7 INSTRUMENTATION AND CONTROLS

7.1 Introduction

The AP1000 Design Control Document (DCD) Tier 2 Chapter 7, “Instrumentation and Controls” contains the description of and commitments pertaining to the primary instrumentation and control (I&C) systems of the AP1000 design. The I&C systems provide protection against unsafe reactor operation during steady-state and transient power operations. In addition, they initiate selected protective functions to mitigate the consequences of design-basis events and accidents, and to safely shutdown the plant either by automatic means or by manual actions.

DCD Tier 2 Section 7.1, “Introduction,” describes the AP1000 general I&C system architecture, with specific emphasis on the protection and safety monitoring system (PMS) design and design process. DCD Tier 2 Section 7.2, “Reactor Trip,” discusses the I&C aspects of the reactor trip function. DCD Tier 2 Section 7.3, “Engineered Safety Features,” addresses the engineered safety feature actuations. Systems required for safety shutdown are discussed in DCD Tier 2 Section 7.4, “Systems Required for Safe Shutdown.” Safety-related display information is discussed in DCD Tier 2 Section 7.5, “Safety-Related Display Information.” Interlocks important to safety are discussed in DCD Tier 2 Section 7.6, “Interlock Systems Important to Safety.” Control systems and diverse actuation system are discussed in DCD Tier 2 Section 7.7, “Control and instrument Systems."

7.1.1 Acceptance Criteria

The acceptance criteria used as the basis for the staff's review are set forth in the Standard Review Plan (SRP), NRC technical report designation (NUREG-0800), that includes Title 10 of the Code of Federal Regulations (10 CFR) Part 50, “Domestic Licensing of Production and Utilization Facilities,” and 10 CFR Part 52, "Early Site Permits; Standard Design Certifications; and Combined Licenses for Nuclear Power Plants." The primary section of the SRP used for this review is Chapter 7, "Instrumentation and Controls," Revision 4 dated June 1997.

SRP Chapter 7 provides guidance for the review of I&C systems in light-water nuclear power plants. Revision 4 identifies the procedures for reviewing digital systems. These procedures are in SRP Chapter 7 Appendix 7.0-A; SRP Chapter 7 Appendix 7.1-A; SRP Sections 7.1, 7.8, and 7.9; and Branch Technical Position (BTPs) Instrumentation and Controls Branch (HICB)-11, HICB-14, HICB-17, HICB-18, HICB-19, and HICB-21. SRP Appendix 7.1-C and SRP Sections 7.2 through 7.7 provide additional review guidance.

The following regulations are also listed in SRP Chapter 7 as being applicable to digital I&C systems:

- 10 CFR 50.55a(a)(1)
- 10 CFR 50.55a(h)

- 10 CFR 50.62
- 10 CFR Part 50, Appendix A, “General Design Criteria (GDC), for Nuclear Power Plants,” as follows:
  - GDC 1, “Quality Standards and Records”
  - GDC 2, “Design Basis for Protection Against Natural Phenomena”
  - GDC 4, “Environmental and Dynamic Effects Design Bases”
  - GDC 12, “Suppression of Reactor Power Oscillations”
  - GDC 13, “Instrumentation and Control”
  - GDC 19, “Control Room”
  - GDC 20, “Protection System Functions”
  - GDC 21, “Protection System Reliability and Testability”
  - GDC 22, “Protection System Independence”
  - GDC 23, “Protection System Failure Modes”
  - GDC 24, “Separation of Protection and Control Systems”
  - GDC 25, “Protection System Requirements for Reactivity Control Malfunctions”
  - GDC 29, “Protection Against Anticipated Operational Occurrences”

The following regulatory guides and industry standards provide information, recommendations, and guidance, and are acceptable bases for implementing the above-noted requirements for hardware and software features of safety-related digital systems:

- Institute of Electrical and Electronics Engineers (IEEE) Standard (Std) 7-4.3.2-1982, "Application Criteria for Programmable Digital Computer Systems in Safety Systems of Nuclear Power Generating Stations," as endorsed by Regulatory Guide (RG) 1.152, "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants"
- IEEE Std 323-1974, "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations," as endorsed by RG 1.89, "Qualifications for Class 1E Equipment for Nuclear Power Plants"
- IEEE Std 338-1987, "IEEE Standard Criteria for Periodic Testing of Nuclear Power Generating Station Safety Systems," as endorsed by RG 1.118, "Periodic Testing of Electric Power and Protection Systems"
- IEEE Std 344-1987, "IEEE Recommended Practices for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations"
- IEEE Std 379-1988, "Application of the Single Failure Criterion to Nuclear Power Generating Station Class 1E Systems," as endorsed by RG 1.53, "Application of the Single-Failure Criterion to Nuclear Power Plant Protection Systems"
- IEEE Std 384-1992, "Criteria for Independence of Class 1E Equipment and Circuits," as endorsed by RG 1.75, "Physical Independence of Electrical Systems"
- IEEE Std 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," as endorsed by RG 1.153, "Criteria for Power, Instrumentation, and Control Portions of Safety Systems"
- IEEE Std 730-1989, "Software Quality Assurance Plans," as referenced in BTP HICB-14, "Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems."

- IEEE Std 828-1990, "Software Configuration Management Plans," as endorsed by RG 1.169, "Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants"
- IEEE Std 829-1983, "Software Test Documentation," as endorsed by RG 1.170, "Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants"
- IEEE Std 830-1984, "Guide for Software Requirements Specifications," as endorsed by RG 1.172, "Software Requirements Specification for Digital Computer Software Used in Safety Systems of Nuclear Power Plants"
- IEEE Std 1012-1986, "IEEE Standard for Software Verification and Validation Plans," as endorsed by RG 1.168, "Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants"
- IEEE Std 1016-1987, "IEEE Standard for Recommended Practices for Software Design Descriptions"
- IEEE Std 1028-1988, "IEEE Standard for Software Reviews and Audits," as endorsed by RG 1.168
- IEEE Std 1042-1987, "IEEE Guide to Software Management," as endorsed by RG 1.169
- IEEE Std 1074-1995, "IEEE Std for Developing Software Life Cycle Processes," as endorsed by RG 1.173, "Developing Software Life Cycle Processes for Digital Computer Systems used in Safety Systems of Nuclear Power Plants"
- MIL-STD-461C, "Electromagnetic Emission and Susceptibility Requirements for the Control of Electromagnetic Interference"
- IEC Std 880, "Software for Computers in the Safety Systems of Nuclear Power Stations," as referenced in the SRP
- ASME NQA-2a-1990, Part 2.7, "Quality Assurance Requirements of Computer Systems for Nuclear Facility Applications," as referenced in the SRP
- Electric Power Research Institute (EPRI) Topical Report TR-107330, "Generic Requirements Specification for Qualifying a Commercially Available PLC [Programable Logic Controller] for Safety-Related Applications in Nuclear Power Plants," approved by the NRC on July 30, 1998
- EPRI Topical Report TR-102323-R1, "Guidelines for Electromagnetic Interference Testing in Power Plants," approved by the NRC on April 16, 1996
- EPRI Topical Report TR-106439, "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications," approved by the NRC in April 1997

7.1.2 Basis and Method of Review

The AP1000 I&C system uses a microprocessor-based distributed digital system to perform plant protection functions and safety monitoring, as well as plant control functions. To ensure that the digital I&C system is implemented properly, the staff considered existing regulatory requirements, guides, and standards in the SRP, and additional standards applicable to digital systems. The use of digital computer technology in protection and control systems raises the possibilities that software for these computer systems could be vulnerable to programming errors and lead to safety-significant common-mode failures. The primary factors for defense

against common-mode failures are quality and diversity in the digital I&C system design. This is discussed further in Sections 7.1.3, 7.1.4, 7.1.5, and 7.1.6 of this report.

The AP1000 uses passive safety systems that rely on natural forces such as density differences, gravity, and stored energy to provide water for core and containment cooling. The active AP1000 systems are not classified as safety-related, and credit is not taken for these active systems in the design-basis accident analyses described in DCD Tier 2 Chapter 15, “Accident Analysis,” unless their operation makes the consequences of an accident more limiting. The non-safety-related active systems in the AP1000 provide defense-in-depth functions and supplement the capability of the safety-related passive systems.

This report also describes certain items that will be included in the, DCD Tier 1, “Information,” which includes the design description; the inspections, tests, analyses and acceptance criteria (ITAAC); and the interface requirements for design certification. The Tier 1 Information development process, its bases, and its acceptability are discussed in Chapter 14 of this report. Chapter 7 of this report discusses only those areas that relate specifically to the I&C systems' certified design process, in addition to specific I&C design characteristics. References to previously reviewed plant designs and topical reports are provided where applicable.

7.1.3 General Findings

DCD Tier 2 Chapter 7 for the AP1000 design has been written to provide for the use of either the I&C systems similar to the AP600 design or the Common Qualified Platform design as described in Topical Report CENPD-396-P, Revision 1, "Common Qualified Platform," issued May 2000.

7.1.3.1 Compliance with SRP Criteria

The acceptance criteria listed in SRP Table 7-1 identifies the Commission's regulations and industry codes and standards applicable to I&C system design. The SRP provides additional review guidance and acceptance criteria that are not provided in the specified requirements, standards, and other references. SRP Table 7-1 provides a cross-reference to the DCD sections that address the applicable standards and criteria. In general, the applicant has committed to meet the SRP guidance with few exceptions. The few exceptions that the applicant has requested are noted in DCD Tier 2 Sections 1.9, “Compliance with Regulatory Criteria,” and 3.1, “Conformance with Nuclear Regulatory Commission General Design Criteria,” and the applicable sections of this report. The most important aspects of those criteria that are required to be certified by rule-making will be included in DCD Tier 1. This information is discussed in Section 7.1.4 of this report.

The requirements of 10 CFR Part 50, Appendix A, contains the GDC applicable to I&C systems. DCD Tier 2 Section 3.1 generally discusses compliance with the requirements of the GDC, and references other DCD chapters for specifics.

SRP Chapter 7 Appendix 7-B, "General Agenda, Station Site Visits," provides a general agenda for the station site visit related to the I&C systems, and includes verification of layouts,

separation and isolation, test features, and potential for damage due to fire, flooding, or other environmental effects. Since the design certification for the AP1000 design under 10 CFR Part 52 will be issued before a construction site is selected, this SRP review item cannot be completed at this stage of the review. The inspection tasks identified (in SRP Chapter 7 Appendix 7-B) as necessary for design certification will be addressed through the ITAAC process and commitments to pre-operational tests described in DCD Tier 2 Chapter 14. The review described in SRP Chapter 7 Appendix 7-B will be accomplished as part of the testing and inspections done by the Combined License (COL) applicants referencing the AP1000 certified design.

7.1.3.2 Compliance with Industry Standards

DCD Tier 2 references IEEE Standard 603 for the design of the AP1000 I&C systems. 10 CFR 50.55a(h) requires protection systems to meet the requirements of IEEE Standard 603-1991. DCD Tier 2 Section 7.1.4.2, “Conformance With Industry Standards” listed other IEEE Standards which have been found acceptable by the NRC staff through RG endorsement or inclusion in the SRP. The DCD further references Westinghouse Topical Report CENPD-396-P for detailed design of the PMS. Topical Report CENPD-396-P Section 4, identifies the Common Qualified Platform's compliance to the Industry Codes and Standards. The staff regards the application of acceptable standards throughout the I&C system design and production process as an important element of the quality demonstration. The application for the design certification must contain a level of information sufficient to enable the staff to make its safety determination. The staff concludes that an explicit commitment to industry hardware- and software-related standards is important in achieving high quality in the digital I&C system product.

7.1.3.3 Compliance with 10 CFR Part 52

Since the AP1000 has been submitted for design certification, the requirements of 10 CFR Part 52 apply in addition to those of 10 CFR Part 50. 10 CFR Part 52 requires a level of design detail beyond a simple commitment to conformance with the existing requirements. The requirement of 10 CFR 52.47(a)(2) specifies that:

> The application must contain a level of design information sufficient to enable the Commission to judge the applicant's proposed means of assuring that construction conforms to the design and to reach a final conclusion on all safety questions associated with the design before the certification is granted. The information submitted for a design certification must include performance requirements and design information sufficiently detailed to permit the preparation of acceptance and inspection requirements by the NRC, and procurement specifications and construction and installation specifications by an applicant. The Commission will require, prior to design certification, that information normally contained in certain procurement specifications and construction and installation specifications be completed and available for audit if such information is necessary for the Commission to make its safety determination.

The requirements 10 CFR 52.47(b)(1) also states that, ". . . this rule must provide an essentially complete nuclear power plant design except for site-specific elements." The following sections of this report describe the information provided by the applicant (and the staff's conclusions concerning conformance with the SRP criteria), additional criteria necessary to address digital I&C technology, and the above requirements of 10 CFR Part 52.

The applicant has not completed developing the design of the AP1000 digital I&C system. Therefore, the staff's safety determination under 10 CFR Part 52 will rely on a satisfactory demonstration by the COL applicant that the digital I&C system design development process, as documented in the DCD, will ensure a quality product. The staff will then confirm the effectiveness of the COL applicant's implementation of this process through audits of the ITAAC implementation at various phases of the design development. The design acceptance criteria (DAC) approach enables the staff to conclude that if the I&C system design is implemented in accordance with the design process; the associated inspections, tests and analyses performed; and the acceptance criteria (ITAAC) will verify that the system will be operated in accordance with the design certification.

7.1.4 Tier 1 Material

In an August 28, 2000, letter, as supplemented by letter dated February 13, 2002, the applicant requested the staff to review the acceptability of the applicant's proposed use of DAC to support the development of the design certification application for the AP1000 design. As a result of its pre-application review, in Office of the Secretary of the Commission (SECY)-02-0059, "Policy Issue Information," dated April 1, 2002, the staff concluded that the use of DAC in the I&C and control room (human factors engineering) areas is acceptable because these areas are characterized by a rapidly changing technology. Requiring completion of the design at the design certification stage may result in the design becoming obsolete by the time a plant is constructed. The staff concludes, in SECY-02-0059, that it is acceptable to use the DAC approach in the I&C, control room (human factor engineering), and piping design areas, contingent upon the ability of the applicant and the staff to agree on adequate DAC during the design certification review. Although recognizing the DAC approach as a possible substitute for required design details, the staff concluded that the use of DAC, instead of detailed design information, should be limited. The restrictions should be based upon a consideration of those design areas affected by rapidly changing technologies, or design areas for which as-built, or as-procured, information is not available.

The concept of DAC would enable the staff to make a final safety determination, subject only to satisfactory design implementation and verification by the COL applicant, through appropriate use of ITAAC. The staff defined DAC as a set of prescribed limits, parameters, procedures, and attributes upon which the NRC relies, in a limited number of technical areas, in making a final safety determination to support a design certification. The acceptance criteria for DAC become the acceptance criteria for ITAAC, which are part of the design certification, and called Tier 1 Material (or Tier 1 Information).

In Volume 1 of the DCD, the applicant provided the Tier 1 Information. The Tier 1 Information contains the design descriptions and associated inspections, tests, analyses, and acceptance

criteria. The applicant organized its AP1000 Tier 1 Information in a manner similar to that used for the evolutionary designs (ABWR & System 80+) and the AP600 design. The I&C systems Tier 1 information, that includes system descriptions and ITAAC, proposed by the applicant for AP1000 is similar to AP600 Tier 1 information. DCD Tier 1 Section 2.5 identifies the I&C systems design description and ITAAC. It includes:

- 2.5.1 Diverse Actuation System
- 2.5.2 Protection and Safety Monitoring System
- 2.5.3 Plant Control System
- 2.5.4 Data Display and Processing System
- 2.5.5 In-core Instrumentation System
- 2.5.6 Special Monitoring System
- 2.5.7 Operation and Control Centers System
- 2.5.8 Radiation Monitoring System
- 2.5.9 Seismic Monitoring System
- 2.5.10 Main Turbine Control and Diagnostic System

The staff's review of Tier 1 information is addressed in Section 14.3 of this report.

7.1.5 I&C System Architecture

The AP1000 I&C systems are comprised of the following major systems:

- PMS
- plant control system (PLS)
- operation and control centers system (OCS)
- data and display processing system (DDS)
- in-core instrumentation system (IIS)
- special monitoring system (SMS)
- diverse actuation system (DAS)

The PMS monitors the plant processes using a variety of sensors, performs calculations, comparisons, and logic functions based on those sensor inputs, and actuates a variety of equipment. Most of the time, the PMS operates automatically without input from plant personnel except for system start-up, testing, calibration, and maintenance. The PMS is used to operate safety-related systems and components and includes the following major components:

- plant protection subsystems
- engineered safety features coincidence logic
- engineered safety features actuation subsystems
- reactor trip switchgear
- qualified data processing subsystems
- main control room and remote shutdown workstation multiplexers
- sensors
- communication features

- maintenance, test, and bypass features

The PLS controls and coordinates the plant systems during start-up, ascent to power, power operation, and shutdown conditions; integrates the automatic and manual control of the reactor, reactor coolant, and various reactor support processes for required normal and off-normal conditions; controls the non-safety-related decay heat removal systems during shutdown; and permits the operator to control plant components from the main control room or remote shutdown workstation. The PLS accomplishes these functions through use of the following features:

- Rod control
- Pressurizer pressure and level control
- Steam generator (SG) water level control
- Steam dump (turbine bypass) control
- Rapid power reduction

The OCS includes the complete operational scope of the main control room, remote shutdown workstation, the technical support center, emergency operations facility, local control stations and associated workstations for these centers.

The DDS comprises the equipment used for processing data that results in non-Class 1E alarms and displays for both normal and emergency plant operations.

The IIS provides the flux map of the reactor core and in-core thermocouple signals for post-accident monitoring.

The SMS provides loose parts monitoring of the reactor coolant system.

The DAS provides a backup to the PMS for some specific diverse automatic or manual actuation, and provides diverse indications to assist in operator manual actions. The DAS is a defense-in-depth system that is designed to provide essential protection functions in the event of a postulated common-mode failure of the PMS.

