7.0 INSTRUMENTATION AND CONTROL

Westinghouse has submitted information in support of its Design Certification Amendment application that Westinghouse considers "proprietary" within the meaning of the definition provided in Title 10, Code of Federal Regulations, Section 2.390(b)(5). Westinghouse has requested that this information be withheld from public disclosure and the NRC staff agrees that the submitted information sought to be withheld contains proprietary commercial information and should be withheld from public disclosure. This Chapter of the NRC staff's evaluation contains proprietary information that has been redacted in order to make the evaluation available to the public. The redacted information appears within "square brackets" as follows:

[ ]

The complete text of this Chapter, containing proprietary information can be found at ADAMS Accession Number ML102210237 and can be accessed by those who have specific authorization to access Westinghouse proprietary information.

7.1 Introduction

Chapter 7 of the AP1000 design control document (DCD), Revision 17, contains changes to the descriptions of commitments pertaining to the primary instrumentation and control (I&C) systems of the AP1000 design, as evaluated in NUREG-1793, "Final Safety Evaluation Report (FSER) Related to the Certification of the AP1000 Standard Design," issued by the U.S. Nuclear Regulatory Commission (NRC) in September 2004. Additionally, AP1000 DCD Tier 1, Section 2.5, contains changes to the proposed design description and inspection, test, analysis, and acceptance criteria (ITAAC) for I&C systems. This FSER supplement must be used in concert with the original version of NUREG-1793 to completely understand the full evaluation of the AP1000 I&C Systems standard design. The sections identified and addressed below have had additions, alterations, or deletions incorporated into the technical information presented previously in the certified design of Revision 15 of the AP1000 DCD. The sections not listed below had no appreciable technical changes and thus are not included in this FSER supplement.

Although all open items (OIs) have been resolved prior to the final issuance this supplement of the safety evaluation report (SER), the SER discusses what OIs were generated when it considered an applicant's original submittal and response to be inadequate.

In the latest revision of the AP1000 DCD, Revision 17, Westinghouse Electric Company (Westinghouse) provided additional information related to the architecture of its safety-related I&C protection system, referred to as the protection and safety monitoring system (PMS); the diverse back-up system to the PMS, the diverse actuation system (DAS); and data communications protocols and methods utilized to ensure a secure development and operational environment (SDOE). Westinghouse also proposed minor modifications to some of the interlock and control systems.

7.1.3.1 Compliance with Standard Review Plan (SRP) Criteria

The NRC staff reviewed the additional and amended information provided by Westinghouse, using the guidance in Chapter 7, "Instrumentation and Control Systems," of NUREG-0800,

"Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: Light Water Reactor Edition" (hereafter referred to as the SRP), Revision 5. The NRC developed NUREG-1793 using the guidance of Revision 4 of the SRP, which did not contain Section 7.8, "Diverse Instrumentation and Control Systems," or Section 7.9, "Data Communication Systems." Therefore, although this supplement follows the format of NUREG-1793, the NRC added Section 7.8, "Diverse Instrumentation and Control Systems," and Section 7.9, "Data Communication Systems," to discuss the staff's review of these issues. Where necessary, the staff correlated the information in Sections 7.8 and 7.9 with other pre-existing Chapter 7 sections.

7.1.3.2 Compliance with Industry Standards

Westinghouse submitted a number of technical reports (TR) associated with I&C systems, which it incorporated by reference into the AP1000 DCD. Based upon the letter, "Secondary References in a Design Certification Rule," dated May 3, 1994 (ADAMS Accession Number ML003708073), the staff determined with the concurrence of utility representatives and other members of the commercial nuclear industry that documents referenced in Tier 1 and Tier 2 information within the AP1000 DCD should be considered part of the licensing basis. Therefore, the addition of these documents is deemed acceptable to the staff.

In several cases, Westinghouse referenced different revisions of the same industry standards and other regulations in its TRs from those referenced in DCD Revision 15. Westinghouse stated that all newly created or revised technical documents that do not refer to the guidance or standards certified in Revision 15 of the AP1000 DCD will reference currently issued guidance or standards provided the newly referenced guidance or standards include all acceptance criteria to those references certified in the Revision 15. The staff found the response acceptable.

7.1.3.3 Compliance with 10 CFR Part 52

Based upon the discussion in Section 7.1.3.3 of NUREG-1793, the standardized power plant designer or combined license (COL) applicant will satisfactorily demonstrate that "the digital I&C system design development process, as documented in the DCD, will ensure that the digital I&C system, as designed, will satisfactorily accomplish its safety functions."

All newly submitted documentation is to support and agree with all previously submitted design documents to enable the NRC to reach the same conclusion as in NUREG-1793.

The regulations in 10 CFR 52.63, "Finality of Standard Design Certifications," are applicable to modifications addressed in this chapter, which supplements NUREG-1793 to address Westinghouse's amendment request.

7.1.4 Tier 1 Material

Revision 17 of AP1000 DCD Tier 1, Section 2.5, contains information associated with the DAS and the PMS within the first two phases of the software, logic-based, or programmable technology design processes. The proposed alteration to the DAS design allows the use of technology other than microprocessor-based systems (i.e., firmware or analog technology) and the selection of the specific PMS design platform, the Common Q platform. Revision 17 of the DCD also proposes to remove part of the design acceptance criteria (DAC), which is a subset of

ITAAC, in Tier 1, Section 2.5. Sections 7.2 and 7.8 of this FSER supplement discuss these changes.

Westinghouse classifies the first two phases of the PMS and DAS lifecycles as the Design Requirements (or Conceptual) phase and System Definition phase, for both the PMS and the DAS in the certified design. Branch Technical Position (BTP) 7-14 Revision 5 as well as Branch Technical Position HICB-14, to which the AP1000 DCD was certified, within Chapter 7 of the SRP refers to these two phases of development as the "Planning Activities" phase and the "Requirements Activities" phase of the PMS software lifecycle (SLC) and the DAS programmable technology lifecycle respectively.

AP1000 DCD Tier 1, Section 2.5.1, identifies the ITAAC for the DAS, and Section 2.5.2 identifies the ITAAC for the PMS. Section 2.5.1, Design Description 4, and Table 2.5.1-4, entitled "Inspections, Tests, Analyses and Acceptance Criteria," discuss Design Commitment Number 4, which identifies the phases of the programmable technology development life cycle for the DAS. Likewise, Section 2.5.2, Design Description 11, and Table 2.5.2-8, also entitled "Inspections, Tests, Analyses and Acceptance Criteria," discuss Design Commitment Number 11, which identifies all phases of the software lifecycle (SLC) for the PMS. Based on the cover letter received with Revision 17 of the AP1000 DCD, Westinghouse considers both of these items DAC.

