor-operated valves)
5	EC0MOD01	Main generator breaker ES01 fails to open
6	ED3MOD01	Fixed component fails: circuit breaker, inverter or static transfer switch
7	ZO1MOD01, Z02MOD01	Diesel generator fails to start and run or breaker 102 fails to close
8	Z02DG001TM, Z02DG001TM	Standby diesel generator unavailable due to testing and maintenance

**Note:**

1. The ranking is the order of the decreasing risk achievement component importance.

D-RAP Phase I

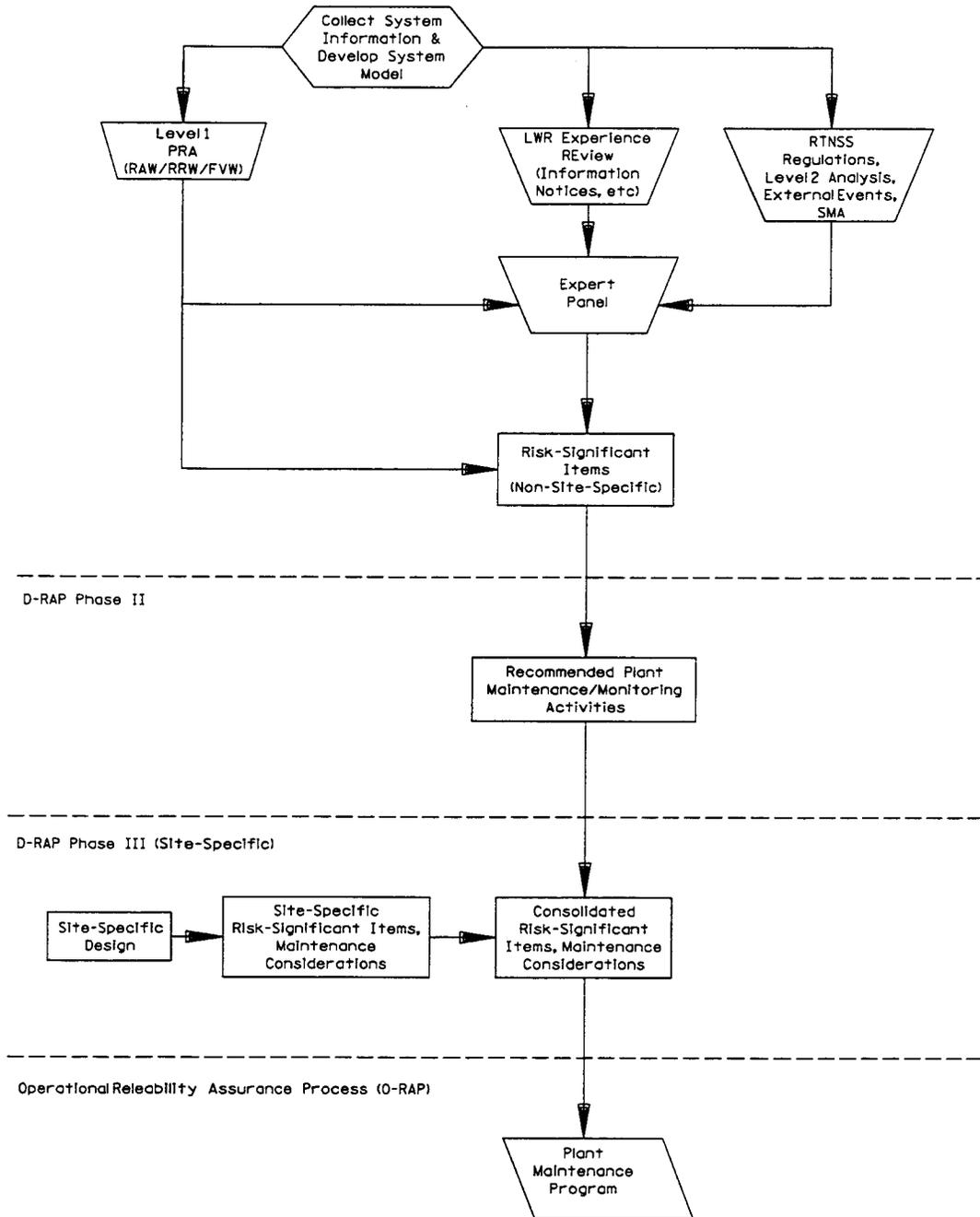


Figure 17.4-1

**Design Reliability Assurance Program and O-RAP**