7.1.6 Defense-in-Depth and Diversity Assessment of the AP1000 Protection System

The first design reviewed by the staff specifically to address defense against potential common-mode failures in digital systems was the Westinghouse RESAR-414 standardized design. The results of the staff's review of RESAR-414 were published in NUREG-0493, "A Defense-in-Depth and Diversity Assessment of the RESAR-414 Integrated Protection System," issued March 1979. NUREG-0493 discussed common-mode failures and different types of diversity, and presented a method for assessing the defense-in-depth of the design.

The staff described concerns with common-mode failures and other digital system design issues in SECY-91-292, "Digital Computer Systems for Advanced Light Water Reactors," dated

September 16, 1991. SECY-91-292 describes how common-mode failures could defeat the redundancy achieved by the hardware architectural structure, but could also result in the loss of more than one echelon of defense-in-depth provided by the monitoring, control, reactor protection, and engineered safety functions performed by the digital I&C systems. The two principle factors for defense against common-mode/common-cause failures are quality and diversity. Maintaining high quality will increase the reliability of both individual components and complete systems. Diversity in assigned functions (for both equipment and human activities), equipment, hardware, and software can reduce the consequences of a common-mode failure.

The modules in the AP1000 PMS are to be implemented by microprocessor-based designs with identical or similar hardware and software used in all four divisions. Because of this similarity, the concerns expressed in NUREG-0493 and SECY 91-292 apply directly to the PMS.

Several regulations and industry standards address the need for defense against potential common-mode failures:

- GDC 22, "Protection System Independence," requires that "design techniques, such as functional diversity or diversity in component design and principles of operation, shall be used to the extent practical to prevent loss of the protection function."

- 10 CFR 50.55a(h) (IEEE 603-1991) requires that "equipment, not subject to failure caused by the same credible event, shall be provided to detect the event..."

- IEEE 379-1988 states that "certain common-cause failures shall be treated as single failures when conducting the single failure analysis. Such failures can be in dissimilar components and can have dissimilar failure modes."

Also, 10 CFR 50.62 addresses common-mode failure issues concerning mitigation of anticipated transients without scram (ATWS).

Common-cause failures not subject to single-failure analysis include those that can result from external environmental effects, design deficiencies, manufacturing errors, and operator errors. Design qualification and quality assurance programs are intended to afford protection from external environmental effects, design deficiencies, and manufacturing errors. Personnel training, proper control room design, and operating and maintenance procedures are intended to afford protection from maintenance and operator errors.

NUREG-0493 discusses several different types of diversity, each of which offers certain protection against common-mode failures. For example, neutron flux and reactor pressure are diverse signals for initiation of reactor scram. Equipment diversity includes using different kinds of equipment to perform a function. An example of equipment diversity described in NUREG-0493 is the use of relay versus solid-state logic in the I&C system. It is difficult to define how much improvement in safety results from a given kind or degree of diversity. For microprocessor design, this is especially difficult because there is no industry consensus on a method to quantify software reliability and/or availability.

As stated above, the staff considers the two principle factors for defense against common-mode failures to be quality and diversity. The quality in the design process aspects of the AP1000 I&C systems is addressed in Section 7.2.8 of this report. Quality is achieved, in part, by the use of quality design standards for the hardware and software, and by the I&C system testing to be performed.

The staff's position on I&C system diversity for advanced light water reactors (ALWRs) stated in SECY-93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor Design," April 2, 1993, as approved by the Commission in an SRM dated July 21, 1993, is as follows:

1. The applicant shall assess the defense-in-depth and diversity of the proposed I&C system to demonstrate that vulnerabilities to common mode failures have been adequately addressed.

2. In performing the assessment, the vendor or applicant shall analyze each postulated common-mode failure for each event that is evaluated in the accident analysis section of the Safety Analysis Report using best-estimate methods. The vendor or applicant shall demonstrate adequate diversity within the design for each of these events.

3. If a postulated common-mode failure could disable a safety function, then a diverse means, with a documented basis that the diverse means is unlikely to be subject to the same common mode failure, shall be required to perform either the same function or a different function. The diverse or different function may be performed by a non-safety system if the system is of sufficient quality to perform the necessary function under the associated event conditions.

4. A set of displays and controls located in the main control room shall be provided for manual system-level actuation of critical safety functions and monitoring of parameters that support the safety functions. The displays and controls shall be independent and diverse from the safety computer system identified in Items 1 and 3 above.

Staff review guidance on this position is included in the SRP Chapter 7, Appendix 7-A, BTP 19, "Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems."

In response to the NRC staff's position on I&C system diversity for ALWRs, the applicant submitted WCAP-15775, "AP1000 Instrumentation and Control Defense-in-Depth and Diversity Report," issued April 2002, which describes the diversity and defense-in-depth features of the AP1000 instrumentation and control architecture following the guidelines outlined in BTP-19. The staff finds that the report demonstrated conformance to the acceptance criteria in BTP-19.

The analysis to protect against common-mode failure in the AP1000 I&C architecture was done as part of the probabilistic risk assessment (PRA) for the AP1000 design. In the PRA, failures of the I&C system architecture including common cause failures were analyzed. The PMS analysis is described in AP1000 PRA Revision 2 Chapter 26, "Protection and Safety Monitoring System", and the PLS is described in PRA Revision 2 Chapter 28, "Plant Control System," of the PRA document. The analyses of the diverse, non-safety-related DAS is described in PRA Revision 2 Chapter 27, "Diverse Actuation System."

In addition, the applicant submitted WCAP-13793, "AP600 System/Event Matrix" issued 1994, which describes how the AP600 systems are used to protect the reactor during different events. For each event, WCAP-13793 lists different safety and non-safety-related systems which are used to protect the reactor, and identifies systems that provide reactor shutdown, reactor coolant system (RCS) makeup, core decay heat removal, and containment cooling. This topical report also includes the type of actuation and electrical power requirements for each system. The purpose of this document is to demonstrate that there are multiple levels of defense for each type of event. The DAS has been credited with providing reactor protection functions in every event analyzed. WCAP-13793 is an AP600 document. Since the AP1000 systems which are used to protect the reactor, shut down the reactor, provide RCS makeup, provide core decay heat removal, and provide containment cooling the same as those in AP600, the staff finds that the analyses described in the WCAP-13793 is applicable to AP1000.

Based on its review, the staff finds that the applicant has assessed the defense-in-depth and diversity of the AP1000 I&C system and demonstrated that vulnerabilities to common-mode failures have been adequately addressed. The applicant has analyzed each postulated common-mode failure for each event that is evaluated in the accident analysis section of the DCD, and has addressed the diversity requirements within the design for each of these events. The DAS, as proposed, performs the same functions as the PMS when a postulated common-mode failure disables the PMS protection functions. In addition, the DAS, as proposed, has displays, independent and diverse from the PMS, that can support the manual actions to be performed in the event a postulated common-mode failure disables the PMS. Therefore, the staff concludes that the proposed design satisfies the Commission's position on I&C system diversity. The evaluation of the DAS is discussed further in Section 7.7.2 of this report.

7.1.7 Commercial-Grade Item Dedication

Digital components to be used in safety systems must be qualified for their intended application either by a 10 CFR Part 50, Appendix B quality assurance program or by dedicating the item for use in the safety system as defined in 10 CFR Part 21. NRC has approved the EPRI Topical Report TR-106439, "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications," in 1997. The "Requirements on the Dedicator" section in EPRI TR-106439 states the following:

> The process of performing commercial-grade item procurement and dedication activities is itself a safety-related process and, as such, must be controlled and performed in accordance with a quality assurance (QA) program that meets the

> requirements of 10 CFR [Part] 50[,] Appendix B. This applies to the dedicating entity whether it is the utility or a third-party dedicator.

The applicant is an approved 10 CFR Part 50, Appendix B supplier. The staff does not attempt in this review to renew the applicant's status as an approved 10 CFR Part 50, Appendix B supplier. During the review of the Common Qualified Platform, the staff audited a sampling of manuals for commercial grade dedication activities. On the basis of the audit, the staff finds that the procedures and processes in the manuals correspond to the requirements of IEEE 7-4.3.2 and the guidance of EPRI TR-106439 and, therefore, provide an acceptable program for the dedication of commercial-grade items. During the review of the Common Qualified Platform, the staff has reviewed the reports of the dedication of commercial-grade AC160 hardware and software for use in nuclear safety systems. On the basis of that review, the staff concludes that the AC160 Programmable Logic Controllers system meets the requirements set forth in BTP HICB-18, "Guidance on the use of Programmable Logic Controllers in Digital Computer-Based Instrumentation and Control Systems," and follows the guidance in EPRI TR-106439 and is, therefore, acceptable for use in nuclear power plants.

On the basis of the staff's review of the Common Qualified Platform flat panel display system (FPDS), the staff concludes that the applicant has acceptably dedicated the commercial-grade QNX4, Version 4.25b and Photon microGUI, Version 1.13b in accordance with the guidance in EPRI TR-106439 for use as the operating system and display builder for the FPDS in the Common Qualified Platform.

Included in the commercial dedication issue is the qualification of the automated tools and design support software. It is necessary for the I&C system developer to verify that the tools function correctly. The staff expects the developer to verify the quality of the tools used in the design.

Also related to the issue of commercial dedication, is the staff's concern regarding communication by the suppliers to the end-user of errors discovered in the suppliers' tools or software. This is similar to the 10 CFR Part 21 defect reporting required for Class-1E equipment vendors. The COL applicant referencing the AP1000 Commercial Dedication Program shall commit that any change to the software commercial dedication process of the safety-related system requires NRC review and approval before implementation. Any request for changes should either be specifically described in the COL application or submitted for license amendment after issuance of the license. This is addressed generically in DCD Tier 2 Section 7.1.6, "Combined License Information," where it states that the "Combined License applicants referencing the AP1000 certified design will provide resolution for generic open items and plant-specific action items resulting from NRC review of the I&C platform." This is COL Action Item 7.1.7-1.

7.2 Reactor Trip System

7.2.1 System Description

The reactor trip system (RTS) performs the reactor scram function by interrupting electrical power to the rod control system and allowing the control rods to fall by gravity into the reactor core. The RTS includes power sources, sensors, communication links, software/firmware, initiation circuits, logic matrices, bypasses, interlocks, switchgear, actuation logic, and actuated devices that are required to initiate a reactor trip. The RTS is designed to automatically initiate the rapid insertion of the control rods of the reactivity control system to ensure that the specified acceptable fuel design limits are not exceeded. Manual initiation is also provided as a backup to automatic initiation. The RTS also provides status information to the operator, and status and control signals to other systems and annunciators. The RTS, which is qualified as a Class 1E safety system and is environmentally and seismically qualified, provides the following reactor trip functions:

- nuclear start up trips
  - source range high neutron flux trip
  - intermediate range high neutron flux trip
  - power range high neutron flux trip (low setpoint)
- nuclear overpower trips
  - power range high neutron flux trip (high setpoint)
  - power range high positive flux rate trip
- core heat removal trips
  - overtemperature delta T trip
  - overpower delta T trip
  - low pressurizer pressure trip
  - low reactor coolant flow trip
  - reactor coolant pump underspeed trip
  - high reactor coolant pump bearing water temperature trip
- primary system overpressure trips
  - high pressurizer pressure trip
  - high pressurizer water level trip
- loss of heat sink trip
  - low SG water level trip (in any SG)

- feedwater isolation trip
  - High-2 SG water level in any SG trip
- automatic depressurization system actuation trip
- core makeup tank injection trip
- safeguard actuation trip
- manual trip

The RTS automatically initiates rapid insertion of the control rods to scram the reactor when warranted by any one of the predetermined conditions listed above. The reactor trip is initiated by means of four redundant divisions of sensor channels, trip logic, and trip actuators (except the manual scram function, which can be accomplished from the main control room by two redundant switches). The RTS is a four division system where each parameter is monitored by four sensor channels, one in each division. Each division of sensor channels is powered from the respective Class-1E battery-backed power supply. The coincidence logic (two-out-of-four) requires the two tripped signal inputs from the same parameter. The RTS will periodically be tested during plant operation as defined by the technical specifications in DCD Tier 2 Chapter 16.

Complete electrical and physical separation is maintained between the four RTS divisions in order to meet the criteria of IEEE 603-1991. This requirement will be verified during the implementation of the ITAAC as defined in DCD Tier 1 Section 2.5.2. A trip of any sensor or logic channel is annunciated and causes that channel to lock in the trip mode until manually reset. The RTS is fail-safe in that a loss of power to a channel will result in that channel going to the tripped condition. Other failures, such as a break in a communications link, are detected by the self-diagnostics of the individual microprocessor that will put the output to the tripped state.

The staff reviewed the RTS for conformance to 10 CFR 50.55a(h)(3) (which requires conformance to the requirements of IEEE Standard 603-1991, and correction sheet dated January 30, 1995). IEEE 603 includes the requirements for meeting the single-failure criterion, independence, control and protection system interaction (isolation), testing, bypass and bypass indication (including removal of bypass), and manual initiation. The staff concludes that the RTS description and drawings in the DCD establish a clear commitment to the above requirements of IEEE 603.

7.2.2 Protection and Safety Monitoring System Description

The PMS provides detection of off-normal conditions and actuation of appropriate safety-related functions necessary to achieve and maintain the plant in a safe shutdown condition. The PMS controls safety-related components in the plant that are operated from the main control room or

remote shutdown workstation. In addition, the PMS provides the equipment necessary to monitor the plant safety-related functions during and following an accident as required by RG 1.97.

The PMS for the AP1000 implements its functions by software logic installed in programmable digital devices (data processors). Plant data and other signals are exchanged between data processors by means of isolated data links and data highways. The functions of the PMS are implemented in separate processor-based subsystems. Each subsystem is located on an independent computer bus to prevent propagation of failures and to enhance availability. Each subsystem is implemented in a separate card chassis. Subsystem independence is maintained by the following design features:

- Separate dc power sources for redundant subsystems with output protection to prevent interaction between redundant subsystems upon failure of a subsystem.
- Separate input or output circuitry to maintain independence at the subsystem interfaces.
- Deadman signals: A device, circuit, or function that forces a predefined operating condition on the cessation of a normal dynamic input parameter to improve the reliability of hard-wired data that crosses the subsystem interface.
- Optical coupling or resistor buffering between two subsystems or between a subsystem and an input/output module.

WCAP-13382, “AP600 Instrumentation and Control Hardware Description,” issued May 1992, and WCAP-14080, “AP600 Instrumentation and Control Software Architecture and Operation Description,” issued June 1994 provide a detailed description of the AP600 PMS design. These two topical reports were accepted by the staff under AP600 design certification. Based on the review of the topical reports, the staff found that they conform to standards and guidelines discussed in the SRP Chapter 7. Since the I&C system architecture, hardware and software of AP1000 PMS and the systems, equipment, and components that PMS controls and monitors are the same as those in AP600, the staff finds that these two topical reports are applicable to the AP1000 design.

Alternatively, the AP1000 PMS may be based on the Common Qualified Platform design as described in Topical Report CENPD-396-P. The evaluation of the Common Qualified Platform design is addressed in Sections 7.2.3 and 7.2.4 of this report. The PMS initiates an automatic reactor trip and automatic actuation of engineered safety features. The PMS 2-out-of-4 initiation logic reverts to a 2-out-of-3 coincidence logic if one of the 4 channels is bypassed. The PMS (using the Common Qualified Platform design) does not allow simultaneous bypass of 2 redundant channels. The PMS has redundant divisions of safety-related postaccident parameter display. Each PMS division is powered from its respective Class 1E dc and uninterruptible power supply (UPS) division. Dedicated fixed position controls and indications are provided in the main control room for the reactor trip and the engineered safety feature functions.

Reliability of the PMS is provided by the following features:

- The reactor trip functions are divided into two subsystems.
- The ESF functions are processed by two microprocessor-based subsystems that are functionally identical in both hardware and software.
- Continuous monitoring and failure detection/alarm is provided.
- The PMS equipment is designed to accommodate a loss of normal heating, ventilation, and air conditioning (HVAC). PMS equipment is protected by the passive heat sinks upon failure or degradation of the active HVAC.
- The PMS equipment is under the design reliability assurance program (D-RAP).

7.2.3 Common Qualified Platform Design and COL Action Items

The detailed design of the Common Qualified Platform is described in Topical Report CENPD-396-P. The staff issued safety evaluations approving the Common Qualified Platform in August 11, 2000, June 22, 2001, and April 2, 2003. The Common Qualified Platform is designed as a standard digital I&C platform with a modular structure for nuclear safety related applications, including component replacement and complete system upgrades. The Common Qualified Platform is applicable to post accident monitoring systems, core protection calculator systems, reactor protection systems, plant protection systems, engineered safeguards systems and other nuclear safety related applications. The Common Qualified Platform is a computer system consisting of a set of commercial-grade hardware and previously developed software components dedicated and qualified for use in nuclear power plants.

On August 11, 2000, the NRC staff issued a safety evaluation report entitled, “Acceptance for Referencing of Topical Report CENPD-396-P. Section 6 of that safety evaluation report identified 14 plant specific action items. In response to the staffs AP1000 request for additional information (RAI) 420.028, the applicant addressed each of these 14 plant specific action items (PSAI). These items are covered by the ITAAC process that will verify the design requirements. The ITAAC process is documented in DCD Tier 1 Section 2.5.2. The resolutions on each of these PSAIs are addressed as follows:

PSAI 6.1: Each licensee implementing a specific application based upon the Common Qualified Platform must assess the suitability of the S600 I/O modules to be used in the design against its plant-specific I/O requirements.

Resolution: The Quality Assurance Program described in DCD Tier 2 Chapter 17 for procurement, fabrication, installation, construction and testing of systems and components in the facility will cover this issue.

PSAI 6.2: A hardware user interface that replicates existing plant capabilities for an application may be chosen by a licensee as an alternative to the (FPDS). The review of the implementation of such a hardware user interface would be a plant specific action item.

Resolution: The applicant stated that AP1000 safety systems will use the FPDS as developed by the applicant. An alternative hardware interface will not be used.

PSAI 6.3: If a licensee installs a Common Qualified Platform application that encompasses the implementation of FPDS, the use of the FPDS must be treated in the plant specific failure modes and effects analysis (FMEAs).

Resolution: This item is included in item PSAI 6.10 .