To address the DAC, Westinghouse provided design information related to the design requirements and system definition phases of the PMS SLC and the DAS programmable technology lifecycle. For both the DAS and PMS sections (Sections 2.5.1 and 2.5.2, respectively) of the Tier 1 document, Westinghouse proposed the removal of the first two phases of the SLC processes in Revision 17 of the AP1000 DCD. Sections 7.2.5 and 7.2.8 of this FSER supplement provide further discussion of this topic as it relates to the PMS, and Sections 7.8.2 and 7.8.3 discuss the lifecycle development process for the DAS.

7.1.5 Instrumentation and Control System Architecture

In support of Revision 17 of the AP1000 DCD, the staff reviewed the following TRs:

- APP-GW-GLR-071/WCAP-16675-P, "AP1000 Protection and Safety Monitoring System Architecture Technical Report," Revision 3 (TR-89). This report describes how the PMS will function. Section 7.2.2, "Protection and Safety Monitoring System Description," and are discussed in Section 7.9 of this FSER supplement.
- APP-GW-GLR-065/WCAP-16674-P, "AP1000 I&C Data Communication and Manual Control of Safety Systems and Components," Revision 2 (TR-88). This report provides critical design aspects of the communications methodology and various protocols when dealing with inter- and intra-division communications and safety-related to non-safety-related communications methods. The report also contains key information related to the manual operation of the AP1000 safety systems. Sections 7.2.2, 7.5.3, 7.9.3, and 7.9.4 of this FSER supplement discuss WCAP-16674-P in greater detail.
- APP-GW-GLN-022, "AP1000 Standard Combined License Technical Report DAS Platform Technology and Remote Indication Change," Revision 1 (TR-97), dated May 2007. This report provides information associated with the relocation of DAS equipment, and it also incorporates changes to allow a microprocessor-based or alternative technology to serve as the principal design of the DAS platform. Section 7.1.6 of this

FSER supplement, “Diversity and Defense in Depth Assessment of the AP1000 Protection System,” and Section 7.8, “Diverse Instrumentation and Control Systems,” provide additional discussion on APP-GW-GLN-022.

- APP-GW-GLR-017, “AP1000 Standard Combined License Technical Report,” Revision 0 (TR-42). This report summarizes Westinghouse’s proposed resolution of the 10 generic open items (GOIs) and 14 plant-specific action items (PSAIs) associated with the NRC review of the Westinghouse Common Q platform. Section 7.2.3 of this FSER supplement contains more information on this document.
- APP-GW-GLR-024/WCAP 16361-P, “AP1000 Setpoint Calculations for Protective Functions,” Revision 0 (TR-28). This report discusses the calculation of setpoints and setpoint methodology for the PMS. Section 7.2.7 of this FSER supplement addresses additional information on setpoint methodology in AP1000 I&C systems.
- APP-GW-GLR-018, “Failure Modes and Effects Analysis and Software Hazards Analysis for AP1000 Protection System,” Revision 0 (TR-43). This report summarizes the steps taken to perform the failure modes and effects analysis (FMEA) and software hazards analysis (SHA) and serves primarily as a pointer to the AP1000 FMEA and SHA reports.
- APP-GW-JJ-002/WCAP-16438-P, “FMEA of AP1000 Protection and Safety Monitoring System,” Revision 2. This report provides the postulated failure modes and effects the PMS will undergo as a result of the given failures.
- APP-PMS-GER-001/WCAP-16592-P, “Software Hazard Analysis of AP1000 Protection and Safety Monitoring System,” Revision 1. This report discusses the risks associated with the use of software or programmable technology in protection and control systems. The report will be discussed further in Section 7.2 of this FSER supplement.
- APP-GW-GLN-004, “Instrument and Control Design Change,” Revision 0 (TR-39), incorporates signal and other name changes to the post-accident monitoring system (PAMS), which interfaces with the qualified data processing system (QDPS).
- WCAP-17179, “AP1000 Component Interface Module Technical Report,” Revision 1. This report discusses the design of the Component Interface Module (CIM) within the PMS in greater detail than within the WCAP-16675-P, report. The report is discussed further in Sections 7.2 and 7.9 of this FSER supplement.
- WCAP-17184-P, “AP1000 Diverse Actuation System Planning and Functional Design Summary Technical Report,” Revision 1. The report defines the planning process and other design attributes of the DAS. The report will be discussed in greater detail in Section 7.8 of this FSER supplement.
- WCAP-17201-P, "AC160 High Speed Link Communication Compliance to DI&C-ISG-04 Staff Positions 9, 12, 13 and 15 Technical Report," Revision 0. This report discusses how the PMS will comply with certain acceptance criteria within Digital Instrumentation and Controls (DI&C) Interim Staff Guidance (ISG)-04. The TR will be further evaluated in Section 7.9 of this FSER supplement.
- WCAP-17226-P, “Self-Powered Detector Signals in the AP1000 In-Core Instrumentation System", Revision 1. This report discusses the interactions between the non-safety-related In-Core Instrumentation System (IIS) and the safety-related Core Exit Thermocouples (CETs). As the report covers the interaction of safety-related CETs and the IIS, this report will be covered in Section 7.5.7 of this FSER supplement.

- APP-GW-J0R-012, "AP1000 PMS Security Review," Revision 0. This report discusses how the PMS is constructed in an SDOE and will be discussed further in Section 7.9
- APP-GW-GLR-137, “Bases of Digital Overpower and Overtemperature Delta-T (OPΔT/OTΔT) Reactor Trips,” Revision 0. This report, also known as APP-GW-GLR-005, discusses the changes associated with how the PMS calculates its OPΔT and OTΔT signals. In addition to the content within Section 7.2, Appendix 7A of this FSER supplement provides additional information regarding this TR.