PSAI 6.4: Each licensee implementing a Common Qualified Platform application must verify that its plant environmental data (i.e., temperature, humidity, seismic, and electromagnetic compatibility) for the locations in which the Common Qualified Platform equipment is to be installed are enveloped by the environment considered for the Common Qualified Platform qualification testing, and that the specific equipment configuration to be installed is similar to that of the Common Qualified Platform equipment used for the test.

Resolution: The PMS equipment temperature and humidity qualification is covered by DCD Tier 1 Section 2.5.2, Item 4; the seismic qualification is covered by DCD Tier 1, Section 2.5.2, Item 2; and the electromagnetic interference/radio frequency interference qualification is covered by DCD Tier 1, Section 2.5.2, Item 3. Through these ITAAC verification process, the COL applicant is responsible to verify that its plant-specific environmental conditions for all modes of operation for the locations in which the Common Qualified Platform equipment is to be installed are within the envelope of the topical report.

PSAI 6.5: The software program manual specifies plans that will provide a quality software life cycle process, and that these plans commit to documentation of life cycle activities that will permit the staff to review the implementation of the life cycle process for specific application on a plant specific basis.

Resolution: The software life cycle process is covered by DCD Tier 1, Section 2.5.2, Item 11. The evaluation of the Common Qualified Platform's life cycle process is documented in the NRC safety evaluation report "Acceptance for Referencing of Topical Report CENPD-396-P, Revision 1, "Common Qualified Platform," dated August 11, 2000.

PSAI 6.6: When implementing a Common Qualified Platform safety system, the licensee must review the applicant's timing analysis and validation tests for that Common Qualified Platform system in order to verify that it satisfies its plant specific requirements for accuracy and response time presented in the accident analysis in Chapter 15 of the Safety Analysis Report.

Resolution: The accuracy and response time of the AP1000 safety systems will be commensurate with the Chapter 15 safety analysis. The COL applicant is responsible for the setpoint analysis. The setpoint analysis shall be performed by the COL applicant as defined in DCD Tier 1, Section 2.5.2, Item 10 and DCD Tier 2 Section 7.1.6. This is COL Action Item 7.2.7-1 as discussed in Section 7.2.7 of this report.

PSAI 6.7: The operator's module and the maintenance and test panel provide the human machine interface for the Common Qualified Platform. Both will include display and diagnostic capabilities unavailable in the existing analog safety systems. The human factor considerations for specific applications of the Common Qualified Platform will be evaluated on a plant-specific basis.

Resolution: The human factors program is the responsibility of the COL applicant and is covered by DCD Tier 1 Section 3.2 and DCD Tier 2 Section 18.2.6, "Combined License Information." This is COL Action Item 18.2.4-1, as discussed in Chapter 18 of this report.

PSAI 6.8: If the licensee installs a Common Qualified Platform PAMS, core property calculator or DPPS, the licensee must verify on a plant-specific basis that the new system provides the same functionality as the system that is being replaced, and meets the functionality requirement applicable to those systems.

Resolution: The AP1000 is a new plant safety system installation; therefore, this action is not applicable.

PSAI 6.9: Modifications to plant procedures and/or TS due to the installation of a Common Qualified Platform safety system will be reviewed by the staff on a plant-specific basis. Each licensee installing a Common Qualified Platform safety system shall submit its plant specific request for license amendment with attendant justification.

Resolution: The AP1000 is a new plant safety system installation. The COL applicant will be responsible for plant procedures as discussed in DCD Tier 2 Section 13.5.1. This is COL Action Item 13.5.1-1, as discussed in Section 13.5.1 of this report.

PSAI 6.10: A licensee implementing any Common Qualified Platform applications must prepare its plant-specific model for the design to be implemented and perform the FMEA for that application.

Resolution: COL applicants referencing the AP1000 certified design shall perform FMEA for each AP1000 safety system. The FMEAs will confirm that no single failure of a safety system component will defeat more than one of the four protective channels, assuring proper protective action at the system level. This is discussed in DCD Tier 2 Section 7.2.3, "Combined License Information." This is COL Action Item 7.2.3-1.

PSAI 6.11: A licensee installing a Common Qualified Platform system shall demonstrate that the plant-specific Common Qualified Platform application complies with the criteria for defense against common-mode failure in digital instrumentation and control systems and meets the guidance of BTP HICB-19.

Resolution: The AP1000 design includes both the PMS and the DAS. Both the PMS and DAS provide manual and automatic protective functions. The design features of PMS

will be verified by ITAAC in DCD Tier 1 Section 2.5.2, and the design features of DAS will be verified by ITAAC in DCD Tier 1 Section 2.5.1. The completion of ITAAC processes on both the PMS and the DAS will verify the design features and the functional requirements in both systems.

PSAI 6.12: A licensee implementing a Common Qualified Platform digital plant protection system shall define a formal methodology for overall response time testing.

Resolution: A formal methodology will be defined for response time testing of AP1000 safety systems. This methodology is covered by DCD Tier 1 Section 2.5.2, Item 10. DCD Tier 2 Section 7.1.6, "Combined License Information," states that the COL applicant will provide a calculation of setpoints for protective functions consistent with the methodology presented in WCAP-14605, “Westinghouse Setpoint Methodology for Protection System - AP600," issued April 1996. This is COL Action Item 7.2.3-2.

PSAI 6.13: A licensee implementing the Common Qualified Platform system shall analyze the capacity of the shared resources to accommodate the load increase due to sharing.

Resolution: The shared resource issue relates to multiple Common Qualified Platform based systems using the same resources such as the AF100 bus or an Operator Module. An analysis will be performed to ensure that the capacity of shared resources for AP1000 safety systems is commensurate with anticipated loads. This issue will be addressed as part of the design process that is covered by DCD Tier 1 Section 2.5.2, Item 11.

PSAI 6.14: The licensee must ascertain that the implementation of the Common Qualified Platform does not render invalid any of the previously accomplished TMI action items.

Resolution: The safety-related instrumentation systems are designed and built to conform to the applicable criteria, codes, and standards concerned with the safe generation of nuclear power. This issue will be addressed as part of the design process that is covered by DCD Tier 1 Section 2.5.2.

7.2.4 Common Qualified Platform Generic Open Items Resolutions

On August 11, 2000, the NRC staff issued a safety evaluation report (SER) regarding Topical Report CENPD-396-P. Section 7 of that safety evaluation report identified 10 generic open items (GOIs). The GOI resolutions are documented in the staff's safety evaluation reports dated June 22, 2001 and April 2, 2003 for closeout of the Common Qualified Platform Open Items related to reports CENPD-396-P, Revision 1, and CE-CES-195, Revision 1, “Software Program Manual for Common Qualified Platform Systems,” issued May 2000.

7.2.5 PMS Design Process Review

SRP Chapter 7, BTP HICB-14, "Guidance on Software Review for Digital Computer-Based I&C Systems," provides guidance for reviewing the design of the safety-related digital I&C system. The staff's acceptance of software for safety system functions is based upon (1) confirmation that the software was developed in accordance with acceptable software development plans, (2) evidence that the plans were followed in an acceptable software life cycle, and (3) evidence that the process produced acceptable design outputs. BTP-14 requires certain information that needs to be reviewed with respect to digital I&C design process and implementation. In response to RAIs 420.001 and 420.023, the applicant submitted Topical Report WCAP-15927, "Design Process for AP1000 Common Qualified Platform Safety Systems," issued August 2002, to define the process for system level design, software design and implementation, and hardware design and implementation for the AP1000 protection system development. Additional details regarding the Common Qualified Platform software development plans are discussed in document CE-CES-195.

The AP1000 protection system development (life cycle phases) includes the following phases occur in the development of application hardware and software:

- Conceptual (Project Definition)
- System Definition
- Software Design
- Hardware Design
- Software Implementation
- Hardware Implementation
- System Integration
- Installation

The flow of activities is similar to that of a classic "waterfall" development process. It is intended that these activities may be both iterative and overlapping. Work may commence on a given development phase before preceding phases are complete. Testing activities are also defined as part of the design verification and validation (V&V) process. The testing activities complement the hardware implementation, software implementation, system integration, and installation phases.

AP1000 PMS can use the Common Qualified Platform to perform safety-related protective functions as discussed in Sections 7.2.1 and 7.3.1 of this report. The Common Qualified Platform is designed based on industry standards, regulatory requirements and engineering experience in and knowledge of the types of functions that are required for typical safety system applications. The Common Qualified Platform consists primarily of the ABB AC160 hardware and software product line, including the Advant development tools. The AC160 product line is not developed by the applicant. It is developed commercially. It was selected and qualified by the applicant for use in Common Qualified Platform applications by a process of commercial dedication. The Common Qualified Platform also contain products that are not ABB Advant commercial components. These include software and hardware elements that are developed by the applicant specifically for the Common Qualified Platform.

The software program manual (SPM) describes the requirements for the software design and development process and for the use of software in Common Qualified Platform systems. The SPM consists of several basic elements:

- A software safety plan, which identifies the processes that will reasonably assure that safety-critical software does not have hazards that could jeopardize the health and safety of the public.
- A software quality assurance plan, which describes the process and practice of developing and using software. The software quality assurance plan addresses standards, conventions, reviews, problem reporting and other software quality issues.
- A verification and validation program, which describes the method of assuring correctness of the software.
- A software configuration management plan, which describes the method of maintaining the software in an identifiable state at all times.
- A software operations and maintenance plan, which describes software practices after delivery to a customer.

The SPM also discusses software management, documentation and other matters related to software design and use.

The SPM has been reviewed by the staff in conjunction with the review of Topical Report CENPD-396-P. In the SER on CENPD-396-P, “Acceptance for Referencing of Topical Report CENPD-396-P, Revision 1, "Common Qualified Platform,” issued August 11, 2000, the staff concluded that the SPM specifies plans that will provide a quality software life cycle process, and that these plans commit to documentation of life cycle activities that will permit the staff or others to evaluate the quality of the design features upon which the safety determination will be based. The staff will review the implementation of the life cycle process and the software life cycle process design outputs for specific applications on a plant-specific basis.

In DCD Tier 1 Section 2.5.2, Item 11 specifies that the PMS hardware and software is developed using a planned design process which provides for specific design documentation and reviews during the following life cycle stages:

- Design requirement phase, may be referred to as conceptual or project definition phase
- System definition phase
- Hardware and software development phase, consisting of hardware and software design and implementation
- System integration and test phase
- Installation phase

An Inspection will be performed on the process’ used to design the hardware and software. The process shall define the organizational responsibilities, activities, and configuration management controls for the following:

- Establishment of plans and methodologies.
- Specification of functional requirements.

- Documentation and review of hardware and software.
- Performance of system tests and the documentation of system test results.
- Performance of installation tests and inspections.

In accordance with the Quality Assurance Program, administrative control procedures are used to establish software quality assurance and configuration management for process computer software, firmware, and associated software development, computer systems, and associated documentation. They ensure that the integrity of a process software product is known and preserved throughout its life cycle (from development to retirement). These controls also apply to the development tools and systems used to develop and test process software.

In DCD Tier 2 Section 7.1.7, both CE-CES-195 and WCAP-15927 are designated as Tier 2* documents. Any change to these two documents will require NRC approval. The Software Program Manual (CE-CES-195) describes the software design and development process. This document covers Software Safety Plan, Software Quality Assurance Plan, Software V&V Plan, Software Configuration Management Plan, Software Operation and Maintenance Plan. This is a generic software related document. The guidance in WCAP-15927 should be followed when using the Common Qualified Platform during implementation of the AP1000 plant specific design application.

7.2.6 Protection Systems Test Intervals and Allowed Outage Time

DCD Tier 2 Chapter 16 Sections TS 3.3.1 and TS 3.3.2 refer to Topical Report WCAP-10271-P-A, Supplement 2, Revision 1, “Evaluation of Surveillance Frequencies and Out of Service Times for the Reactor Protection Instrumentation System” as the basis for some of the TS completion times. However, Topical Report WCAP-10271 is based on the protection systems use of analog system hardware. Many aspects of the functional design are different for the AP1000 digital systems. In response to RAI 630.021, the applicant has not demonstrated the applicability of the generic analyses of WCAP-10271 for the AP1000 protection system. The COL applicant needs to provide detailed plant protection system FMEA and component reliability data to justify the TS completion time. In response to NRC staff’s additional comment, by letter, dated April 7 2003, the applicant agreed to add a COL action item to perform a plant specific FMEA for the protection system to determine the “Completion Time” in plant TS, Section TS 3.3.1 and TS 3.3.2.

The AP1000 TS for these values that rely on the FMEA for their basis will use brackets around the reference value in the “Completion Time” column. This is addressed in DCD Tier 2 Section 7.2.3, where it states that the "Combined License applicants referencing the AP1000 certified design will provide an FMEA for the protection and safety monitoring system." This is COL Action Item 7.2.6-1.

7.2.7 Protection Systems Setpoint Methodology

In DCD Tier 2 Appendix 1A, “Compliance with Regulatory Criteria,” the applicant stated that the AP1000 design conforms to RG 1.105, “Instrument Setpoint for Safety-Related Systems.” However, no setpoint methodology documentation was provided. In its response to RAI 420.11

dated October 1, 2002, the applicant stated that WCAP-14605 describes the methodology that will be used by the COL applicant to perform the setpoint study. The methodology can be used for performing setpoint studies independent of the hardware used for the protection system. For example, the value used for rack calibration accuracy may change as the result of a platform change; however, the methodology used to account for rack calibration accuracy will not change. Thus, the methodology, but not the setpoint study itself, is independent of PMS platform. The general requirement for setpoints is that they be established high enough to preclude inadvertent actuation, but low enough to ensure that a proper margin is maintained in the setpoint determination. The staff finds that the Westinghouse setpoint methodology is in conformance with the guidance provided in Branch Technical Position BTP-12, "Guidance on Establishing and Maintaining Instrument Setpoints," and therefore is acceptable.

In DCD Tier 2 Chapter 16, Table 3.3.1-1, “Reactor Trip System Instrumentation” and Table 3.3.2-1, “Engineered Safeguards Actuation System Instrumentation,” the values specified in brackets in the Trip Setpoint column are the DCD Tier 2 Chapter 15 safety analysis values and for information only. The actual setpoints will not be established at this time. The COL applicant should provide the plant specific trip setpoints, based on the specific I&C system design and equipment installed and update tables 3.3.1-1 and 3.3.2-1, accordingly. This is addressed generically in DCD Tier 2 Section 7.1.6, where it states that the "Combined License applicants referencing the AP1000 certified design will provide a calculation of setpoints for protective functions consistent with the methodology presented in WCAP-14605." This is COL Action Item 7.2.7-1.

7.2.8 PMS Evaluation Findings and Conclusions

For the PMS design, the applicant has committed to conformance with applicable standards and regulatory guides referenced in the DCD. Based on the review of the information with respect to the relevant regulatory guides and standards in the SRP Chapter 7, the staff finds that the requirements of 10 CFR 50.55a(a)(1) and GDC 1 have been met.

The requirements of 10 CFR 50.55a(h) specify that protection systems meet the requirements of IEEE Standard 603-1991. The applicant submitted Topical Report WCAP-15776, “Safety Criteria for the AP1000 Instrumentation and Control Systems,” issued April 2002, which describes the design-bases for the safety system and discusses the conformance to the general functional requirements of IEEE Standard 603-1991. The staff has reviewed the WCAP-15776 and verified the design description in DCD Tier 2 Chapter 7 and other AP1000 docketed information. The following are the staff’s findings with respect to the conformance to the IEEE 603-1991 requirements:

IEEE 603 Sections 4.1 and 4.2 require, in part, the identification of the design basis events applicable to each mode of operation. The AP1000 safety systems are designed to protect the health and safety of the public by limiting the release of radioactive material during Conditions II, III, and IV events. The release of radioactive material is designed to be within acceptable limits, as defined in DCD Tier 2 Chapter 15, “Accident Analyses.” The PMS automatically initiates appropriate protective action when a condition monitored by the system reaches a preset level. The safety analyses demonstrate that even under conservative critical conditions

for design basis-accidents, the safety system provides confidence that the plant is put into and maintained in a safe state following a Condition II, III, or IV accident. Based on the discussion above, the staff finds that the AP1000 design meets the requirements of IEEE 603 Sections 4.1 and 4.2.

IEEE 603 Section 4.3 requires permissive conditions. The AP1000 PMS is designed so that protective functions are initiated and accomplished during various reactor operating modes. The following specific design bases apply:

- Where operating requirements necessitate automatic or manual block of a protective function, the block is automatically removed whenever the appropriate permissive conditions are not met. Hardware and software used to achieve automatic removal of the block of a protective function are part of the PMS and, as such, are designed in accordance with the same criteria as the protective function.

- Block of a protective function is automatically cleared when the protective function is required to function.

Therefore, the staff finds that the AP1000 design satisfies the IEEE 603 Section 4.3 requirement.

IEEE 603 Section 4.4 requires defining protective system variables and their range and rate of changes. DCD Tier 2 Sections 7.2 and 7.3 describe the variables required to be monitored for protective action and their ranges and rates of change. Based on the discussion above, the staff finds that the AP1000 design meets the IEEE 603 Section 4.4 requirement.

IEEE 603 Section 4.5 requires means of manual actions. In the AP1000 design, means are provided in the main control room for manual initiation of protective functions at the system level. The manual controls are a backup to the automatic protection provided by the PMS. Manual actuation relies on minimum equipment and once initiated, proceeds to completion unless the operator deliberately intervenes. Failure in the automatic initiation portion of a system-level function does not prevent the manual initiation of the function. The AP1000 human system interface design includes a minimum inventory of dedicated or fixed position displays and controls. The fixed-position displays and alarms are quickly and easily retrievable. Based on the discussion above, the staff finds that the AP1000 design meets the IEEE 603 Section 4.5 requirement.

IEEE 603 Section 4.6 requires the identification of the minimum number and location for those spatial dependence variables. In the AP1000 design, thermowell-mounted RTD installed in each reactor coolant loop provide the hot and cold leg temperature signals to the PMS. Three thermowells in each hot leg are mounted 49°C (120°F) apart in the cross-sectional plane of the piping, to obtain a representative temperature sample. This hot leg temperature measurement arrangement is because of the hot leg temperature streaming effect and because the measurement varies as a function of thermal power. The PMS averages these signals using electronic weighting average methods. The cold leg RTDs are located downstream of the reactor coolant pump (RCP). The pumps provide mixing of the coolant. No special arrangement is required. Radial neutron flux is not a spatially dependent concern because of

core radial symmetry. Excore detectors furnish axially-dependent information to the overtemperature and overpower calculators. Based on the discussion above, the staff finds that the AP1000 design meets the IEEE 603 Section 4.6 requirement.

IEEE 603 Section 4.7 requires, in part, that the range of transient and steady-state conditions be identified for the energy supply and the environment during normal, abnormal, and accident conditions under which the system must perform. The AP1000 equipment is environmentally qualified to meet the accident conditions through which it operates to mitigate the consequences of the accident. Equipment is seismically qualified to meet safe shutdown earthquake levels. The safety system is powered by Class 1E dc and a uninterruptible power supply system. Based on the discussion above, the staff finds that the AP1000 design meets the IEEE 603 Section 4.7 requirement.

IEEE 603 Section 4.8 requires, in part, the identification of conditions having potential for causing functional degradation of safety system performance and the proposed protective action. The DCD specifies that the AP1000 design has the ability to initiate and accomplish protective functions during and following natural phenomena such as earthquakes, tornadoes, hurricanes, floods, and winds. Plant safety is provided despite degraded conditions caused by internal events such as fire, flooding, explosions, missiles, electrical faults, and pipe whip. Based on the discussion above, the staff finds that the AP1000 design meets the IEEE 603 Section 4.8 requirement.

IEEE 603 Section 4.9 requires the identification of the methods used to determine that the reliability of the safety system design is appropriate for each such design. In addition, it requires the identification of the methods used to verify that any qualitative or quantitative reliability goals imposed on the system design have been met. The PMS meets its unavailability allocation, (i.e., the PMS together with DAS shall contribute less than 3.0 hours per year to the overall plant unavailability). The PMS is design to contribute less than 2.5 hours per year to the plant unavailability calculations. The primary design features provided by the PMS to meet this requirement are:

- The ability to withstand single failures, including loss of power sources.
- Provision made for the periodic in-situ testing of equipment.
- Modular design allowing on-line replacement.
- Extensive diagnostic facilities to identify the location of faulty modules and components.
- A verification and validation program demonstrates the adequacy of the hardware and software.

The reliability criterion is based on deterministic criteria of IEEE 603 and IEEE 7-4.3.2 as discussed under IEEE 603 Section 5 below.

Based on the discussion above, the staff finds that the AP1000 design meets the IEEE 603 Section 4.9 requirement.

IEEE 603 Section 4.10 requires identification of the critical points in time or plant conditions for which the protective actions shall be initiated. The PMS automatically initiates appropriate

protective actions when a condition monitored by the system reaches a preset level. The critical points in time are determined by the PMS response time modeled in the accident analyses. The PMS will be designed and tested to meet the response times assumed in the accident analyses. Based on the discussion above, the staff finds that the AP1000 design meets the IEEE 603 Section 4.10 requirement.

IEEE 603 Section 4.11 requires that equipment protective features are designed to place the safety system in a safe state. In the AP1000 design, each protection feature has different characteristics and therefore different techniques are used to achieve a fail-safe design. Examples of protective features for selected functions include:

- Reactor trip circuits are designed to fail in the tripped state.
- Engineered safety features actuated components are designed to fail into a state that has been demonstrated to be acceptable if conditions such as disconnection, loss of power source, or postulated adverse environments are experienced.
- Sensor circuits are designed so that a loss of power will produce a “safe” signal or will produce an off-scale value or a signal that can be identified by the protection system as “bad”. Digital protective equipment input circuits are designed to recognize off-scale or bad values and take appropriate action (alarm, actuate or use substitute value from redundant channel).
- Actuation signals from multiple protection system divisions are provided to improve the reliability of the protection system.

Based on the discussion above, the staff finds that the AP1000 design meets the IEEE 603 Section 4.11 requirement.

IEEE 603 Section 4.12 requires identification of any other special design basis that may be imposed on the system design. The AP1000 has a DAS which is a non-safety system that is diverse and separate from the safety-related PMS. The DAS provides functions necessary to reduce the risk associated with postulated common mode failures of critical protection systems. Based on the discussion above, the staff finds that the AP1000 design meets the IEEE 603 Section 4.12 requirement.

IEEE 603 Section 5, “Safety System Criteria,” requires that the safety systems shall, with precision and reliability, maintain plant parameters within acceptable limits established for each design-basis event. The power, instrumentation, and control portions of each safety system shall be comprised of more than one safety group of which any one safety group can accomplish the safety function. The AP1000 design in conformance with each of these criteria are addressed as follows:

IEEE 603 Section 5.1, "Single Failure Criterion," requires the AP1000 safety system to include sufficient redundancy to meet system performance requirements even if the system is degraded by a single failure. Redundancy begins with the sensors monitoring the variables and continues through the signal processing and actuation electronics. Redundant actuations are also provided. Two or more diverse functions initiate most protective actions. No single failure within the safety system causes a Condition II event to progress to a Condition III event, or a

Condition III event to progress to a Condition IV event. To prevent common mode failures, additional measures such as functional diversity, physical separation, and testing as well as administrative control during design, production, installation, and operation will be employed. Based on the discussion above, the staff finds that the AP1000 design meets the IEEE 603 Section 5.1 criterion.

IEEE 603 Section 5.2, "Completion of Protective Action Criterion"

In the AP1000 design, features are provided to ensure that system-level actions go to completion. The operator can stop the action of an engineered safety feature (on a component-by-component basis) by deliberate intervention. Component-level manual reset controls permit the operator to take this action only after the system-level signal is reset. The provision for component-level manual reset is to stop safeguard functions due to inadvertent actuation. Based on the discussion above, the staff finds that the AP1000 design satisfies the IEEE 603 Section 5.2 criterion.

IEEE 603 Section 5.3, "Quality Criterion"

The AP1000 quality assurance program conforms to GDC 1. The design V&V program demonstrates the adequacy of the hardware and software for the PMS. The software development process is consistent with the following standards:

- ANS/IEEE 7-4.3.2-1993, “IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations”
- IEEE 828-1990, “IEEE Standard for Software Configuration Management Plans”
- IEEE 829-1983, “IEEE Standard for Software Test Documentation”
- IEEE 830-1993, “Recommended Practice for Software Requirements Specifications”
- IEEE 1012-1986, “IEEE Standard for Software Verification and Validation Plans”
- IEEE 1028-1988, “IEEE Standard for Software Review and Audit”
- IEEE 1042-1987, “IEEE Guide to Software Configuration Management”

WCAP-13383 provides a planned design process for Eagle System hardware and software development during the following life cycle stages:

- Design requirement phase
- System definition phase
- Hardware and software development phase
- System test phase
- Installation phase

WCAP-15927 provides a planned design process for Common Qualified Platform system hardware and software development during the following life cycle stages:

- Conceptual phase
- System definition phase
- Software design phase

- Hardware design phase
- Software implementation phase
- Hardware implementation phase
- System integration phase
- Installation phase

Topical Reports WCAP-13383 and CENPD-396-P provide guidance on the design process, the V&V process, and the commercial dedication process.

The design process, V&V and commercial dedication process are stated to be in conformance with IEEE standard 7-4.3.2 and other IEEE standards related to software quality and guidance documents. Based on the review of these documents, the staff finds that the process meets the acceptance criteria and the PMS design satisfies the IEEE Std. 603 Section 5.3 criterion.

IEEE 603 Section 5.4, "Equipment Qualification Criterion" requires that the safety system equipment shall be qualified by type test, previous operating experience, or analysis, or any combination of these three methods, to substantiate that it will be capable of meeting, on a continuing basis, the performance requirements as specified in the design basis. The staff has reviewed the information in DCD Tier 2 Sections 3.11 and 3.10, the AP1000 electrical equipment within the safety system is environmentally and seismically qualified to meet the conditions through which it must operate to mitigate the consequences of the accident. Therefore, the staff finds that the PMS design satisfies the IEEE 603 Section 5.4 criterion.

IEEE 603 Section 5.5, "System Integrity Criterion" requires that the safety system shall be designed to accomplish their safety functions under the full range of applicable conditions enumerated in the design basis. The AP1000 DCD describes that the PMS is designed to maintain its capability to initiate its protective functions during and following natural phenomena that are credible to the plant, such as earthquakes, tornadoes, hurricanes, floods, and winds. Functional capability of the system is maintained during events such as fires, flooding, explosions, missiles, electrical faults, and pipe whip. The equipment is environmentally and seismically qualified. Based on the discussion above, the staff finds that the AP1000 design satisfies IEEE 603 Section 5.5 criterion.

IEEE 603 Section 5.6, "Independence Criterion" requires that redundant portions of a safety system provided for a safety function shall be independent of and physically separated from each other to the degree necessary to retain the capability to accomplish the safety function during and following any design basis event requiring that safety function. The AP1000 DCD states that physical separation of redundant safety divisions is carried throughout the system, extending from the sensors to the devices actuating the protective function. Separation of wiring is achieved using separate wire ways, cable trays, and containment penetrations for each division. Separate power feeds energize each redundant protection division. Cable separation and conformance to RG 1.75 will be further discussed in Chapter 8 of this report. Based on the discussion above, the staff finds that the AP1000 design satisfies IEEE 603 Section 5.6 criterion.

IEEE 603 Section 5.7, “Capability for Test and Calibration Criterion” requires that safety system equipment shall be provided with the capability for testing and calibration while retaining the capability to accomplish their safety functions. The AP1000 DCD states that testing from sensor inputs of the PMS through to the actuated equipment is accomplished through a series of overlapping sequential tests, with the majority of the tests capable of being performed with the plant at full power. Where testing final equipment at power would upset plant operation or damage equipment, provisions are made to test the equipment at reduced power or when the reactor is shutdown. Each division of the PMS includes a test subsystem. The test subsystem does not test the engineered safety feature (ESF) actuators. This portion of the test may be accomplished by using component-level actuation signals. For those final devices that can be operated at power without upsetting the plant or damaging the equipment, the test is performed by actuating the manual actuation control that causes the device to operate. Position switches on the device itself send a signal back to the ESF actuation subsystem, where it is transmitted to the main control room (MCR) for display. The display verifies that the manual command is successfully completed. When the channel is bypassed for testing, the bypass is manually instated and removed by the test subsystem. Based on the discussion above, the staff finds that the AP1000 design satisfies the IEEE 603 Section 5.7 criterion.

IEEE 603 Section 5.8, “Information Display Criterion” requires that the display instrumentation for manual actions to accomplish the safety function shall be part of the safety system. The display instrumentation shall provide accurate, complete, and timely information. If the protective actions of some part of a safety system have been bypassed for any purpose, continued indication of this fact for each affected safety group shall be provided in the control room. The AP1000 DCD states that no manual controlled actions are assumed in the DCD Tier 2 Chapter 15 analyses, therefore, no Type A Variables (a variable that provides information needed by the operator to perform manual action associated with design-basis accident events) are defined for the post accident monitoring instrument. The PMS status information provided to the operator includes parameter values, logic status, equipment status, and actuation device status. An alarm alerts the operator of deviations from normal operating conditions. The PMS provides the operator, (via the data display and processing system) with continuous indication of bypassed status. The majority of the operations employ soft controls, soft control displays, and plant information displays. These displays appear on display devices such as cathode tubes, flat panel screen, or visual display units. The AP1000 human system interface design includes a minimum inventory of dedicated or fixed-position display and controls. The minimum inventory display and controls will perform critical safety functions. Based on the review of information in DCD Tier 2 Chapters 7 and 18, the staff finds that the AP1000 design satisfies the IEEE 603 Section 5.8 criterion.

IEEE 603 Section 5.9, “Control of Access Criterion” requires that the design shall permit the administrative control of access to safety system equipment. These administrative controls shall be supported by provisions within the safety systems, by provision in the generating station design, or by a combination thereof. The AP1000 DCD states that the PMS provides for administrative control over access to the means for manually bypassing protection channels and for manually blocking protective functions. Administrative control of access is provided to setpoint adjustments, channel calibration adjustments and test points. Cabinet doors are

normally locked. Based on the discussion above, the staff finds that the AP1000 design satisfies IEEE 603 Section 5.9 criterion.

IEEE 603 Section 5.10, "Safety System Repair Criterion" requires that the safety systems shall be designed to facilitate timely recognition, location, replacement, repair, and adjustment of malfunctioning equipment. The AP1000 DCD states that the PMS facilitates the recognition, location, replacement, repair, and adjustment of malfunctioning components or modules. The built-in diagnostics provide a mechanism for periodically verifying the operability of modules in the PMS, and of rapidly locating malfunctioning assemblies. Continuous on-line error checking also detects and locates failures. Channel bypass permits replacement of malfunctioning sensors or channel components, (without jeopardizing plant availability), while still meeting the single-failure criterion. Based on the discussion above, the staff finds that the AP1000 design satisfies IEEE 603 Section 5.10 criterion.

IEEE 603 Section 5.11, "Identification Criterion" requires that (1) safety system equipment shall be distinctly identified in accordance with the requirements of IEEE 384, (2) components or modules mounted in equipment or assemblies that are as being a single redundant portion of a safety system, (3) identification of safety system equipment shall be distinguishable from other purposes, (4) identification of safety system equipment shall not require frequent use of reference material, and (5) the associated documentation shall be distinctly identified. The AP1000 DCD states that redundant divisions of the safety system have distinctive markings. The color-coded nameplates provide identification of equipment associated with protective functions and their division associations. Non-cabinet mounted protective equipment and components have an identification tag or nameplate. Small electrical components, such as relays, have nameplates on the enclosure that houses them. The staff finds that the design satisfied IEEE 603 Section 5.11 criterion.

IEEE 603 Section 5.12, "Auxiliary Features Criterion" states that (1) auxiliary supporting features shall meet all requirements of this standard; (2) other auxiliary features that (a) perform a function that is not required for the safety systems to accomplish their safety functions, and (b) are part of the safety system by association, shall be designed to meet those criteria necessary to ensure that these components, equipment, and systems do not degrade the safety systems below an acceptable level. The AP1000 DCD states that the AP1000 Electrical Power System provides reliable power for the safety equipment required for the plant I&C system and other vital functions needed for shutdown of the plant. For the station blackout situation, the dc batteries constitute the source of electrical power for operation of the required dc and ac instrument uninterruptible power supply. When ac power is available, the non-safety-related nuclear island nonradioactive ventilation system (VBS) provides HVAC service to the instrument room and MCR. IF the VBS is not available, the main control room emergency habitablilty system provides emergency passive heat sinks for the instrument room, MCR, and dc equipment room. The heat sink for each room limits the temperature rise inside each room during the 72 hour period. If power is lost for more than 72 hours, the temperature of the instrument room and the MCR will be maintained by operating two ancillary fans to supply outside air to two areas. Based on the discussion above, the staff finds that the AP1000 design satisfies IEEE 603 Section 5.12 criterion.

IEEE 603 Section 5.13, "Multi-Unit Stations Criterion" requires that the sharing of structures, systems, and components between units at multi-unit generating stations is permissible provided that the ability to simultaneously perform required safety functions in all units is not impaired. The AP1000 DCD states that the AP1000 is a single-unit plant. If more than one unit were built on the same site, the units would not share any of the safety systems. Based on the discussion above, the staff finds that the AP1000 design satisfies IEEE 603 Section 5.13 criteria.

IEEE 603 Section 5.14, "Human Factor Considerations Criterion" states that human factors shall be considered at the initial stages and throughout the design process to assure that the functions allocated in whole or in part to the human operator(s) and maintainer(s) can be successfully accomplished to meet the safety system design goals. The AP1000 human factors engineering design process has been developed to conform to NUREG 0711, "Human Factors Engineering Program Review Model." The 10 elements of the design process provided a structure top-down system analysis using accepted human factors engineering principles. The human factor design process review is further discussed in Chapter 18 of this report.

IEEE 603 5.15, "Reliability Criterion" requires that for those systems for which either quantitative or qualitative reliability goals have been established, appropriate analysis of the design shall be performed in order to confirm that such goal have been achieved. The AP1000 I&C safety systems PRA is discussed in Chapter 26 of the AP1000 PRA report. The PRA aspect of the PMS is addressed in Chapter 19 of this report.

Based on its review of the DCD commitments and other docketed references, the staff reached the following conclusions:

- The staff evaluated the PMS design description in the DCD and compared it to the SRP, applicable RGs, and industry codes and standards (including the information required by the IEEE 603-1991, Section 4, "Design Bases for Safety Systems," Section 5, "Safety System Criteria.)" Based on its review, the staff concludes that the design meets appropriate SRP criteria. The staff also concludes that the PMS meets the design-basis requirements of IEEE 603.

- The PMS includes systems and components that the applicant has committed to design to survive the effects of earthquakes, other natural phenomena, abnormal environments, and missiles as discussed in DCD Tier 2 Chapter 3. Therefore, the staff concludes that the applicant's commitments meet the requirements of GDC 2 and 4 for the PMS.

- The staff concludes that the design for the PMS described in DCD Tier 2 Chapters 6, 7, and 15 and DCD Tier 1 Section 2.5.2 provides instrumentation to monitor variables and systems over their anticipated ranges for normal operation, for anticipated operational occurrences, and for accident conditions as appropriate to assure adequate safety, including those variables and systems that can affect the fission process, the integrity of the reactor core, the reactor coolant boundary, and the containment and its associated systems. As described above, the staff concludes that appropriate controls are provided

to maintain the variables and systems within prescribed ranges. Therefore, the staff finds that the RTS design satisfies the requirements of GDC 13, and GDC 19.

- The staff concludes that design of the PMS has the capability (1) to initiate automatically the operation of the reactivity control systems to assure that specified acceptable fuel design limits are not exceeded as a result of anticipated operational occurrences, and (2) to sense accident conditions and to initiate the operation of systems and components important to safety. Therefore, the requirements of GDC 20 are satisfied.

- The staff concludes that periodic testing of the PMS, as described in the DCD, conforms with the criteria of RG 1.22 and RG 1.118. The staff further concludes that the applicant commitments to IEEE 603, with regard to system reliability and testability, are consistent with the requirements of GDC 21, and are acceptable.

- The staff concludes that the design of the PMS meets the criteria of RG 1.75 for protection system independence. The design techniques, such as functional diversity and diversity in components, are designed to the extent practical to prevent loss of protection function. Therefore, the staff concludes that the PMS meets the requirements of GDC 22.