The staff reviewed WCAP-16592-P, “Software Hazards Analysis of AP1000 Protection and Safety Monitoring System,” Revision 1, and determined the information in the report adequately addresses the subject matter related to hazards or risks associated with the use of software or programmable technology in the PMS with one notable exception. Revision 1 of the report fails to discuss the potential hazards and/or risks associated with utilizing a firmware-based device, such as the CIM or safety remote node controller (SRNC) within the CIM subsystem of the PMS. While the CIM and SRNC will not use any software during their operation, the use of a programming language and other similar protocols during device development must be addressed and any hazards associated with the CIM and SRNC development process must be adequately mitigated or eliminated prior to their use within the PMS. Based upon the additional information required by the staff to make a determination of acceptability, Westinghouse submitted a response to RAI-SRPSHA-01, Revision 1, on June 28, 2010. The staff finds the commitments to update the SHA, including the removal of text stating that since the CIM and SRNC execute no software when operating, there is no need to cover their development or operation in the SHA, are acceptable. Additionally, in the response, Westinghouse commits to adding several potential hazards and mitigation strategies based upon the use of the CIM System in the PMS in Section 5 of the SHA. The NRC staff previously identified this issue as OI-SRP7.1-ICE-02 and, based upon the response to RAI-SRPSHA-01, Revision 1, it will now be captured as **CI-SRP7.1-ICE-01.**

Westinghouse replaced the remote shutdown workstation with the remote shutdown room (RSR). The staff finds that the change complies with all applicable acceptance criteria. Specifically, according to design drawings presented to the staff, the RSR transfer switch exists in a hallway located between the main control room (MCR) and the RSR. The staff asked Westinghouse to explain how it provides positive control of the reactor at all times, in accordance with Title 10 of the Code of Federal Regulations (10 CFR) 50.54(k). Westinghouse responded to Request for Additional Information (RAI) RAI-SRP7.1-ICE-13 by stating that control of the RSR switch would be primarily through administrative or procedural control. In a “normal” evacuation of the MCR, licensed operators would pre-staff the RSR before transferring reactor control. In an extreme life-threatening emergency, the licensed operators would be directed to manually scram the reactor before exiting the MCR, and, during the short journey to the RSR, move the transfer switch to RSR control and execute the necessary operator actions that follow a reactor scram. The staff finds this approach acceptable.

In response to RAI-SRP7.1-ICE-14, Westinghouse provided additional information regarding the overall makeup of its electrical distribution system. The staff reviewed the proposed grounding system for instrumentation and computer systems. Section 8.3.1.1.7 of the AP1000 DCD describes the four primary grounding systems for the AP1000. In particular, the instrument and computer systems use a separate radial grounding system. Based upon the information in the referenced section and the diagrams in Chapter 8 for the Class 1E instrumentation power distribution system, the staff finds the grounded, three-phase wye transformer configuration

acceptable for the I&C systems.

In Section 7.1.7, "References," of Revision 17 of the AP1000 DCD, Westinghouse deleted several references from the certified reference section without sufficient basis. As a result the NRC staff identified this as OI-SRP7.1-ICE-03. In its response to OI-SRP7.1-ICE-03, dated June 22, 2010, Westinghouse committed to update key reference documents within Chapter 7 of AP1000 DCD, Tier 2, as well as update Tier 2, Table 1.6-1. Additionally, Westinghouse commits to update its Tier 2* document list with WCAP-16361-P and WCAP-17179-P, and restore WCAP-15927, Revision 2, to the Tier 2* list as well. In addition, Westinghouse commits to remove all references to APP-GW-GLR-104, and other associated references to cyber security, as the staff's review under 10 CFR Part 50 does not encompass a cyber security review. Further information on cyber security is provided in Chapter 13 of the SER for the respective combined license (COL). Based upon the staff's review of Westinghouse's commitments in the OI-SRP7.1-ICE-03 response, the staff finds the changes are acceptable and captures the issue as **CI-SRP7.1-ICE-02**.

The staff could not identify several of the abbreviations Westinghouse used in some of its originally amended TRs. In RAI-SRP7.1-ICE-25, the staff asked Westinghouse to define all abbreviations in the text and diagrams in TR-89, and similar documents, as well as terms such as "hardwired," "bypass function," "partial trip mode," and "failsafe trip." The NRC discussed these issues with Westinghouse technical staff on January 29 - 30, 2009, at its Rockville, Maryland office. The staff received adequate responses to RAI-SRP7.1-ICE-24, RAI-SRP7.1-ICE-25, RAI-SRP7.2-ICE-02, RAI-SRP7.2-ICE-03, and RAI-SRP7.2-ICE-06; which Westinghouse has incorporated into the current revision of WCAP-16675-P and other affected TRs.

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

Section 7.8 of this FSER supplement discusses the safety evaluation of changes to the approved PRA-based diversity and defense-in-depth (D3) design.

7.2 Reactor Trip System

7.2.2 Protection and Safety Monitoring System Description

As described in Revision 17 of the AP1000 DCD, Westinghouse identified the Common Q platform as its safety-related protection system platform, negating the reference to WCAP-13383, "AP600 Instrumentation and Control Hardware and Software Design Verification and Validation Process Report," since that report primarily dealt with the use of the Eagle 21 platform, which will not be used in the AP1000 design. Specifically, in Section 7.1 of the AP1000 DCD Tier 2, Westinghouse removed references to the use of the Eagle 21 protection system hardware and committed to use the Common Q platform. This change was verified in Westinghouse's response to OI-SRP7.1-ICE-03, dated June 22, 2010, which the staff finds acceptable. As a result, removal of WCAP-13883 from the AP1000 DCD, Tier 2, Chapter 7, is acceptable.

In WCAP-16675-P, Revision 3 (Agencywide Documents Access and Management System (ADAMS) Accession Number ML100050345 and ML1000500343 for the publically available version), Westinghouse provided design information on the AP1000 PMS. Additionally, Westinghouse submitted WCAP-16674-P, Revision 2, (ADAMS Accession Number

ML100050344 and ML1000500342 for the publically available version) which addressed data communications and manual component control of safety-related systems, and WCAP-17179-P, Revision 1, which discussed a subsystem within the PMS responsible for allowing non-safety-related control of safety-related components during normal plant operation known as the CIM System. In the event of a PMS actuation, the PMS overrides non-safety-related control through the CIM and takes the safety-related components to their safe state. This task is accomplished through priority logic within the CIM. The CIM System resides within the Engineering Safety Features Actuation System (ESFAS) portion of the PMS. The CIM System's primary active components are the CIM and SRNC.

The staff reviewed the design and architecture of the PMS to assess how it meets regulatory requirements and addresses the acceptance criteria associated with an I&C safety system. The PMS encompasses the functions of the reactor trip system (RTS), ESFAS, PAMS, and QDPS. Section 7.5 of this FSER supplement contains additional information regarding the QDPS.