- Based on the staff's review of the results of the failure modes analysis for the PMS, in conjunction with the results of the studies of the PMS design for defense against common-mode failures as discussed in Section 7.1.6 of this report, the staff concludes that the PMS design meets the requirements of GDC 23.

- The staff finds that the PMS is designed to meet the requirements of IEEE 603 regarding protection and control system interaction. Therefore, the staff concludes that the PMS design meets the requirements of GDC 24."

- The staff concludes that the PMS satisfies the protection system requirements for malfunction of the reactivity control system, such as accidental withdrawal of control rods. DCD Tier 2 Chapter 15 addresses the capability of the system to ensure that fuel design limits are not exceeded for such events. Therefore, the staff finds that the PMS satisfies the requirements of GDC 25.

- Based on its review of the PMS design for compliance with all of the above GDCs, the staff concludes that the PMS provides protection against anticipated operational occurrences. Therefore, the staff finds the PMS satisfies the requirements of GDC 29.

- On the basis of the applicant's commitment to meet the requirements of 10 CFR 50.55a(h)(3) with regard to IEEE 603-1991, and the staff's conclusion noted above, the staff concludes that the requirements of 10 CFR 50.55a(h) are satisfied.

7.3 Engineered Safety Features Actuation Systems

7.3.1 System Description

This section describes the instrumentation and controls for equipment to initiate various engineered safety features. Because the ESFAS is part of the PMS, the evaluation of the design and qualification of the PMS, as discussed in Section 7.2 of this report, also applies to the ESFAS.

Four sensors normally monitor each variable used for an engineered safety feature actuation. Analog measurements are converted to digital form by analog-to-digital converters within each of the four divisions of the PMS. Following required signal conditioning or processing, the measurements are compared against the setpoints for the engineered safety feature to be activated. When the measurement exceeds the setpoint, the output of the comparison results in a channel partial trip condition. The partial trip information is transmitted to the ESF coincidence logic to form the signals that result in an engineered safety feature actuation. The voting logic is performed twice within each division. Each voting logic element generates an actuation signal if the required coincidence of partial trips exists at its inputs. The signals are combined within each division of ESFAS coincidence logic to generate a system-level signal.

The system-level signals are then broken down to the individual signals to actuate each component associated with a system-level engineered safety feature. The interposing logic accomplishes this function and also performs necessary interlocking so that components are properly aligned for safety. Component-level manual actions are also processed by this interposing logic. The power interface transforms the low level signals to voltages and current commensurate with the actuation devices they operate. The actuation devices, in turn, control motive power to the final engineered safety feature component.

The safeguard actuation function is necessary to mitigate the effects of high energy line breaks both inside and outside of containment. A safeguards actuation (S) signal actuates the alignment of the core makeup tank (CMT) valves for passive injection to the reactor coolant system. The S signal provides two primary functions:

- Primary side water addition to ensure maintenance or recovery of reactor vessel (RV) water level; and
- Boration to ensure recovery and maintenance of shutdown margin (k_{eff} <1.0)

The S signal also initiates the reactor trip, turbine trip, reactor coolant pumps trip, containment isolation, main feedwater control valves closure, main feedwater pumps trip, and closure of isolation and crossover valves.

The S signal is generated from any of the following initiating conditions:

- low pressurizer pressure
- low lead-lag compensated steamline pressure
- low reactor coolant inlet temperature
- high-2 containment pressure
- manual initiation

The following subsections describe the signals and initiation logic for each engineered safety feature.

7.3.1.1 Containment Isolation

Containment isolation provides isolation of the containment atmosphere and selected process systems which penetrate containment from the environment. This function is necessary to prevent or limit the release of radioactivity to the environment in the event of a large-break loss-of-coolant accident (LOCA).

A signal to actuate containment isolation is generated from any of the following conditions:

- Automatic or manual safeguards actuation signal
- Manual initiation
- Manual actuation of passive containment cooling

Manual reset is provided to block the automatic actuation signal for containment isolation. Separate momentary controls are provided for resetting each division. No other interlocks or permissive signals apply directly to the containment isolation function.

7.3.1.2 In-Containment Refueling Water Storage Tank (IRWST) Injection

The passive core cooling system (PXS) provides core cooling by gravity injection and recirculation for decay heat removal following an accident. The IRWST has two injection flow paths. Each injection path includes a normally open motor operated isolation valve and two parallel lines, each isolated by one check valve and one squib valve in series.

IRWST injection on Low-2 hot leg level is automatically blocked when the pressurizer water is above the P-12 setpoint. This reduces the probability of a spurious injection. This block is removed when the core makeup tank actuation on low pressurizer level function is manually blocked to allow mid-loop operation.

Signals to align the IRWST for injection are generated from the following conditions:

- Actuation of the fourth stage of the automatic depressurization system
- Coincidence loop 1 and loop 2 hot leg levels below Low-2 setpoint for a duration exceeding an adjustable time delay
- Manual initiation

7.3.1.3 Core Makeup Tank Injection

The CMT injection provides the passive injection of borated water into the RCS. Injection provides RCS makeup water and boration during transients or accidents when the normal makeup supply from the chemical and volume control system (CVS) is lost or insufficient. Two tanks are provided. CMT injection mitigates the effects of high energy line breaks by adding primary side water to ensure maintenance or recovery of RV water level following a LOCA, and

by borating to ensure recovery or maintenance of shutdown margin following a steam line break.

Signals to align the CMTs for injection are generated from the following conditions:

- Automatic or manual safeguards actuation
- Automatic or manual actuation of the first stage of the automatic depressurization system
- Low-2 presurrizer level
- Low wide range SG level coincident with High hot leg temperature
- Manual initiation
- Pressurezer water level increasing above the P-12 interlock

7.3.1.4 Automatic Depressurization System Actuation

The automatic depressurization system (ADS) provides a sequenced depressurization of the reactor coolant system to allow passive injection from the CMTs, accumulators, and the IRWST to mitigate the effects of a LOCA. The depressurization is accomplished in four stages, with the first three stages discharging into the IRWST and the last stage discharging into containment. Each of the first three stages consists of two parallel paths with each path containing an isolation valve and a depressurization valve.

A signal to actuate the first stage of the ADS is generated from any of the following conditions:

- Core makeup tank injection alignment signal coincident with core makeup tank level less than the Low-1 setpoint in either core makeup tank in two of the four divisions
- Extended loss of ac power sources
- Manual initiation

The first stage depressurization valves are opened following a preset time delay after the actuation of the isolation valves. The second stage isolation valves are opened following a preset time delay after the second stage isolation valves are actuated, similar to the stage one. The third stage valves are opened following a preset time delay after the third stage isolation valves are actuated.

The fourth stage of the ADS consists of four parallel paths. Each of these paths consists of a normally open isolation valve and a depressurization valve. The four paths are divided into two groups with two paths in each group. The fourth stage valves can be opened under three conditions:

- Manual initiation coincident with RCS Wide Range Pressure - Low, or ADS Stages 1, 2, and 3 Actuation
- CMT Level - Low coincident with RCS Wide Range Pressure - Low
- Coincident RCS Loop 1 and 2 Hot Leg Level - Low

7.3.1.5 Reactor Coolant Pump Trip

The RCP trip allows the passive injection of borated water into the RCS. Injection provides RCS makeup water and boration during transients or accidents when the normal makeup supply from the CVS is lost or insufficient. Two tanks provide passive injection of borated water by gravity when the reactor coolant pumps are tripped. CMT injection mitigates the effects of high energy line breaks by adding primary side water to ensure maintenance or recovery of RV water level following a LOCA, and by borating to ensure recovery or maintenance of shutdown margin following a steam line break. RCP trip on high bearing water temperature protects the RCS coast down.

A signal to trip reactor coolant pumps is generated from any one of the following conditions:

- Automatic or manual safeguards actuation signal
- Automatic or manual actuation of the first stage of the ADS
- Low-2 pressurizer level
- Low wide range SG level coincident with High hot leg temperature
- Manual initiation of core makeup tank injection
- High reactor coolant pump bearing water temperature

7.3.1.6 Main Feedwater Isolation

The primary function of main feedwater isolation is to prevent damage to the turbine due to water in the steam lines and to stop excessive flow of feedwater into the SGs.

Signals to isolate the main feedwater supply to the SGs are generated from any of the following conditions:

- Automatic or manual safeguards actuation
- Manual initiation
- High-2 SG narrow range water level
- Low-1 reactor coolant system average temperature coincident with P-4 permissive
- Low-2 reactor coolant system average temperature coincident with P-4 permissive

7.3.1.7 Passive Residual Heat Removal Heat Exchanger Alignment

The passive residual heat removal (PRHR) system heat exchanger provides emergency core decay heat removal when the startup feedwater system is not available to provide a heat sink.

A signal to align the PRHR heat exchanger to passively remove core heat is generated from any of the following conditions:

- Core makeup tank injection alignment signal
- First stage automatic depressurization system actuation
- Low wide range SG level
- Low narrow range SG level coincidence with Low startup feedwater flow
- High-3 pressurizer water level
- Manual initiation

7.3.1.8 Turbine Trip

The primary function of the turbine trip is to prevent damage to the turbine due to water in the steam lines. This function is necessary in MODES 1 and 2, and in MODE 3 above P-11 to mitigate the effects of a large steam line break (SLB) or a large feedline break. Failure to trip the turbine following a SLB or large feedline break can lead to additional mass and energy being delivered to the SGs, resulting in excessive cooldown and additional mass and energy release in containment.

A signal to initiate turbine trip is generated from any of the following conditions:

- Reactor trip
- High-2 SG narrow range water level
- Manual feedwater isolation

7.3.1.9 In-Containment Refueling Water Storage Tank Containment Recirculation

The PXS provides core cooling by gravity injection and recirculation for decay heat removal following an accident. The PXS has two containment recirculation flow paths. Each path contains two parallel flow paths, one path is isolated by a motor operated valve in series with a squib valve and one path is isolated by a check valve in series with a squib valve.

Signals to align the in-containment refueling water storage tank containment recirculation isolation valves are generated from the following conditions:

- Low-3 in-containment refueling water storage tank water level in coincidence with fourth stage automatic depressurization system actuation
- Manual initiation
- Extended loss of ac power sources

7.3.1.10 Steam Line Isolation

Isolation of the main steamlines provides protection in the event of a SLB inside or outside containment. For a SLB upstream of the isolation valves, closure of the isolation valves limits the accident to the blowdown from only the affected SG. For a SLB downstream of the isolation valves, closure of the isolation valves terminates the accident as soon as the steam line depressurizes.

A signal to isolate the steam line is generated from any of the following conditions:

- Manual initiation
- High-2 containment pressure
- Low lead-lag compensated steam line pressure
- High steam line pressure negative rate
- Low reactor coolant inlet temperature

7.3.1.11 Steam Generator Blowdown System Isolation

SG blowdown isolation is provided to preserve the SG water inventory in anticipation of the use of the PRHR system. SG blowdown isolation is initiated from one of the following signals:

- Passive residual heat removal heat exchanger alignment signal
- Low narrow range SG level

7.3.1.12 Passive Containment Cooling Actuation

The passive containment cooling system has no containment heat removal function during normal plant operations. It is continuously maintained for readiness to respond in an emergency. The passive containment cooling system is actuated by:

- Manual initiation
- High-2 containment pressure

The actuation signal opens the passive containment cooling system valves that allow gravity flow from the passive containment cooling water storage tank to the top of the containment shell. The evaporation of the water on the containment shell provides the passive cooling.

7.3.1.13 Startup Feedwater Isolation

Isolation of the startup feedwater system is provided to prevent reactor overcooling effects or SG overfill that may damage the main turbine. The startup feedwater system isolation is initiated from one of the following two signals:

- Low reactor coolant inlet temperature
- High-2 SG narrow range water level
- Manual actuation of main feedwater isolation

The low reactor coolant inlet temperature signal is interlocked with the P-11 permissive logic. The isolation signal closes the startup feedwater control and isolation valves, and trips the startup feedwater pump.

7.3.1.14 Signal to Block Boron Dilution

This function is provided to protect against malfunctions of the CVS, which could cause unacceptable boron dilution during shutdown. On a coincidence of two of the four divisions, boron dilution is blocked. The flux doubling signal may be blocked manually above the P-6 power level, and is automatically reinstated below the P-6 permissive logic.

Signals to block boron dilution are generated from any of the following conditions:

- Excessive increasing rate of source range nuclear power
- Loss of ac power source
- Reactor trip

7.3.1.15 Chemical and Volume Control System Isolation

The safety functions provided by the CVS are limited to (1) containment isolation of the CVS lines penetrating containment; (2) termination of inadvertent RCS boron dilution; (3) isolation of makeup on a SG or pressurizer high level signal; and (4) preservation of the RCS pressure boundary, including isolation of normal chemical and volume control system letdown from the RCS.

The signal to actuate the isolation of the CVS is generated from:

- High-2 pressurizer level
- High-2 SG narrow range water level
- Automatic or manual safeguards actuation signal coincident with High-1 pressurizer level
- High-2 containment radioactivity
- Manual initiation

7.3.1.16 Signal to Block Steam Dump

Signals to block steam dump (turbine bypass) are generated from either of the following conditions:

- Low-2 reactor coolant system average temperature coincident with P-4 permissive
- Manual initiation

7.3.1.17 Control Room Isolation and Air Supply Initiation

Isolation of the MCR and initiation of the air supply provides a protected environment from which operators can control the plant following an uncontrolled release of radioactivity. Signals to initiate isolation of the MCR, to initiate the air supply, and to open the control room pressure relief isolation valves are generated from one of the following conditions:

- High-2 control room air supply radioactivity level
- Loss of ac power sources
- Manual initiation

7.3.1.18 Auxiliary Spray and Letdown Purification Line Isolation

The CVS maintains the RCS fluid purity and activity level within acceptable limits. The CVS purification line receives flow from the discharge of the RCPs. The CVS also provides auxiliary spray to the pressurizer. To preserve the reactor coolant pressure in the event of a break in the

CVS loop piping, the purification line and the auxiliary spray line is isolated on a pressurizer water level Low 1 setpoint in any two of the four divisions. This helps maintain reactor coolant system inventory.

7.3.1.19 Containment Air Filtration System Isolation

Some design-basis accidents, such as a LOCA, may release radioactivity into the containment where the potential would exist for the radioactivity to be released to the atmosphere and exceed the acceptable site dose limit. Isolation of the containment air filtration system provides protection to prevent radioactivity inside containment from being released to the atmosphere.

A signal to isolate the containment air filtration system is generated from any of the following conditions:

- Automatic or manual safeguards actuation signal
- Manual actuation of containment isolation
- Manual actuation of passive containment cooling
- High-1 containment radioactivity

7.3.1.20 Normal Residual Heat Removal System Isolation

The normal residual heat removal system (RNS) suction line is isolated by closing the containment isolation valves on High-2 containment radioactivity to provide containment isolation following an accident. This line is isolated on a safeguards actuation signal. However, the valves may be reset to permit the RNS pumps to perform their defense-in-depth functions postaccident. Should a high containment radiation signal (above High-2 setpoint) develop following the containment isolation signal, the RNS valves would reclose.

Signals for isolating the RNS lines are generated from any of the following conditions:

- Automatic or manual safeguards actuation signal
- High-2 containment radioactivity
- Manual initiation

7.3.1.21 Refueling Cavity Isolation

The containment isolation valves in the lines between the refueling cavity and the spent fuel pool cooling system are isolated on a Low spent fuel pool level in two-out-of-three divisions. This helps to maintain the water inventory in the refueling cavity due to line leakage.

7.3.1.22 Chemical and Volume Control System Letdown Isolation

A signal to isolate the letdown valves of the CVS is generated upon the occurrence of a Low-1 hot leg level in either of the two hot leg loops. This helps to maintain reactor system inventory. These letdown valves are also closed by the containment isolation function.

7.3.1.23 Pressurizer Heater Block

Pressurizer heaters are automatically tripped upon receipt of a core makeup tank operation signal or a Pressurizer Water Level - High-3 signal. This pressurizer heater trip reduces the potential for SG overfill and automatic ADS Stages 1, 2, and 3 actuation for a SG tube rupture event. Automatically tripping the pressurizer heaters reduces the pressurizer level swell for certain non-LOCA events (such as loss of normal feedwater, inadvertent CMT operation, and CVS malfunction resulting in an increase in RCS inventory). For small break LOCA analysis, tripping the pressurizer heaters supports depressurization of the RCS following actuation of the CMTs.

Signals for blocking the operation of the pressurizer heaters are generated from any of the following conditions:

- Core makeup tank injection alignment signal
- High-3 pressurizer water level

7.3.1.24 Steam Generator Relief Isolation

The function of the SG power operated relief valve (PORV) and block valve isolation is to ensure that the SG PORV flow paths can be isolated during a SG tube rupture (SGTR) event. The PORV flow paths must be isolated following a SGTR to minimize radiological release from the ruptured SG into the atmosphere. The PORV flow path is assumed to open due to high secondary side pressure, during the SGTR. Dose analyses take credit for subsequent isolation of the PORV flow path by the PORV and/or the block valve which receive a close signal on low steam line pressure.

A signal for closing the SG PORV and their block valves is generated from any of the following conditions:

- Manual initiation
- Low lead-lag compensated steam line pressure

7.3.2 Blocks, Permissives, and Interlocks for Engineered Safety Features Actuation

To allow some flexibility in unit operations, several interlocks are included as part of the ESFAS. These interlocks permit the operator to block some signals, automatically enable other signals, prevent some actions from occurring, and cause other actions to occur. The interlock functions backup manual actions to ensure plant operation under the conditions assumed in the safety analyses. The interlocks for ESFAS are as follows:

- The P-4 interlock (Reactor Trip) is enabled when the reactor trip breakers in 2-out-of-4 divisions are open. It is also enabled by all automatic reactor trip actuations. The P-4 interlock may:
    - trip the main turbine

  - permit the block of automatic safeguards actuation after time delay
  - blocks boron dilution
  - isolate main feedwater coincident with low reactor coolant temperature

- The P-6 interlock intermediate range neutron flux is actuated when the respective nuclear instrumentation system intermediate range channel goes approximately one decade above the minimum channel reading. Above the setpoint, the P-6 interlock allows a manual block of the flux multiplication actuation, permitting block of boron dilution.