The discussion of the PMS in the following sections contains information presented in the publicly available, non-proprietary version of the following reports:

- APP-GW-GLR-137, Revision 0 (also known as APP-GW-GLR-005) – (ML092360182)
- WCAP-16674-NP, Revision 2 – (ADAMS Accession Number ML1000500342)
- WCAP-16675-NP, Revision 3 – (ADAMS Accession Number ML100050343)
- WCAP-17179-NP, Revision 1 – (ADAMS Accession Number ML100050187)
- WCAP-16438-NP, Revision 2 – (ADAMS Accession Number ML090790513)
- WCAP-16592-NP, Revision 1 – (ADAMS Accession Number ML093560889)

7.2.2.1 PMS Functional Requirements

The PMS performs the functions of the RTS, ESFAS, PAMS, and QDPS. During normal operation, administrative procedures and plant control systems maintain the reactor in a safe state, preventing damage to the three barriers (fuel clad, reactor coolant system, and reactor containment building) that prevent the spread of radioactive material to the environment. Accident conditions causing one or more of the barriers to be threatened could occur. Thus, the PMS monitors key plant parameters and automatically initiates various protective functions to prevent the violation of any of the three barriers. When violation of a barrier cannot be prevented, PMS will attempt to maintain the integrity of the remaining barriers. This ensures that, given a design-basis event, the site boundary radiation releases will be maintained below the limits in 10 CFR Part 100, "Reactor Site Criteria." The system functions by actuating a variety of equipment and by monitoring the plant process using a variety of sensors and operations that perform calculations, comparisons, and logic functions, based on those sensor inputs. The PMS functional requirements documents discuss the protective functions of the system and the requirements these functions place on the equipment that performs them.

7.2.2.1.1 Reactor Trip Functions

The PMS generates an automatic reactor trip for the following conditions:

- source range high neutron flux trip

- intermediate range high neutron flux trip
- power range high neutron flux trip (low setpoint)
- power range high neutron flux trip (high setpoint)
- power range high positive flux rate reactor trip
- overtemperature delta-T (OTΔT) reactor trip
- overpower delta-T (OPΔT) reactor trip
- reactor trip on low pressurizer pressure
- reactor trip on low reactor coolant flow
- reactor trip on reactor coolant pump underspeed
- reactor coolant pump bearing water temperature
- pressurizer high-pressure reactor trip
- pressurizer high-water-level reactor trip
- reactor trip on low-water level in any steam generator
- high-2 steam generator water level in any steam generator
- automatic depressurization systems actuation reactor trip
- core makeup tank actuation reactor trip
- reactor trip on safeguards actuation
- manual reactor trip

Revision 15 of the AP1000 DCD identified the reactor trip functions listed above. Westinghouse modified the design description of several reactor trip functions in Revisions 16 and 17 of the AP1000 DCD. Specifically, Westinghouse proposed the following modifications:

- The source range high neutron flux trip is delayed when the detector's high-voltage power supply is energized to prevent a spurious trip. The staff finds this acceptable, since the detector would be energized before being declared operable.
- The equations for performing the OTΔT and OPΔT reactor trips were modified. The staff determined, through an examination of TR, APP-GW-GLR-137, Revision 0, and associated RAIs and satisfactory Westinghouse responses, that the new equations were equivalent to the previous equations but in a different format. Therefore, the changes are acceptable. Appendix 7A provides a more detailed evaluation of APP-GW-GLR-137. However the commitments made by Westinghouse in both the APP-GW-GLR-137 report and the associated RAI responses dealing with: (1) the addition of the aforementioned report as a reference in Section 7.2.4, References, of the AP1000 DCD, (2) the updating of time constants used that require an update to Figure 7.2-1, and (3) the incorporation of all the RAI responses into a newly revised TR to address all changes based upon the questions raised during the review of the original report will be referred to as **CI-SRP7.2-ICE-01**. Additionally, for the references to Section 5.0 of TR APP-GW-GLR-137, Westinghouse committed to revise its WCAP-16361-P, "Westinghouse Setpoint Methodology for Protection Systems – AP1000," Revision 0, as a result of these

changes. The forthcoming revision of the WCAP-16361-P report will be addressed in Section 7.2.7 of this report.

- Reference to Permissive P-8 (power range nuclear power above setpoint) was removed, as Permissive P-10 made it redundant. The staff finds the change acceptable.
- Reactor Trip on High Reactor Coolant Pump Bearing Water Temperature. The trip has been modified to occur if any reactor coolant pump experiences a high bearing water temperature without the P-10 interlock being able to block the trip when reactor power is below the P-10 setpoint. As this modification is conservative in nature, in that the number of permissives needing to be satisfied before the trip occurs have been reduced, the change is deemed acceptable.
- Westinghouse removed the automatic rod withdrawal block, which prevents rod withdrawal if the negative flux rate setpoint is exceeded, in Revision 16 of the AP1000 DCD. As a result, based upon the removal of the associated text and table information in Chapter 7 of Revision 17 of the AP1000 DCD, the staff understands the previously discussed P-17 interlock to have been removed from use in the PMS. Since this control action utilized the non-safety-related rod control system for its actuation or, in the case of the block signal, the lack of actuation, the removal of the block action is beyond design basis as it pertains to this evaluation and is therefore acceptable.

The NRC determined that the other changes to the reactor trip functions, such as editorial changes or changes that added conservatism to the design, were minor; therefore, the chapter does not discuss them further.

7.2.2.1.2 Engineered Safety Features Actuation System Functions

The PMS performs both reactor trip and ESFAS functions. The AP1000 design provides I&C to sense accident situations and initiate engineered safety features (ESFs). The occurrence of a limiting fault, such as a loss-of-coolant accident or a secondary system break, requires a reactor trip plus actuation of one or more of the ESFs. This combination of events prevents or mitigates damage to the core and reactor coolant system components and provides containment integrity.

The PMS is actuated when safety system setpoints are reached for selected plant parameters. The selected combination of process parameter setpoint violations is indicative of primary or secondary system boundary challenges. Once the system receives the required logic combination, the PMS equipment sends the signals to actuate appropriate ESF components.

The PMS initiates the following ESF system-level actuations:

- safeguards actuation
- containment isolation
- in-containment refueling water storage tank injection
- core makeup tank injection
- automatic depressurization system
- reactor coolant pump trip
- main feedwater isolation

- passive residual heat removal actuation
- turbine trip
- containment recirculation
- steamline isolation
- steam generator blowdown system isolation
- passive containment cooling actuation
- startup feedwater isolation
- boron dilution block
- chemical and volume control system isolation
- steam dump control
- main control room isolation
- auxiliary spray and purification line isolation
- containment air filtration isolation
- refueling cavity isolation
- chemical and volume control system letdown isolation
- pressurizer heater block
- steam generator relief isolation
- normal residual heat removal containment isolation
- demineralized-water transfer and storage system isolation
- reactor vessel head vent valve control

Revision 15 of the AP1000 DCD identified the ESF system-level actuations listed above. Westinghouse incorporated several minor changes to Section 7.3 of the AP1000 DCD, and the staff finds the changes acceptable.

7.2.2.1.3 Component Control Functions

Westinghouse provides control of individual safety-related components that perform Class 1E functions. Component-level control consists of the following functions:

- resolution of multiple demands (priority logic) for a given component from various systems
- application of manual component demands
- performance of the component protection logic (e.g., torque limit, antipump latch)
- reporting of component status to the plant information system
- local component control

The following inputs are required for control of individual components:

- automatic system-level actuation commands from the reactor trip and ESF actuation logic
- manual system-level actuation commands from the fixed position switches in the MCR and RSR
- individual safety component control commands from the non-safety-related plant control system (PLS) for component actuations with no onerous consequences (for test, maintenance, restoration, and non-credited actuations)
- individual safety component control commands from the safety and QDPS displays in the MCR for component actuations with onerous consequences
- component feedback signals from the individual safety components to the PMS

The outputs to individual safety-related components consist of hardwired control signals to open or close a solenoid valve, motor-operated valve, or circuit breaker.

7.2.2.2 AP1000 Protection and Safety Monitoring System Operation

The PMS detects off-nominal conditions and actuates 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 MCR or RSR workstation. In addition, the PMS provides the equipment necessary in its QDPS sub-system to monitor the plant's safety-related functions during and following an accident, as identified in RG 1.97, "Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants," Revision 3.

The AP1000 PMS consists of four redundant divisions, designated A, B, C, and D. The PMS performs the necessary safety-related signal acquisition, calculations, setpoint comparison, coincidence logic, reactor trip and ESF actuation functions, and component control functions to achieve and maintain the plant in a safe shutdown condition. The PMS also contains maintenance and test functions to verify proper operation of the system. The PMS includes four redundant safety displays, one for each division and two QDPS displays, located on the primary dedicated safety panel (PDSP) in the MCR. Only two of the four divisions contain software to drive QDPS displays and to provide PAMS information to the operator, on Divisions B and C. The system's use of four redundant divisions is one of the mechanisms employed to satisfy single-failure criteria and improve system availability.

The I&C equipment performing reactor trip and ESF actuation functions, its related sensors, and the reactor trip switchgear are, for the most part, four-way redundant. This redundancy permits the use of bypass logic, so that a division or an individual channel within a division taken out of service can be accommodated by the operating portions of the protection system that revert to a two-out-of-three (2oo3) logic function from a two-out-of-four (2oo4) logic function. Additional discussion related to bypasses and the indication of inoperable channels within the PMS can be found in Section 7.5.6 of this report.

Four redundant measurements, using four separate sensors, are made for each variable used for reactor trip or ESF actuation within a single division. Each division, which is comprised of two redundant channels, processes one measurement. Analog signals are converted from remote sensor outputs to digital form by analog-to-digital converters within the division's bistable processor logic (BPL) modules - one per channel. Signal conditioning is applied to selected

inputs to the BPL, after the digital conversion. Following necessary calculations and processing, the measurements are compared against the applicable setpoint for that variable. A partial trip signal for a parameter is generated in the BPL if the channel's measurement exceeds its predetermined or calculated limit. Processing of variables for a reactor trip is identical in each of the four redundant divisions of the protection system.

Two local coincidence logic processors (LCL), within each division receive the output signal from each division's BPLs. The LCL subsystem acts to initiate a reactor trip or ESF actuation when a predetermined condition in 2oo4 independent safety divisions reaches a partial trip or partial actuation state. The LCL also provides for the bypass of trip or actuation functions to accommodate periodic tests and maintenance.

7.2.2.2.1 Reactor Trip Operation

The reactor trip coincidence logic performs the logic function to combine the partial trip signals from the BPL subsystems and generates a failsafe trip output signal to the reactor trip switchgear. The reactor trip signal from each of the four divisions of the PMS is sent to the division's reactor trip circuit breakers (RTCBs). Each division controls two RTCBs. The design of the RTCB placement ensures that the reactor trip would still occur, even in the presence of a failure of one of the division's two RTCBs. The reactor is tripped when two or more divisions actuate, thereby generating a reactor trip signal opening their breakers. The automatic trip demand signal initiates the following two actions: it deenergizes the undervoltage trip coils on the RTCBs, and it energizes the shunt trip devices on the RTCBs. Either action causes the breakers to trip. Opening the appropriate trip breakers by any two divisions removes power to the rod drive mechanism coils, allowing the rods to fall into the core. This rapid negative reactivity insertion causes the reactor to shut down. Section 7.2.2.3.7, "Capability for Test and Calibration," provides further information on testing RTCBs.

7.2.2.2.2 ESF Actuation

The ESF coincidence logic processors perform the logic function to combine the partial actuation signals from the BPL subsystems, along with automatic and manual permissives, blocks, and resets, to generate a fault tolerant actuation output signal to the integrated logic processor (ILP) subsystems.

The primary functions of the ESF logic processors are to process inputs, calculate system-level actuation, combine the automatic actuation with the manual actuation and manual bypass data, and transmit the data to the ILPs. To perform the ESF coincidence logic calculations, the ESF processors require data from the BPL subsystems and also use manual inputs (such as setpoints and system-level blocks and resets) from the MCR and the RSR workstation.

The ESF logic processors perform the following functions:

- Receive bistable data supplied by the four divisions of BPL subsystems and perform 2oo4 voting on this data.
- Implement system-level logic and transmit the output to the ILP processors for ESF component fan-out and actuation.

- Process manual system-level actuation commands received from the MCR and/or RSR.

The ESF component control function uses redundant ILPs, which serve as LCL output control signal "fan-out" devices, that distribute the activate signal to the various SRNCs that forward their given output to their respective CIMs. The CIMs provide a distributed interface between the safety system and plant equipment for control of non-modulating safety-related plant components. The safety-related input to the CIM comes from both of its respective SRNCs within the PMS, while the non-safety-related input enters the CIM through the non-safety-related remote node controller (RNC). Non-modulating control relates to the opening or closing of solenoid valves and solenoid pilot valves and the opening or closing of motor-operated valves and dampers. It also provides the plant operator with information on the equipment status, such as an indication of component position (full closed, full open, valve moving), component control modes (manual, automatic, local, remote), or abnormal operating conditions (power not available, failure detected).

The staff approved the Common Q platform portion of the AP1000 PMS, previously based on information contained in the Common Q topical report (ADAMS Accession Number ML031830959). The safety evaluations of the topical report appear in Westinghouse documents with ADAMS Accession Numbers ML003740165, ML011690170, and ML030550776. However, regarding the use of the ESFAS functions, the PMS design uses distribution devices known as ILPs, SRNCs, and CIMs, which had not been previously evaluated in the Common Q platform. Westinghouse provided design information detailing the functions of each of the aforementioned components. Sections 7.2.2.3.13 through 7.2.2.3.15 contain the technical discussion regarding the additional information the NRC staff reviewed for each of these components before determining their acceptability. The ILP is an intra-divisional device that receives its input from the LCL and distributes its outputs to a given SRNCs that forward their outputs to their assigned CIM. Besides distributing the activate signals to non-modulating safety-related devices, the CIM serves as an interface control device, as it receives inputs from both the safety-related PMS and the non-safety-related PLS to actuate the requested vital components of the safety-related ESFAS.