- The P-11 interlock (pressurizer pressure) permits a normal unit cooldown and depressurization without safeguards actuation or main steam line and feedwater isolation. With pressurizer pressure channels less than the P-11 setpoint, it may:

  - permit manual block of safeguards actuation on low pressurizer pressure, low compensated steam line pressure, or low reactor coolant inlet temperature
  - permit manual block of steam line isolation on low reactor coolant inlet temperature
  - permit manual block of steam line isolation and SG PORV block valve closure on low compensated steam line pressure
  - coincident with manual actions of (B) or (C), automatically unblocks steam line isolation on high negative steam line pressure rate
  - permit manual block of main feedwater isolation on low reactor coolant temperature
  - permit manual block of startup feedwater isolation on low reactor coolant inlet temperature
  - permit manual block of steam dump block on low reactor coolant temperature
  - permit manual block on normal RNS isolation on high containment radioactivity

- The P-12 interlock (pressurizer level) is provided to permit mid-loop operation without CMT actuation, IRWST actuation, reactor coolant pump trip, or purification line isolation. With pressurizer level channels less than the P-12 setpoint, it may:

  - permit manual block of CMT actuation on low pressurizer level to allow mid-loop operation
  - permit manual block of RCP trip on low pressurizer level to allow mid-loop operation
  - permit manual block of auxiliary spray and purification line isolation on low pressurizer level to allow mid-loop operation
  - coincident with manual action of (A), automatically unblocks IRWST injection and fourth stage ADS initiation on low hot leg level to provide protection during mid-loop operation

- The P-19 interlock (RCS pressure) - is provided to permit water solid conditions in lower modes without automatic isolation of the CVS makeup pumps. With RCS pressure below the P-19 setpoint, it may:

  - permit manual block of CVS isolation on high pressurizer water level
  - permit manual block of PRHR HX alignment on high pressurizer water level

7.3.3 Essential Auxiliary Supporting Systems

In the AP1000 design, many essential auxiliary supporting systems traditionally classified as safety-related are classified as non-safety-related defense-in-depth systems that are important to safety. Their implementation requires regulatory oversight in accordance with SECY-94-084, "Policy and Technical Issues Associated with the Regulatory Treatment of Non-Safety Systems in Passive Plant Design," which identifies the staff's position on technical and policy issues pertaining to the regulatory treatment of non-safety systems (RTNSS) for passive ALWRs. The applicant uses PRA insights to identify systems, structures and components that are important in protecting the utilities investment and for preventing and mitigating severe accidents.

To provide reasonable assurance that these systems, structures and components are operable during anticipated events, the short-term availability controls are provided. These short-term availability controls define:

- Which equipment should be operable
- Operational modes when the equipment should be operable
- Testing and inspections that should be used to demonstrate the equipment's operability
- Operational modes that should be used for planned maintenance operations
- Remedial actions that should be taken if the equipment is not operable

These systems are included in the reliability assurance program and the operational reliability assurance process.

The following systems are included in the short-term availability control program:

- Instrumentation Systems
  - DAS ATWS Mitigation
  - DAS engineered safety features actuation
- Plant Systems
  - RNS
  - RNS - RCS open (need 2 trans at modes 5&6)
  - Component cooling water system - RCS open (need 2 trans at modes 5&6)
  - Service water system - RCS open (need 2 trans at modes 5&6)
  - Passive containment cooling system water makeup - Long term shutdown
  - MCR cooling - Long term shutdown
  - I&C room cooling - Long term shutdown
  - Hydrogen Ignitors
- Electrical Power Systems
  - AC power supplies
  - AC power supplies - RCS open (need 2 trans at modes 5&6)
  - AC power supplies - Long term shutdown
  - Non Class 1E DC and UPS system

The AP1000 RTNSS evaluation is addressed in Chapter 22 of this report.

7.3.4 ESFAS Evaluation Findings and Conclusions

The staff evaluated the ESFAS design description in the DCD against the criteria of the SRP, applicable RGs, and industry codes and standards, (including the requirements of Sections 4 and 5 of IEEE 603-1991 which are the requirements stated in10 CFR 50.55a(h)). The ESFAS detects a plant condition requiring the operation of ESF systems and initiates operation of those systems.

Because the ESFAS is part of the PMS, the evaluation of the design and qualification of the PMS, as discussed in Section 7.2 of this report, also applies to the ESFAS.
This review was concerned with the trip parameter sensors, PMS, and protection actuation circuits. On the basis of the staff's review of the information provided in the DCD Tier 2 Chapters 6, 7, 8, and 9, and the commitments made in the DCD Tier 1 Section 2.5.2 ITAAC Table, the staff concludes that the DCD provides an acceptable design description and commitments to the appropriate SRP criteria, and the commitment to implement the design by ITAAC process ensures that the ESFAS will perform as designed.

The staff concludes that the design of the AP1000 ESFAS meets the relevant requirements of GDC 1, 2, 4, 13, 19-24, 29, 34, 35, and 41, 10 CFR 50.55a(a)(1), and 10 CFR 50.55a(h), and therefore, is acceptable.

7.4 Systems Required for Safe Shutdown

7.4.1 System Description

The instrumentation and controls necessary to establish and maintain safe-shutdown conditions following an accident are designed to achieve two basic functions:

(1) maintain the core in a subcritical condition
(2) maintain adequate core cooling by removing residual heat

To accomplish a safe shutdown, the required functions are reactor trip, coolant circulation, residual heat removal, and depressurization. The ESF systems are designed to establish and maintain postaccident safe-shutdown conditions for the plant.

There are two different safe shutdown conditions that are expected following a transient or accident condition. One is short-term safe shutdown and the other is long-term safe shutdown. Short-term safe shutdown refers to the plant conditions from the start of an event until about 36 hours later. Long-term safe shutdown refers to the plant conditions after this 36 hour period. The short-term safe shutdown conditions include maintaining the reactor subcritical, the reactor coolant average temperature less than or equal to no-load temperature, and adequate coolant inventory and core cooling. These shutdown conditions shall be achieved following any of the design basis events using safety-related equipment. The long-term safe shutdown conditions are the same as the short-term conditions except that the coolant temperature shall be less than 215.6°C (420°F). GDC 34 requires that a system to remove residual heat be provided for

long term cooling. This long-term condition must be achieved within 36 hours and maintained indefinitely using safety-related equipment.

The non-safety-related systems are not required for safe shutdown of the plant. When the plant safe shutdown does not include accident response or mitigation, the non-safety-related systems normally used to support plant shutdown operations are expected to be available and can be used to support safe shutdown operations.

The following ESF systems automatically function to place the plant in a safe-shutdown condition without operator action:

- Protection and Safety Monitoring System
  - Passive Core Cooling System, including the following equipment:
  - PRHR heat exchanger
  - CMT
  - accumulators
  - IRWST
  - automatic depressurization valves

- Passive Containment Cooling System
- Class 1E dc and Uninterruptable Power Supply System
- Containment Isolation Valves
- Reactor System
- Control Rods

For establishing safe-shutdown conditions, control is possible from either the MCR or the remote shutdown workstation. The monitoring instrumentation available in the main control room for safe shutdown is safety-related and is part of the qualified display processing system.

7.4.2 Safe Shutdown From Outside the Main Control Room

If evacuation of the MCR is required because of some abnormal MCR condition, the operator can establish and maintain safe-shutdown conditions at the remote shutdown workstation. The design basis for safe shutdown at the remote shutdown workstation is an event that requires evacuation of the MCR, coincident with the loss of offsite power and a single active failure without a concurrent design-basis accident.

One remote shutdown workstation is provided for the plant, which is similar to the operator workstations in the MCR and is designed to the same standards. The remote shutdown workstation contains controls for the safety-related equipment required to establish and maintain safe shutdown. Additionally, control of non-safety-related components is available, allowing operation and control when ac power is available.

The remote shutdown workstation is provided for use following an evacuation of the MCR only. No actions are anticipated from the remote shutdown workstation during normal, emergency, routine shutdown, refueling, or maintenance operations. Operator control capability at the

remote shutdown workstation is normally disabled. Operator control capability can be transferred from the main control room workstations to the remote shutdown workstation if the control room requires evacuation. Procedures will instruct the operator to trip the reactor prior to evacuating the control room and transferring control to the remote shutdown workstation. This operator control transfer capability cannot be disabled by any single active failure coincident with the loss of offsite power.

The control transfer function is implemented by multiple transfer switches. Each individual transfer switch is associated with only a single safety-related or single non-safety-related group. These switches are located behind an unlocked access panel. Entry into this panel will result in alarms at the MCR and the remote shutdown workstation. The access panel is located within a fire zone which is separate from the MCR. The manual reactor trip switches located in the MCR is not affected by this control transfer function.

In addition to the controls and indications provided at the remote shutdown workstation, the following controls are provided outside the MCR:

- reactor trip capability at the reactor trip switchgear
- turbine trip capability at the turbine
- start/stop controls for the diesel generators located at each diesel generator local control panel
- local control at motor control centers and electrical switchgear.

DCD Tier 2 Section 7.4.3.1.1 states that "the operator displays located in the main control room and on the remote shutdown workstation are also not affected by this control transfer function. The displays on the remote shutdown workstation are operational during normal operation (from the main control room) so that they can be utilized with no delay if transfer to the remote shutdown workstation is required." This is acceptable to the staff because it maintains continuity of operation between the MCR and the remote shutdown workstation and the indication of the status of the parameters required for safe shutdown is available to the operators at both locations before, during, and following transfer between the control room and the remote shutdown workstation, and vice-versa.

7.4.3 Evaluation Findings and Conclusions

In DCD Tier 2 Section 7.4, the applicant states that, in the event of a turbine or reactor trip, non-safety-related plant systems automatically function to place the plant in hot standby (i.e., a safe-shutdown condition). Additional non-safety-related systems are available to permit the operator to manually perform normal routine plant depressurization and cooldown. The DCD also states that the ESF systems are designed to establish and maintain safe-shutdown conditions for the plant following an accident. Non-safety-related systems are not required for postaccident safe shutdown of the plant. When available, the operator will rely on the non-safety-related shutdown systems before actuating ESF systems for safe shutdown.

The staff conducted a review of these systems for conformance to the guideline in the RGs and standards applicable to these systems. The staff concludes that the DCD has adequately

described the guidelines applicable to these systems. Based on the review of the system design for conformance to the guidelines, the staff finds that there is reasonable assurance that the systems fully conform to the guideline applicable to these systems. Therefore, the staff finds that the requirements of GDC 1 and 10 CFR 50.55a(a)(1) have been met.

The review included the identification of those systems and components for the safe shutdown systems which are designed to survive the effects of earthquakes, other natural phenomena, abnormal environments and missiles. Based on the review of DCD Tier 2 Sections 3.10 and 3.11 which address the qualification programs to demonstrate the capability of those systems and components to survive the earthquakes, other natural phenomena, abnormal environments and missiles, the staff concludes that the AP1000 design has identified for those systems and components for the plant safe shutdown and those systems and components will be qualified consistent with the design bases, and satisfies the requirements of GDC 2 and GDC 4.

Based on the review, the staff concludes that instrumentation and controls have been provided to maintain variables and systems which can affect the fission process, the integrity of the reactor core, the RCPB, and the containment and its associated systems within prescribed operating ranges during plant shutdown. Therefore, the staff finds that the systems required for safe shutdown satisfy the requirements of GDC 13.

Instrumentation and controls have been provided within the control room to allow actions to be taken to maintain the plant in a safe condition during shutdown, including a shutdown following an accident. Equipment outside the control room has been provided for prompt shutdown of the reactor and to maintain the unit in a safe condition during shutdown. The staff finds that the AP1000 design satisfies the requirements of GDC 19.

The review of the instrumentation and control systems required for safe shutdown includes conformance to the requirements of testability, operability with onsite and offsite electrical power, and single failure criterion. The staff finds that the AP1000 design satisfies the requirements of GDC 34, 35, and 38.

The staff concludes that the design of the safe shutdown systems is acceptable and meets the relevant requirements of GDC 1, 2, 4, 13, 19, 34, 35, and 38, and 10 CFR 50.55a(a)(1).

7.5 Safety-Related Display Information

7.5.1 System Description

This section describes the instrumentation used by the operator to monitor and maintain safe operation of the AP1000 plant through operational occurrences and postaccident conditions. The applicant classified the variables for this instrumentation in accordance with the guidance of RG 1.97, except for the addition of the Type F classification, which is unique to the AP1000

design. The six types of variables that provide information to the control room operator are as follows:

- Type A variables are needed to diagnose the plant status in accordance with emergency operating instructions. These variables also provide information to assist the operator in taking specified, preplanned, manually controlled actions where automatic actions are not provided in order to recover from design-basis accidents and achieve a safe-shutdown condition.

  There are no specific preplanned, manually-controlled actions for postaccident safe shutdown in the AP1000 design. Therefore, no Type A variable was identified in the DCD.

- Type B variables are needed to assess the process of accomplishing or maintaining the following:

  - reactivity control
  - reactor coolant system integrity
  - reactor coolant system inventory control
  - reactor core cooling
  - heat sink maintenance
  - containment integrity

- Type C variables monitor the potential for causing a gross breach of a fission product barrier which includes the in-core fuel cladding, the RCPB, or the primary reactor containment.

- Type D variables monitor the performance of plant safety-related systems used to attain a safe-shutdown condition (by mitigating the consequences of an accident) and subsequent plant recovery.

- Type E variables monitor the habitability of the main control room. These variables are also used in determining the magnitude of radioactivity releases, assessing releases of radioactive materials, and monitoring radiation levels and radioactivity in the environment surrounding the plant.

- Type F variables provide information that allows the control room operators to take specified, preplanned, manually controlled actions using non-safety-related systems, to prevent the unnecessary actuation of safety-related systems. These variables are also used by the control room operators to monitor non-safety-related systems used to mitigate the consequences of an accident and subsequent plant recovery, and to operate non-safety related systems used for plant cooldown and to maintain plant shutdown conditions.

The design and qualification requirements of the instrumentation for the different variable types are divided into three categories, as follows:

- Category 1 instrumentation requires seismic and environmental qualification, application of the single-failure criterion, use of emergency power, and an immediately accessible display.

- Category 2 instrumentation requires environmental and seismic qualification commensurate with the required function. It may require emergency power, but not the application of the single-failure criterion or an immediately accessible display. It requires a rigorous performance verification for a single instrument channel.

- Category 3 instrumentation does not require qualification, application of the single-failure criterion, use of emergency power, or an immediately accessible display. It meets high-quality, commercial-grade qualification.

The applicant identified all postaccident monitoring variables in DCD Tier 2 Table 7.5-1. DCD Tier 2 Table 7.5-1 also provides information associated with each variable, including instrument ranges, type and category, qualification status, number of instruments required, power supply classification, and whether or not information is available as part of qualified postaccident indication on the qualified data processing system (QDPS). Based on the review of the information provided in the DCD, the staff concludes that the safety-related display information system for the AP1000 plant is designed in accordance with the guidelines of RG 1.97.

7.5.2 Processing and Display Equipment

The AP1000 processing and display function is performed by equipment which is part of the PMS, PLS, and DDS. The PMS provides signal conditioning, communications, and display functions for Category I variables and for Category 2 variables that are energized from the Class 1E dc uninterruptible power supply system. The PLS and the DDS provide signal conditioning, communications, and display functions for Category 3 variables and for Category 2 variables that are energized from the non-Class 1E dc UPS. The DDS also provides an alternate display of the variables which are displayed by the PMS. Electrical separation of the DDS and PMS is maintained through the use of isolation devices.

Class 1E position indication signal for valves and electrical breakers are powered by an electrical division with 24-hour battery capacity. The power associated with the actuation signal for each of these valves or electrical breakers is from an electrical division with 24-hour battery capacity, so there is no need to provide position indication beyond this period. The operator will verify that the valves or electrical breakers have achieved the proper position for long-term stable plant operation before position indication is lost. Electrically operated valves, which have the electrical power removed to meet the single failure criterion, are provided with redundant valve position sensors. Each of the two position sensors is powered from a different non-Class 1E power source.

7.5.3 Network Gateway (real-time to PMS)

The network Gateway is shown in block diagrams in DCD Tier 2 Section 7.1, Figures 7.1-1 and 7.1-2. In the AP1000 design, the Gateway will provide interfacing between the non-safety real-time data network and the safety-related PMS network. The Gateway is a standard commercially available device used in communication interfacing and connects two different network systems. It will allow communication protocol translation between the networks mentioned above. The Gateway has two subsystems. One subsystem is safety-related and will communicate with systems within each channel of the PMS and the other subsystem will communicate with the real-time data network. Safety channel independence is maintained. The two subsystems are connected via a fiber-optic link. The design of the Gateway as presented in the DCD is limited in detail since the communication technology available at the time of plant construction may change. Therefore, only the Gateway functional requirements and its conformance with the applicable GDC and with standards regarding safety-related I&C will be considered at this time.

DCD Tier 2 Section 7.1.2.8 states that there is "no potential signal from the non-safety system that will prevent the PMS from performing its safety function." Furthermore, the Gateway will provide electrical and communication isolation features. This is consistent with GDC 24, which states, in part, that "Interconnection of the protection and control systems shall be limited so as to assure that safety is not significantly impaired." It is also consistent with IEEE 7-4.3.2, Section 5.6, which states, in part, that "Data communication...shall not inhibit the performance of the safety function." It is important to recognize that the Gateway is a communication interface whose existence is to facilitate data transfer while not adversely impacting the safety function. Other components within the safety system, discussed in other parts of this chapter, provide electrical isolation. Furthermore, other components of the safety system will ensure that non-safety control signals do not inhibit safety-related automatic or manual controls. This is discussed in DCD Tier 2 Section 7.1.2.8 where application software will ensure safety functions have priority over non-safety controls.

Even though limited detail is provided in the DCD for the communication architecture, the staff finds the use of the Gateway shown in block diagrams in DCD Tier 2 Section 7.1, Figures 7.1-1 and 7.1-2 to be acceptable. The staff's review of this system included postulating a malicious cyber attack on the safety system from the real-time data network. DCD Tier 2 Section 7.1.2.8 addresses this concern and the staff concludes that any real-time network activity should not prevent the PMS from performing its safety-function if the ITAAC design commitment is appropriately implemented.

7.5.4 Operation and Control Centers System

The OCS includes the main control room, the technical support center, the remote shutdown workstation, emergency operation facility, local control station and associated workstations for each of these centers. The human system interface design includes the design of the OCS and

each of the human system interface resources. The AP1000 human system interface resources include:

- Wall panel information system
- Alarm system
- Plant information system
- Computerized procedure system
- Soft control/dedicated controls
- Qualified data processing system

The wall panel information system presents information about the plant for use by the operators. No control capabilities are included. The wall panel information system provides dynamic display of plant parameters and alarm information so that a high level of current plant status can be understood. It provides information important to maintaining the situation awareness of the crew and supporting crew coordination. It also serves as the alarm system overview panel display. The display of plant disturbances (alarms) and plant process data is integrated on this wall panel information system display. The wall panel information system is a non-safety-related system. It is designed to have a high level of reliability.

The AP1000 alarm system is to provide the operation and control centers operating staff with the means for acquiring and understanding the plant's behavior. The alarm system supports the control room crew members by the following steps:

- The "alert" activity, which alerts the operator to off-normal conditions
- The "observe what is abnormal" activity, which aids the user in focusing on the important issues
- The process "state identification" activity, which aids the user in understanding the abnormal conditions and provides corrective action guidance. It guides the operators into the information display system.

The plant information system provides dynamic indications of plant parameters and visual alerts. The plant information system uses color-graphic video display units located on the operation and control centers workstations to display plant process data. These displays provide information important to monitoring, planning, and controlling the operation of plant systems and obtaining feedback on control actions. The displays provided by the plant information system are non-safety-related displays, but provide information about both safety-related and non-safety-related systems.

The computerized procedure system assists plant operators in monitoring and controlling the execution of plant procedures. The computerized procedure system is accessible from the operator workstations in MCR. The design of a backup to the computerized procedure system to handle the event of a loss of the computerized procedure system is developed as part of the human system interface design process. Design options include the use of backup procedures written on paper.

The MCR provides a limited set of dedicated control switches and soft controls. The dedicated control switches are used to perform a dedicated single function, with each switch having a single action. The soft control units are used to provide a compact alternative to the traditional control board switches by substituting virtual switches in place of the discrete switches.

The qualified data processing system is to provide a Class 1E system is designed to present to the MCR operators, the plant parameters which demonstrate the safety of the plant. The qualified data processing system provides for the display of the variables through safety-related displays. The information content of the qualified data processing system displays is provided to the remote shutdown workstation through the plant information system.

7.5.5 The Qualified Data Processing System

The portion of the PMS which is dedicated to providing the safety-related display function is referred to as the QDPS. The QDPS has a redundant configuration consisting of sensors, QDPS hardware, and qualified displays. The QDPS provides postaccident monitoring information at the MCR and the same information can be transmitted to the remote shutdown workstation. The QDPS provides status information on the postaccident Category 1 variables and selected Category 2 or 3 variables, as determined from the function-based task analysis. It also provides a set of system-level displays to support the emergency procedures and aid the operator in implementing function restoration and plant recovery. The QDPS provides the operator with sufficient operational data to safely shut the plant down in the event of a failure of the other display systems.

The QDPS are divided into two separate electrical divisions. Each of the two electrical divisions is connected to a class 1E dc uninterruptible power system with sufficient battery capacity to provide necessary electrical power for 72 hours. If all ac power sources are lost for a period of time that exceeds 72 hours, the power supply system will be energized from the ancillary diesel generator. Instrumentation associated with primary variables that are energized from the Class 1E dc uninterruptible power supply are powered from one of the two electrical divisions with 72-hour battery capacity. Other variables are energized from electrical divisions with 24-hour battery capacity.

7.5.6 Bypass and Inoperable Status Information

RG 1.47, "Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems," states that the operator needs to know the operating status of safety-related systems, and the extent to which safety-related systems have been bypassed. The AP1000 design incorporates this information into the alarm system, the operator’s workstation, and wall panel information system in the MCR. High-level plant status during any plant state is continuously available on the wall panel information system. At the operator’s workstation, physical and functional displays show how a component’s availability or unavailability impacts the alignment and availability of the system. This is indicated on the display that includes the bypassed or deliberately induced inoperability of the protection system and the systems actuated or controlled by that protection system. Alarms on the operator’s workstation and the wall panel information system indicate abnormal conditions. Improper safety system alignments, safety-

related component unavailability, and bypassed protective functions are considered in the alarm logic. This information is continuously monitored by the alarm system.

Indication is provided for the following conditions in accordance with RG 1.47:

- inoperability of any redundant portion of the reactor protection system, systems actuated or controlled by the reactor protection system, and auxiliary or supporting systems that must be operable for the protection system (and the system it actuates) to perform their safety-related functions
- inoperability expected to occur more frequently than once a year
- inoperability expected to occur when the affected system is normally required to be operable
- manually-initiated inoperability

Based on the above discussion, the staff concludes that the AP1000 design conforms with the guidelines of RG 1.47 regarding indicating the operating status, including the bypassed status of safety-related systems. Therefore, the staff concludes that the design is acceptable.

7.5.7 Incore Instrumentation System

Instead of the traditional movable detector system used in most of the operating PWR plants, the AP1000 plant design includes the IIS, a fixed incore detector system, to measure incore neutron flux distribution. The primary function of the IIS is to provide a three-dimensional flux map of the reactor core. This map is used to calibrate neutron detectors used by the protection and safety monitoring system, as well as to optimize core performance. A secondary function of the incore instrumentation system is to provide the PMS with the signal necessary for monitoring core exit temperatures.

During plant operation, the incore instrument thimble assembly is positioned within the fuel assembly and exits through the top of the RV into containment. The fixed incore detector and core exit thermocouple cables are then routed to different data processing stations. The data is processed and the results are available for display in the MCR.

The incore instrumentation system data processor receives the transmitted digitized fixed incore detector signals from the signal processor. It then combines the measured data with analytically derived constants, and certain other plant instrumentation sensor signals, to generate a full three-dimensional indication of nuclear power distribution in the reactor core. The hardware and software which performs the three-dimensional power distribution calculation are capable of executing the calculation algorithms and constructing graphical and tabular displays of core conditions at intervals of less than 1 minute. The analysis software provides information required to activate a visual alarm display to alert the operator about the current existence of, or the potential for, reactor operating limit violations.

The calculation algorithms are capable of determining the core average axial offset using a set of the total 42 incore monitor assemblies. A minimum set of incore monitor assemblies consists of:

- 30 operating assemblies, with at least two operating assemblies in each quadrant, prior to nuclear model calibration; and
- 21 operating assemblies, with at least two operating assemblies in each quadrant, after nuclear model calibration.

The nuclear model calibration is performed after each new core load.

Even though the flux mapping function is not considered as a safety-related function, nevertheless, the quality of the hardware and software of the IIS needs to be equivalent to that of the PMS because the signal from IIS is used to calibrate the ex-core nuclear instrumentation input to the overtemperature and overpower reactor trip setpoints. To ensure the quality of the IIS, the ITAAC for the system design process will be applied. DCD Tier 1 Section 2.5.5 provides the design description and design commitment in the ITAAC table. The ITAAC process will verify the design requirements including the separation provision between class 1E and non-1E components. The staff finds that the information of the IIS provided in DCD Tier 1 and Tier 2 are acceptable.

7.5.8 Special Monitoring System

The digital metal impact monitoring system is a non-safety-related special monitoring system that monitors the reactor coolant system for metallic loose parts. It consists of several active instrument channels, each comprising of a piezoelectric accelerometer (sensor), and signal conditioning and diagnostic equipment. In DCD Tier 2 Section 4.4.6.4, the applicant states that conformance with RG 1.133, "Loose-Part Detection Program for the Primary System of Light-Water-Cooled Reactors," is described in DCD Tier 2 Section 1.9.1. The staff's evaluation of this issue is addressed in Section 4.4 of this report. DCD Tier 1 Section 2.5.6, Table 2.5.6-1 provides the design description of the SMS and its associated ITAAC design commitment. DCD Tier 1 Section 2.5.6 provides design description including the provision to retrieve the metal impact monitoring data in the main control room and design commitment in the ITAAC table. The staff finds that the information of the SMS provided in DCD Tier 1 and Tier 2 are acceptable.

7.5.9 Evaluation Findings and Conclusions

The staff conducted a review of the information systems important to safety for conformance with applicable RGs and industry codes and standards. The staff finds that the DCD has adequately classified and identified the guidelines applicable to these systems. Therefore, the staff finds that the requirements of GDC 1 and 10 CFR 50.55a(a)(1) have been met.

The review included the identification of those information systems and components that are important to safety and are designed to survive the effects of earthquakes, other natural phenomena, abnormal environments, and missiles. Based on its review, the staff concludes

that the DCD has identified those systems and components consistent with the design bases for these systems. DCD Tier 2 Sections 3.10 and 3.11 address the qualification programs to demonstrate the capability of these systems and components to survive these events. The staff finds that the requirements of GDC 2 and 4 have been met.

The non-safety portions of information systems are appropriately isolated from safety systems, including the safety portions of the information systems. The staff finds that the isolation of these systems from safety systems satisfies the requirements of 10 CFR 50.55a(h) and the requirements of GDC 24.

The postaccident monitoring system conforms to the guidelines in RG 1.97 regarding the assessment of plant conditions during and following an accident. The redundant information systems conform to the guidelines for the physical independence of electrical systems provided in RG 1.75. The postaccident monitoring system includes appropriate variables. The range and accuracy of the instrument channels for these variables are consistent with the plant safety analysis. The staff finds that the post-monitoring system meets the requirements of GDC 13 and 19.

The staff reviewed the systems for which a bypassed or inoperable status is indicated in the control room. The staff finds that the bypass indications will give the operators timely information and status so that the operators can mitigate the effects of unexpected system unavailability. Therefore, the bypass indications satisfy the guidelines of RG 1.47. Based on the discussion above, the staff finds that the design meets the applicable requirements of 10 CFR 50.55a(h).

The staff concludes that the design of the information systems important to safety is acceptable and meet the relevant requirements of GDC 1, 2, 4, 13, 19, and 24, 10 CFR 50.55a(a)(1), and 10 CFR 50.55a(h).

7.6 Interlock Systems Important to Safety

The areas reviewed in DCD Tier 2 Section 7.6 include those interlock systems that reduce the probability of occurrence of specific events or verify the state of a safety system. These systems include interlocks to prevent overpressurization of low-pressure systems and interlocks to verify availability of safeguard functions.

The staff reviewed the interlock systems to confirm that such design considerations as redundancy, independence, single failures, qualification, bypasses, status indication, and testing are consistent with the design bases of these systems and commensurate with the importance of the safety functions to be performed.

7.6.1 Normal Residual Heat Removal System Isolation Valves

An interlock is provided for the normally closed, motor-operated RNS inner and outer suction isolation valves. The interlock prevents the RNS suction valves from being opened by operator

action unless the RCS pressure is less than a preset pressure and the IRWST suction and discharge valves are in a closed position.

There are two motor-operated valves in series in each of the two parallel paths of the RNS pumps suction line from the RCS hot leg. The two valves near the RCS hot leg are designated as the inner isolation valves and the two valves near the RNS pumps are designated as the outer isolation valves. The logic for operation of the inner valves and the outer valves is identical. The pressure transmitter used for valve interlocks on the inner valves is diverse from the pressure transmitter used for the outer valve interlocks. These four motor-operated valves are powered from safety-grade 125-V dc busses. The inner valve is powered by a separate power supply from the outer valve of each series combination. The valves may be closed by operator action from the MCR at any time. During extended normal residual heat removal operations following cooldown, the isolation valves' motor breakers are opened or removed to prevent an inadvertent closure of the valves. Alarms are provided in the MCR and on the remote shutdown workstation to alert the operator if RCS pressure exceeds the RNS design pressure after the valves are opened.

The safety function of the RNS isolation valves is to remain closed (i.e., the interlocks prevent the valves from being opened while the reactor is pressurized). In the unlikely event that two RNS isolation valves are opened at power, the RNS relief valves provide system overpressure protection.

The isolation valve interlock logic is provided in DCD Tier 2 Figure 7.2-1, Sheet 18. Because of the possible severity of the consequences of loss of function, the RNS has the following design features:

- The protection system function of RNS isolation is provided by two parallel sets of two valves in series. The interlock components are redundant with the inner valve powered by a separate power supply from the outer valve of each series combination.
- The pressure interlock signals and logic are tested online. This test includes the initiating signals for the interlocks from the protection and safety monitoring system cabinets.

The staff finds that the design for RNS isolation satisfies the single failure criterion and the online testability requirement of IEEE 603-1991, and therefore, is acceptable.

7.6.2 Interlocks for the Accumulator Isolation Valve and IRWST Discharge Valve

The accumulator isolation and IRWST injection isolation valves are safety-related in order to retain their pressure boundary and remain in their open position. The accumulator isolation and IRWST injection valve operators are nonsafety-related since the valves are not required to change position to mitigate an accident. The TS require these valves to be open and power locked out whenever these injection paths are required to be available. The TS require verification every 24 hours that the motor-operated valves are open. They also require verification every 31 days that power is removed. With power locked out, redundant valve position indication is provided in the MCR and remote shutdown workstation. Valve position indication and alarm are provided to alert the operator if these valves are mispositioned. In

addition, the valves have a confirmatory open signal during an accident. The valves also have an automatic open signal when their close permissive clears during plant startup. The confirmatory open and automatic open control signals are provided to the valve operator by the plant control system.

These valves are considered to be in "operating bypass" because, if closed, they prevent the associated systems from performing their intended safety functions. IEEE 603 has a requirement for automatic removal of the operating bypass when the applicable permissives are not met.

The safety analyses in DCD Tier 2 Chapter 15, "Accident Analysis," assume that these valves are not subject to valve mispositioning (prior to an accident) or spurious closure (during an accident). Based on the confirmatory open signals, the TS verification requirements, and conformance with IEEE Std. 603 requirements, the staff finds the design acceptable.

7.6.3 Core Makeup Tank Cold Leg Balance Line Isolation Valves

Each CMT has a cold leg balance line which is provided with a normally open, motor-operated, isolation valve. The balance line isolation valves may be manually controlled from either the MCR or the remote shutdown workstation. A confirmatory open signal to these valves automatically overrides any bypass features that are provided to allow the balance line isolation valve to be closed for short periods of time. The control circuit has a valve maintain-closed actuation function to provide an administratively controlled manual block of the automatic opening of the valve when the pressurizer level is greater than the P-12 interlock. This function allows the valve to be maintained closed if needed for leakage isolation. The maximum permissible time that a CMT cold-leg balance line isolation valve can be closed is specified in the TS. An alarm is actuated when the maintain closed function is reinstated.

Each valve is interlocked so that the following conditions occur:

- If the maintain closed actuation has not been manually initiated, it opens automatically on receipt of a confirmatory open signal with the control circuit in automatic control or during the manual valve close function.
- It opens automatically whenever the pressurizer water level increases above the P-12 interlock, and the control circuit is in automatic control.
- It cannot be manually closed when a confirmatory open signal is present.

During power and shutdown operations, the CMT cold leg balance line isolation valve remains open. To prevent an inadvertent closure of the valve, redundant output cards are used in the protection logic cabinet.

These normally open motor-operated valves have alarms indicating valve mispositioning (with regard to their passive core cooling function). The alarm actuates in the MCR and the remote shutdown workstation.

The staff finds that the interlock logic design of the CMT cold leg balance line isolation valves is consistent with the requirement of IEEE 603 criteria for safety related functions, and therefore, is acceptable.

7.6.4 PRHR Heat Exchanger Inlet Isolation Valve

The PRHR heat exchanger inlet line includes a normally open, motor-operated isolation valve that is controlled from the MCR and remote shutdown workstation. This valve opens when a PRHR actuation signal is initiated. This confirmatory signal provides a means to automatically override bypass features (which are provided to allow closure of the valve in order to perform operability testing). The maximum permissible time is specified in the TS. This valve cannot be manually closed when a PRHR heat exchanger actuation signal is present.

During plant operation and shutdown, the PRHR heat exchanger inlet valve is open. To prevent an inadvertent closure of the valve, redundant output cards are used in the PMS cabinet. Power to the valve is normally locked out at power to prevent a fire-induced spurious closing. DCD Tier 2 Figure 7.2-1, Sheet 17 provides the interlock logic of the PRHR isolation valve.

The PRHR isolation valve has an alarm indicating valve misposition. The alarm in the MCR and the remote shutdown work-station actuates under the following conditions:

- Sensors on the motor operator for the valve indicate the valve is not fully open.
- Redundant sensors on the valve stem indicate the valve is not fully open.

The staff finds that the interlock logic design of the PRHR HX inlet isolation valve is consistent with the requirements of IEEE 603 criteria for safety-related functions and therefore, is acceptable.

7.6.5 Evaluation Findings and Conclusions

The review of the interlock systems important to safety included the interlocks for the following valves:

- RNS isolation valves to prevent overpressurization of low pressure systems when connected to the primary coolant system
- accumulator isolation valves
- IRWST discharge isolation valves
- CMT cold leg balance line isolation valves
- PRHR heat exchanger inlet isolation valves.

The staff conducted a review of these systems for the conformance to the guidelines in the RGs and industry codes and standards applicable to these systems. The staff finds that the DCD has adequately identified the guidelines applicable to these systems and has properly classified them. The staff finds that there is reasonable assurance that the systems fully conform to the guidelines applicable to these systems. Therefore, the design meets the requirements of GDC 1 and 10 CFR 50.55a(a)(1).

Based on the review of interlock system functions, the staff finds that appropriate interlocks are provided to maintain an appropriate design margin to assure that acceptable fuel design limits are not exceeded during any condition of normal operation, including the effects of anticipated operational occurrences. Therefore, the staff finds that the interlock systems satisfy the requirements of GDC 10, 15, 16, 33, 34, 35.

Based on the review of interlock system status information, initiation capabilities, and provisions to support safe shutdown, the staff concludes that the interlock system's capability to monitor interlocks over the anticipated ranges for normal operation, for anticipated operational occurrences, and accident conditions is appropriate to assure adequate safety. Appropriate controls are provided for interlock initiation and bypass. Based on the discussion above, the staff finds that the design satisfies the requirements of GDC 13 and 19.