7.2.2.3 PMS Technical Evaluation

The staff evaluated the technical requirements of the PMS design against the requirements and acceptance criteria in the following documents:

- 10 CFR 50.49, "Environmental Qualification of Electric Equipment Important to Safety for Nuclear Power Plants"
- 10 CFR 50.55a(h), which incorporates by reference IEEE Standard (Std.) 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations" (NOTE: The clauses of IEEE Std. 603-1991 not referenced in the topical-based discussion below are unaffected by the proposed changes described in Revision 17 of the AP1000 DCD).
- 10 CFR Part 50, "Domestic Licensing of Production and Utilization Facilities," Appendix A, "General Design Criteria [GDC] for Nuclear Power Plants"
  - GDC 13, "Instrumentation and Control"
  - 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 29, “Protection Against Anticipated Operational Occurrences”

The industry and staff guidance in Chapter 7 of the SRP applies to the PMS review.

The staff evaluated the PMS architecture against those requirements affected by the additional or modified design information provided on the PMS. Those requirements include single-failure protection, quality, equipment qualification, system integrity, independence, capability for test and calibration, information displays, control of access, repair, automatic and manual control, and bypasses. Section 7.2.7 discusses setpoints. The staff determined that other requirements for I&C systems were not affected by changes in Revision 17 of the AP1000 DCD, compared to those approved in Revision 15. Specifically, Westinghouse uses the Common Q platform as a major portion of the PMS. This supplement evaluated major subcomponents of the PMS, including those that were not previously developed at the time of the staff’s original safety evaluation report for the AP1000 such as the ILP, SRNC, and CIM. Sections 7.2.2.3.13 through 7.2.2.3.15 discuss those evaluations.

7.2.2.3.1 Common Q Technical Evaluation

The staff previously approved the use of the Common Q platform for generic nuclear power plant applications. Section 7.2.2.2.2 of this report contains reference material related to the Common Q topical report and the associated safety evaluations. Westinghouse presented additional planning and design information related to the use of the Common Q platform in the AP1000 design in the form of the newly submitted TRs related to the PMS that were discussed in Section 7.1.5.

7.2.2.3.2 Single-Failure Protection

The staff evaluated the single-failure protection characteristics of the Common Q and PMS against requirements in IEEE Std. 603-1991, Clause 5.1, “Single Failure Criterion,” and GDC 21. The staff used the guidance in RG 1.53, “Application of the Single-Failure Criterion to Nuclear Power Plant Protection Systems,” which endorses IEEE Std. 379-1988, “Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems.”

To address the guidance in RG 1.53, Westinghouse presented the NRC with an FMEA and an SHA to demonstrate the system’s capability to withstand a single-failure event. WCAP-16438-P, Revision 2 (ADAMS Accession Number ML090790514 and ML090790513 for the publically available version), describes the FMEA, and WCAP-16592-P (APP-PMS-GER-001), “Software Hazards Analysis of AP1000 Protection and Safety Monitoring System,” Revision 1 (ADAMS Accession Number ML093560891 and ML093560889 for the publicly available report), describes the SHA for the PMS. The staff’s evaluation of the PMS SHA is described in Section 7.1.5, “Instrumentation and Control System Architecture.”

The staff examined the AP1000 FMEA against the guidance of IEEE Std. 352-1998, “IEEE Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Safety Systems,” and IEEE Std. 379-1988. The staff finds the report provides a satisfactory

demonstration of the system's fault tolerance under various scenarios. Several technical questions were identified regarding specific system responses in the presence of certain failure types and required resolution as shown in the following examples:

- Five CIMs possess a mean time between failure (MTBF) that did not meet the design reliability targets for the PMS. However, the text gave no explanation or analysis as to how the system will minimize, mitigate, or eliminate these failure types. To address this issue, Westinghouse issued a response to RAI-SRP7.1-FMEA-01 in December of 2009, stating that an MTBF Analysis would be conducted and was expected to be completed by July 2010. The response further discusses how, once the MTBF Analysis report is completed, if the failure rates were not in line with the expected failure rate of at least 200,000 hours, the Westinghouse design change process would be utilized to modify the equipment to reach the MTBF goal or adequately explain why the higher rate of failure is acceptable. The staff finds the use of an MTBF Analysis to verify a sufficiently low level of failures of the CIM and SRNC to be acceptable.
- According to the FMEA, when the check sum verification process fails, the setpoints are not updated, however this condition would be restricted to one division only. The FMEA then discusses how the division may trip erroneously or not trip due to the setpoints not being properly updated. In a response dated December 1, 2009, Westinghouse stated, in part, that the cyclic redundancy check (CRC) verification mechanism can fail and the correct setpoint value still be monitored by the MTP. Although the MTP may not receive the updates due to a failure of the CRC, there are continuous lower level diagnostics that provide alarm and indication informing the operators that a fault has occurred between the LCL and the MTP. Additionally, even though the diagnostics and self-tests that are executing continuously are not credited, the fault would be limited to a single division's MTP and is therefore acceptable.
- The FMEA describes how the PMS, through the maintenance and test panel (MTP), periodically adjusts setpoints automatically. This automatic adjustment of setpoints, without operator control, would not meet the requirements in Criterion III, "Design Control," in 10 CFR Part 50, Appendix B. In a response dated November 9, 2009, Westinghouse related the "periodic refreshing" of data was part of the inherent communications in a deterministic format utilized between the AC160 and the MTP. The response stated further that the setpoints within the AC160 can only be altered manually by the operator of the MTP. According to the reply, Westinghouse will update Revision 3 of the FMEA to more clearly state that the system is not continually sending "new" updated setpoints to the AC160, but simply performing its communication function. The staff finds this response acceptable, and confirmatory item **(CI)-SRP7.2-ICE-02** will verify the commitment in the next revision of the FMEA.

When comparing the requirements in Clause 5.1 of IEEE Std. 603-1991 and GDC 21 to the information in WCAP-16675-P and WCAP-16438-P, and after reviewing the responses provided by Westinghouse related to the FMEA, the staff determined the single failure requirements related to IEEE Std. 603 1991 have been adequately addressed. The NRC staff previously identified these issues as OI-SRP7.2-ICE-01 and as a result of the staff's review of the responses provided by Westinghouse and its commitment to update the next revision of the FMEA based upon their responses to RAI-SRP7.1-FMEA-02, RAI-SRP7.1-FMEA-04, RAI-SRP7.1-FMEA-05 and RAI-SRP7.1-FMEA-07 the staff finds the design satisfies the single failure criterion. **CI-SRP7.2-ICE-02** will verify the commitment in the next revision of the FMEA.

7.2.2.3.3 Quality

Clause 5.3 of IEEE Std. 603-1991 and 10 CFR Part 50, Appendix B, "Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants," require safety-related I&C systems to be designed, manufactured, inspected, installed, and tested under an acceptable quality assurance program. SRP Appendix 7.1-D, "Guidance for Evaluation of the Application of IEEE Std. 7-4.3.2"; Section 5.3; and BTP 7-14 specifically address the criteria for a quality software development process. Additionally, the staff evaluated the documentation in the SLC for the Common Q portion of the PMS against the guidance in the following documents:

- Regulatory Guide 1.168, "Verification, Validation, Reviews and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," which endorses IEEE Std. 1012-1998, "IEEE Standard for Software Verification and Validation," and IEEE Std. 1028-1997, "IEEE Standard for Software Reviews and Audits"
- Regulatory Guide 1.169 "Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," which endorses IEEE Std. 828-1990, "IEEE Standard for Software Configuration Management Plans"
- Regulatory Guide 1.170, "Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," which endorses IEEE Std. 829-1983, "IEEE Standard For Software Test Documentation"
- Regulatory Guide 1.171, "Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," which endorses IEEE Std. 1008-1987, "IEEE Standard for Software Unit Testing"
- Regulatory Guide 1.172, "Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," which endorses IEEE Std. 830-1993, "IEEE Recommended Practice for Software Requirements Specifications"
- Regulatory Guide 1.173, "Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," which endorses IEEE Std. 1074-1995, "IEEE Standard for Developing Software Lifecycles and Processes"

In Section 7.2.2.2, the staff discusses the approval of the Common Q platform topical report. However, additional requirements were placed on the SLC for the AP1000 safety system, beyond those described in the Software Program Manual (SPM), WCAP-16096-NP-A, "Software Program Manual for Common Q Systems," Revision 1A, dated January 21, 2005 (ADAMS Accession Number ML050350234). WCAP-15927, "Design Process for AP1000 Common Q Safety Systems," Revision 0, placed additional requirements on the design and testing teams developing the PMS. The certified design (Revision 15) of the AP1000 DCD designated the SPM and WCAP-15927 as Tier 2* documents, requiring NRC approval before altering Westinghouse commitments. The staff recently received, reviewed, and approved the use of WCAP-15927, Revision 2 (ADAMS Accession Number ML091890752). Section 7.2.5 provides further information concerning this matter.

In AP1000 DCD Tier 1, Table 2.5.2-8, Design Description 11, Westinghouse proposed the removal of design requirements and system definition phases of the PMS SLC ITAAC. The design requirements phase corresponds to the planning activities phase of the SLC in SRP

BTP 7-14, and the system definition phase corresponds to the requirements activities phase in the same SRP BTP. Westinghouse made available for audit the software planning documents to support removal of the design requirements phase. The staff audited those software planning documents on several occasions, which are discussed below. Westinghouse describes its quality software development process for the AP1000 project in the Common Q SPM and WCAP-15927, Revision 2, documents. The staff reviewed the proprietary and nonproprietary documentation associated with the first two phases of the SLC as it relates to Common Q portion of PMS system development. Further information regarding lifecycle development and completion as it relates to the PMS is provided in Section 7.2.5.

Westinghouse originally provided 11 documents that comprise the design requirements phase of the AP1000 SLC. On April 9 - 11, 2008; October 9 - 16, 2008; January 22 - 30, 2009; and July 30, 2009, the staff conducted site visits at the Westinghouse Twinbrook location in Rockville, Maryland, to review the proprietary documents associated with the design requirements phase. In RAI-SRP7.1-ICE-03, the NRC asked Westinghouse to explain in the Tier 2 information of the DCD how it meets the requirements of the planning ITAAC. This includes a diagram of the planning process and sufficient planning documentation related to the lifecycle development plan for the Common Q and CIM System within the PMS, and the steps taken by Westinghouse to ensure the PMS is constructed in a SDOE and other project-specific documents. The lack of an adequately detailed CIM System programmable technology lifecycle was captured under OI-SRP7.2-ICE-05 and the discussion of how Westinghouse intends to ensure the PMS is constructed in a SDOE will be covered in Section 7.9. The issue of which documents delineate the design requirements or planning activities phases of the PMS developmental lifecycle and their relationship to one another was reconciled in Section 7.2.5 prior to the staff's acceptance of the design requirements phase of the PMS lifecycle development process as complete. As a result, the issue previously identified as OI-SRP7.2-ICE-02 is considered complete based upon the commitments made in the revised Westinghouse response to OI-SRP7.2-ICE-02 to include an adequately detailed discussion of the design requirements in Chapter 7 of the DCD. This confirmatory item (CI) is captured as **CI-SRP7.2-ICE-03**.

Several proprietary documents listed as proof of completion of the design requirements phase detail the relationship between two Westinghouse organizations: Repair, Replacement, and Automation Services (RRAS) and Nuclear Power Plants (NPP) (e.g., RRAS AP1000 NuStart I&C Program Project Plan (WNA-PN-00031-GEN[1]) and RRAS AP1000 NuStart I&C Program Project Quality Plan (WNA-PQ-00166-GEN[2])). The documents reveal how the subcontractor (Westinghouse RRAS) interfaces with the parent organization (Westinghouse NPP); however, they originally did not describe how Westinghouse NPP interfaces with, and holds accountable, Westinghouse RRAS, employees, and other subcontractors. The NRC requested this information in RAI-SRP7.1-ICE-04. Westinghouse provided a written RAI response stating that its RRAS organization will complete all work on safety systems (i.e., all work performed on the I&C safety systems for the AP1000 will be conducted by either RRAS or its subcontractors, who will be required to function under Revision 5 of the Westinghouse Quality Management System (QMS) Manual). The NRC accepted Westinghouse's use of Revision 5 of the QMS Manual to satisfy the requirements in Appendix B to 10 CFR Part 50. This satisfies RAI-SRP7.1-ICE-04. However, the NRC staff identified the incorporation of this information into Revision 18 of the DCD as **CI-SRP7.2-ICE-04**.