The review included the identification of these interlock systems and components that are designed to survive the effects of earthquakes, other natural phenomena, abnormal environments. Based on the review, the staff finds that these systems satisfy the requirements of GDC 2 and 4.

The staff concludes that the design of the interlock systems is established in accordance with its safety function and is acceptable. Therefore, the staff concludes that the interlock systems meet the relevant requirements of GDC 1, 2, 4, 10, 13, 15, 16, 19, 33, 34, 35, 10 CFR 50.55a(a)(1), and 10 CFR 50.55a(h).

7.7 Control and Instrumentation Systems

7.7.1 System Description

The I&C systems reviewed in this section include control systems used for normal operation. (That is, systems which are not relied upon to perform safety functions following anticipated operational occurrences or accidents, but the control processes may affect plant safety). These control systems perform the following normal operating and normal startup/shutdown functions:

- reactor power control
- rod control
- pressurizer pressure control
- pressurizer water level control
- feedwater control
- steam dump control
- rapid power reduction
- defense-in-depth control

In addition, this section addresses the review of the DAS that provides a diverse backup to the protection system and mitigates the consequences of the ATWS events. This section also addresses the review of non-safety-related defense-in-depth systems that have been determined to be risk significant from the PRA review. These systems were reviewed based on the guidance provided in SECY-94-084 on the RTNSS process.

7.7.1.1 Reactor Power Control System

The reactor power control system performs automatic reactor power control and power distribution control by varying the position of the control rods. Separate control banks are used to regulate reactor power and power distribution. The power control system enables the plant to respond to the load changes for plus and minus 10 percent step load change, ramp load increases and decreases of 5 percent per minute, grid frequency response resulting in a maximum of 10 percent power change of 2 percent per minute. The system also enables daily load-follow operation. These capabilities are accomplished without resulting in a reactor trip or steam dump actuation.

The reactor power control system uses one control subsystem for regulating core power (M banks) and one control subsystem to regulate axial offset (AO bank). During load follow or load regulation response transients, the power control and the axial offset control subsystems jointly function to control both core power and axial offset. The power control system controls the reactor coolant average temperature by regulating the M control rod bank positions. The reactor coolant loop average temperatures are determined from hot and cold leg measurements in each reactor coolant loop. The programmed coolant temperature increases linearly with turbine load. The temperature input signals are fed from protection channels via isolation devices. Deviation of the reactor coolant temperature from the programmed value is the basic control variable for reactor power control. A separate control strategy is used at low-power levels when the turbine is offline and the steam dump system is used to regulate coolant temperature. In this mode, the operator enters a power level setpoint and a desired rate of change into the setpoint calculator. The nuclear power setpoint calculator then supplies a linear ramp change in core power at the selected rate to the new setpoint.

The axial offset control is performed by the axial offset rods. Measurements of axial offset are put into the control system and then compared to an axial offset control "window." When the axial offset error is outside the acceptable control window, the axial offset rods actuate at a fixed speed to recover the axial offset.

To minimize the potential for interactions between the reactor power and the axial offset rod control systems, the reactor power control system takes precedence. If a demand signal exists for movement of the power control rods, the axial offset rods are blocked from moving.

7.7.1.2 Rod Control System

The rod control system receives rod speed and direction signals from the power control system and the axial offset control systems. For power control, the rod speed demand signals vary over the range of 5 to 45 inches per minute (8 to 72 steps per minute). For axial offset control, the rod speed demand signals are fixed at a constant speed of 5 inches per minute (8 steps per minute). Manual control is provided to move a bank in or out at a prescribed fixed speed. In the automatic mode, the rods are withdrawn or inserted within the limits imposed by the control interlocks. The power and axial offset control banks are the only rods that can be manipulated under automatic control.

The three shutdown banks are always in the fully withdrawn position during normal operation and are moved to this position at a constant speed by manual control before criticality. A reactor trip causes them to fall by gravity into the core.

The variable speed rod drive programmer, used in the power control system, inserts small amounts of reactivity at low speed. This permits fine control of reactor coolant average temperature about a small temperature dead band, as well as furnishing controls at high speed for transients such as load rejections.

The digital rod position indication system measures the position of each rod using a detector consisting of discrete coils mounted concentrically with the rod drive pressure housing. The coils are located axially along the pressure housing and magnetically sense the entry and presence of the rod drive shaft through its center line. The demand position system counts the pulses generated in the rod drive control system and provides a digital readout of the demanded bank position. The demanded and measured rod positions are displayed in the MCR. An audible alarm is generated whenever an individual rod position signal deviates from the other rods in the bank by a preset limit. Alarms are also generated if any shutdown rod is detected to have left its fully withdrawn position, or if any M-bank control rods are detected at the bottom position, except as part of the normal insertion sequence. The purpose of the control bank rod insertion alarms and interlocks is to provide warning to the operator of excessive rod insertion and to terminate the insertion.

Rod stops are provided to prevent abnormal power conditions that could result from excessive control rod withdrawal initiated by either a control system malfunction or operator violation of administrative procedures.

7.7.1.3 Pressurizer Pressure Control

Pressurizer pressure control is designed to provide stable and accurate control of the primary system pressure to its predetermined setpoint. During steady-state operating conditions, the pressurizer heater output is regulated to compensate for pressurizer heat loss and a small continuous pressurizer spray. During normal transient operation, pressurizer pressure is regulated to provide an adequate margin to limit unnecessary safety systems actuation or reactor trip.

Small or slowly varying changes in pressure are regulated by modulation of the variable heater control. Decreases in pressure larger than that which can be accommodated by the variable heater control results in the actuation of the backup heaters, as does a large increase in the pressurizer water level. Pressure increases that are too fast to be handled by reducing the variable heater output result in pressurizer spray actuation. Spray continues until pressure decreases to the point that the variable heater alone is capable of regulating pressure. For normal transients including a full-load rejection, the pressurizer pressure control system acts promptly to prevent reaching the high pressurizer pressure reactor trip setpoint.

7.7.1.4 Pressurizer Water Level Control

Pressurizer water level control provides stable and accurate control of pressurizer level within a prescribed deadband around a programmed value. As the reactor coolant system temperature is increased from zero-load to full-load value, the reactor coolant system fluid volume expands. The pressurizer level is programmed to absorb this change. A deadband is provided around the pressurizer level program to intermittently control charging and letdown. When pressurizer level reaches the lower limit of the deadband, the charging system is actuated, which continues to operate until pressurizer level is restored to a limit above the nominal programmed value. When the level reaches the upper limit of the deadband, letdown to the liquid waste processing system is actuated. Automatic pressurizer level control is supplied from the point in the startup cycle where the zero-load level is established up through 100-percent power.

7.7.1.5 Feedwater Control

Two modes of feedwater control are incorporated in the feedwater control system:

- In the high-power control mode, feedwater flow is regulated in response to changes in steam flow, and proportional plus integral SG narrow-range level deviation from a setpoint.

- In the low-power control mode, feedwater flow is regulated in response to changes in SG wide-range water level, and proportional plus integral SG narrow-range level deviation from the preestablished setpoint.

A separate low range feedwater flow measurement is used in the low-power feedwater control mode. The transition from the low-power to the high-power control mode is initiated when the transition point is low enough to allow effective feedforward control using the wide range level. In the high-power control mode, feedwater flow indication is provided within the upper limit of the low range feedwater flow measurement instrument. Tracking of SG level deviation is provided to allow a smooth transition between control modes and between manual and automatic control.

7.7.1.6 Steam Dump Control

The AP1000 has a design objective to sustain a 100-percent load rejection, or a turbine trip from 100-percent power, without generating a reactor trip, requiring atmospheric steam relief, or opening a pressurizer or SG safety valve. The automatic steam dump control system, in conjunction with the rapid power reduction system, is provided to accommodate this abnormal load rejection and to reduce the effects of the transient imposed on the reactor coolant system. The steam dump system is sized to pass 40 percent of the total nominal steam flow. This capacity is sufficient to handle reactor trips from any power level, turbine trips from 50-percent power or less, or load rejections of 50 percent or less.

The steam dump control system has two modes of operation:

- The T_{avg} mode uses the difference between measured auctioneered loop T_{avg} and a reference temperature derived from turbine first-stage impulse pressure to generate a steam dump demand signal. This mode is used for at-power transients requiring steam dump.

- The pressure mode uses the difference between measured steam header pressure and a pressure setpoint to generate a steam dump demand signal. This mode is used for low-power conditions and for plant cooldown.

The load rejection steam dump controller prevents a large increase in reactor coolant temperature following a large, sudden load decrease. The error signal is the difference between the lead-lag compensated selected T_{avg} and the selected reference T_{avg} (designated T_{ref}), based on turbine impulse chamber pressure. Following a sudden load decrease, T_{ref} is immediately decreased and T_{avg} tends to increase. This generates an immediate demand signal for steam dump. Following the opening of the steam dump valve, the control rods insert in a normal controlled manner to reduce the reactor power to match the turbine load. For a reactor trip situation, the load rejection steam dump controller is defeated and the plant steam dump controller becomes active. Since control rods are not available in this situation, the demand signal is the error signal between the lead-lag compensated auctioneered T_{avg} and the no-load reference T_{avg}. When the error signal exceeds a predetermined setpoint, the dump valves are opened in a prescribed sequence.

The steam header pressure control mode is manually selected by the operator. The pressure setpoint is manually adjusted based on the desired reactor coolant system temperature. The controller also has a feature that allows for automatically controlled plant cooldowns at a chosen rate (within limits). The operator can enter the desired cooldown rate and the desired targeted reactor coolant system temperature. The control system then dumps the required steam to achieve the setpoint cooldown rate and the cooldown stops at the target reactor coolant system temperature setpoint.

7.7.1.7 Rapid Power Reduction

The rapid power reduction system reduces nuclear power to a level capable of being handled by the steam dump system for a large load rejection. When a large and rapid turbine load rejection (via a lead/lag circuit) is detected, the circuit provides a signal demanding the release of a preselected number of control rods. Dropping these preselected rods causes the reactor power to rapidly reduce to approximately 50-percent power. The large load rejection also actuates the steam dump system and the power control system via a primary-to-secondary power mismatch signal. Following the initial opening, the steam dump valves modulate closed based upon the (T_{avg} - T_{ref}) signal.

Controlled rod insertion and steam dump modulation continues until power is reduced to approximately 15-percent power. The plant stabilizes with the steam dump maintained to match the steam flow to the thermal load. The operators can then switch to the pressure mode

of control on the steam dump system, recover the released rods, and establish normal rod control. A normal power escalation can then be performed.

7.7.2 Diverse Actuation System

The DAS is a non-safety-related system that provides diverse backup to the protection system. The applicant states that this backup is included to support the AP1000 risk goals by reducing the probability of a severe accident as a result of the coincidence of postulated transients and a postulated common-mode failure in the protection and control systems. The specific functions performed by the DAS are selected based on the PRA evaluation. The DAS provides automatic actuation signals, manual actuation signals, and indications for the plant operators. These signals are generated in a functionally diverse manner from the protection system actuation signals. The common-mode failure of sensors of a similar design is also considered in the selection of these functions.

The DAS automatic actuation is accomplished by a microprocessor-based system. Diversity from the PMS is achieved by using a different architecture, different hardware implementation, and different software. Software diversity is achieved by running different operating systems and programming in a different language. The DAS is subject to the following automatic actuations:

- trip control rods via the motor-generator set, trip turbine, and initiate the PRHR system on low wide range SG level
- initiate PRHR and close the IRWST gutter isolation valves on high hot leg temperature
- trip control rods via the motor-generator set, trip turbine, actuate the CMTs, and trip the reactor coolant pump on low pressurizer water level
- isolate critical containment penetration and start passive containment cooling water flow on high containment temperature

The selection of setpoints and time responses is determined so that the DAS automatic functions do not actuate unless the protection system has failed to actuate to control plant conditions. The DAS automatic logic combines the signals from two redundant subsystems in a two-out-of-two logic. The two-out-of-two logic is implemented by connecting the final actuation devices in series. Actuation signals are output to the loads in the form of normally de-energized, energize-to-actuate contacts, with a nominal voltage of 120 V ac or 125 V dc. The use of the normally de-energized output state, along with the dual, two-out-of-two logic, reduces the probability of inadvertent actuation.

The manual actuation of the DAS is implemented by wiring the controls located in the MCR directly to the final loads in a way that completely bypasses the normal path through the control

board multiplexers, the PMS cabinets, and the DAS automatic logic. The diverse manual functions are as follows:

- reactor and turbine trip
- PRHR actuation and close IRWST gutter isolation valves
- CMT actuation and RCP trip
- ADS valve actuation (stages 1,2,3,&4)
- passive containment cooling actuation
- critical containment penetration isolation
- containment hydrogen ignitor actuation
- initiate IRWST injection
- initiate containment recirculation
- initiate IRWST drain to containment

To support the diverse manual actuations, sensor outputs are displayed in the MCR that is diverse from the protection system display functions. The following indications are provided from at least two sensors per function:

- wide range SG water level for reactor trip and PRHR actuations, and for overfill prevention by manual actuation of the ADS valves
- hot leg temperature for PRHR
- core exit temperature for ADS actuation and subsequent initiation of IRWST injection and also for containment hydrogen igniter actuation
- pressurizer level for CMT actuation and reactor coolant pump trip
- containment temperature for containment isolation and passive containment cooling system actuation

The DAS uses sensors that are separate from those being used by the PMS and the PLS. This prevents failures from propagating to the other plant systems through the shared sensors. There is signal isolation between the two subsystems within the DAS, one for each input and output path. These isolators are characterized by a high common mode voltage withstand capability to provide the necessary isolation against faults propagation between the DAS subsystems. Actuation interfaces are shared between the DAS and the PMS. The DAS actuation devices are isolated from the PMS actuation devices, so as to avoid adverse interactions between two systems. The actuation devices of each system are capable of independent operation that is not affected by the operation of the other. The DAS and the PMS use independent and separate uninterruptible power supplies. This type of interface prevents the failure of an actuation device in one system from propagating a failure into the other system. The DAS is designed to actuate components only in a manner that initiates the safety function. The DAS is designed so that, once actuated, the mitigation action goes to completion, and the subsequent return to operation requires deliberate operator action.

As stated in the AP1000 PRA, the DAS is needed to mitigate ATWS events. For Westinghouse plants, the ATWS rule (10 CFR 50.62) requires diverse actuation of auxiliary feedwater and turbine trip. The DAS provides for the ATWS protection features mandated for the applicant's plants plus a diverse reactor scram. As discussed in Section 7.1.6 of this report, the DAS is

also provided as the system designed to meet the Commission-approved position on I&C system defense-in-depth and diversity and performs the same functions as the PMS for accident mitigation when a postulated common-mode failure disables the PMS.

DCD Tier 1 Section 2.5.1, "Diverse Actuation System," provides a design description and design commitment in the ITAAC table. On the basis of the staff's review of the information stated above, the staff finds that the DAS design meets the requirements of the defense-in-depth position. The design process described in the DCD Tier 1 Section 2.5.1 has provided reasonable assurance that the DAS will meet quality standards, and therefore, is acceptable.

7.7.3 Signal Selector Algorithms

Signal selector algorithms provide the plant control system with the ability to obtain inputs from the PMS. Each signal selector algorithm receives data from each of the redundant divisions of the PMS. The data is received from each division through an isolation device. The signal selector algorithms select those protection system signals that represent the actual status of the plant and reject erroneous signals. Therefore, the control system does not cause an unsafe control action to occur even if one of four redundant protection channels is degraded by random failure simultaneous with another of the four channels bypassed for test or maintenance.

The signal selector algorithms provide validated process values to the plant control system. They also provide the validation status, the average of the valid process values, the number of valid process values, and alarms (if one process value has been rejected). For the logic values received from the PMS, such as permissive, the signal selector algorithms perform voting on the logic values to provide a valid logic value to the plant control system.

The staff concludes that implementing signal selector algorithms in the plant control system design will improve the reliability of the control system and minimize challenges to the protection systems. Therefore, the staff concludes that the signal selector algorithms design is acceptable.

7.7.4 Evaluation Findings and Conclusions

The staff conducted a review of these systems for conformance to the guidelines in the RGs and industry codes and standards applicable to these systems. The staff finds that the DCD has adequately classified and identified the guidelines applicable to these systems. The staff finds that the control systems are appropriately designed and are of sufficient quality to minimize the potential for challenges to safety systems. Based on the review of the system design for conformance to the guidelines, the staff finds that there is reasonable assurance that the systems fully conform to the guidelines applicable to these systems. Therefore, the staff finds that the requirements of GDC 1 and 10 CFR 50.55a(a)(1) have been met.

The control systems that are used for normal operation are not relied upon to perform safety functions, but to control plant processes having a significant impact on plant safety. These control systems include the reactivity control systems, as well as control systems for primary

and secondary coolant flow. The staff's review of the control systems included features of these systems for both manual and automatic control of non-safety-related process systems. The staff concludes that the control systems permit actions to be taken to operate the plant safely during normal operation, including operational occurrences. The staff finds that the control systems satisfy the requirements of GDC 13 and 19.

Isolation devices are used in the AP1000 I&C system design to maintain the electrical independence of divisions, and to prevent interaction between non-safety-related systems and the safety-related system. Isolation devices are incorporated into selected interconnections to maintain division independence. Isolation devices serve to prevent credible faults in one circuit from propagating. On the basis of its review, the staff further concludes that the isolation between control and protection systems meets the guidelines of IEEE-603 as endorsed in RG 1.153, and therefore meets the requirements of 10 CFR 50.55a(h) and GDC 24 for assurance of safety functions in the event of control system failure.

The conclusions of the analysis of anticipated operational occurrences and accidents as presented in DCD Tier 2 Chapter 15 have been used to confirm that plant safety is not dependent upon the response of the control systems. The staff also confirmed that failure of the control systems themselves or as a consequence of supporting system failure, such as loss of power sources, does not result in plant conditions more severe than those described in the analysis of design-basis accidents and anticipated operational occurrences.

The staff concludes that the design of the control systems is acceptable and meets the relevant requirements of GDC 1, 13, 19 and 24, and 10 CFR 50.55a(a)(1), and 10 CFR 50.55a(h).