---

1 Westinghouse altered the numbering format for this document. It is now numbered WNA-PN-00043-WAPP.

2 Westinghouse altered the numbering format for this document. It is now numbered WNA-PQ-00201-WAPP.

In July 2009, the staff conducted an audit of the recently developed proprietary PMS Test Plan, the SRNC and CIM Project Plan, and the CIM System Test Plan documents to ensure compliance with requirements and Westinghouse commitments. Overall, the NRC finds the results of the audit to be acceptable. Originally requested under RAI-SRP7.1-ICE-05, the documents listed above satisfy the need for sufficient test plan information related to the planning phase of the Common Q SLC; therefore, the NRC staff considers RAI-SRP7.1-ICE-05 closed.

Concerning the proprietary AP1000 NuStart Protection and Safety Monitoring System Software Project Plan (WNA-PJ-00071-GEN), the staff raised issues that included how Westinghouse could give a value of zero to the overall risk for software development when the risk in some specific areas was rated as high. Furthermore, Appendix A of the same report states that "Test/System Integration Phase Independent Verification and Validation [IV&V] is not within the scope of the AP1000 NuStart Project." The staff requested additional information in this area in RAI-SRP7.1-ICE-08, which discussed the revision to the table. At a meeting in January 2009, Westinghouse committed to revise notes within the Software Project Plan[3] document, WNA-PJ-00071-GEN, to inform the reader that "zero," in the case of risk, actually means minimal, not "no risk." During the staff visit to the Twinbrook facility on July 30, 2009, the staff confirmed that Westinghouse had incorporated this item into the proprietary software document. Therefore, this item adequately addresses the RAI, which is now considered closed.

The staff reviewed the proprietary document, WNA-PJ-00071-GEN, "AP1000 NuStart PMS Software Project Plan," and its descendent document, the AP1000/NuStart/DOE Design Finalization and Safety Monitoring System Software Development Plan,WNA-PN-00042-WAPP, as part of the design requirements phase review. Appendix A, Item 4, of WNA-PJ-00071-GEN states that the test/system integration phase IV&V is not within the scope of the AP1000 NuStart project. The software project will be frozen at the processor module software test for Division B software. The staff asked the applicant to clarify these statements; specifically, how Westinghouse would test Divisions A, C, and D software and the complete software of each division, beyond the processor module software tests. In a letter dated September 3, 2008, "AP1000 Response to Request for Additional Information (SRP7)" (ADAMS Accession Number ML082520229), the applicant clarified the statements in WNA-PJ-00071-GEN regarding processor module software testing. The letter stated the following:

> The deliverable for the cited plan is a detailed design up to and including the software design. This includes a software demonstration system using a test bed configured for Division B. It was not intended to validate all software for all divisions. The demonstration software for Division B marks the conclusion of the plan's scope.
>
> Once the demonstration software for Division B is complete, a software development plan will be developed to complete the software development life cycle taking credit for work completed in first plan. This would include activities for unit testing, code review, channel integration test for all four divisions, and system integration test, as well as the life cycle V&V activities.
>
> The completed Division B software is a sufficient sample to close the DAC software open issue and the V&V issue, because the completed development of Division B

[3] Westinghouse altered the numbering format for this document. It is now numbered WNA-PD-00042-WAPP. Westinghouse also retitled it, "AP1000 NuStart/DOE Design Finalization Protection and Safety Monitoring System Software Development Plan."

software will demonstrate all of the representative software subroutines included in all of the divisions (i.e., the RPS, ESFAS and QDPS functions).

The staff understands Westinghouse's explanation that the portion of module testing to be combined and constructed into a test bed mimicking Division B of the PMS in its entirety will serve as a "proof of concept" test for PMS and QDPS software and hardware, rather than an interdivisional integration test of the PMS and QDPS, to which Westinghouse is committed, later in the SLC process. The NRC staff accepts this approach and closes RAI-SRP7.1-ICE-09.

Section 7.2.5, "PMS Design Process Review," contains a detailed discussion of the level of quality Westinghouse requires to implement its SLC and programmable technology lifecycle for both the Common Q and CIM Subsystem portions of the PMS, and provides the staff's findings as they relate to overall PMS quality.

7.2.2.3.4 Equipment Qualification

Clause 5.4, "Equipment Qualification," of IEEE Std. 603-1991 states, in part, that 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 reviewed docketed and Westinghouse proprietary documents relating to the overall methodology and approach when dealing with equipment qualification. The Common Q topical report describes the generic equipment qualification of the Common Q equipment. Additionally, AP1000 DCD Tier 1, Table 2.5.2-8, Items 2, 3, and 4, identify ITAAC to address the seismic, electromagnetic/ radio-frequency/electrostatic discharge, and temperature/humidity qualification of PMS equipment. To complete the ITAAC, a licensee incorporating the AP1000 certified design would need to verify that the generic equipment qualification for the Common Q as well as the CIM system portion of the PMS equipment includes the site-specific seismic, electromagnetic/radio-frequency/electrostatic discharge, and temperature/humidity profile. Based on the generic equipment qualification of the Common Q equipment and the ITAAC in Tier 1 of the AP1000 DCD, the staff finds the equipment qualification acceptable for the proposed design certification amendment as it relates to the PMS.

7.2.2.3.5 System Integrity

Clause 5.5 of IEEE Std. 603-1991 states, in part, that safety systems shall be designed to accomplish their safety functions under the full range of applicable conditions enumerated in the design basis. The staff used the guidance in Appendix 7.1-C and Appendix 7.1-D of the SRP to review the PMS and its means of meeting the standard in Clause 5.5.

A special concern with any safety-related digital system is confirmation of its ability, in real time, to ensure completion of the protective actions within critical points of time identified in the design basis. Section 7.9 of this FSER supplement discusses real-time performance with respect to data communications. Items 6a, 6b, and 6c of AP1000 DCD Tier 1, Table 2.5.2-8, would, through their ITAAC, address the overall verification of the system response time. With regard to failure modes, the staff confirmed that the PMS design is such that reactor trip functions fail to the tripped state and ESF functions fail to the as-is state. Additionally, the Common Q

equipment contains self-diagnostics to alarm failed conditions and place the system into a fail-safe state. However, Westinghouse does not propose to use self-diagnostic tests for technical specifications surveillance tests. Based on the ITAAC, FMEA, and self-testing features, the staff finds the PMS design acceptable from a system integrity standpoint.

7.2.2.3.6 Independence

Clause 5.6, "Independence," of IEEE Std. 603-1991 and GDC 22 and 24 require, in part, that safety I&C systems be designed with physical, electrical, functional and communications independence among redundant divisions and between safety and non-safety systems. The staff compared the independence requirements of the Common Q system to the guidance contained in SRP Appendix 7.1-C and Appendix 7.1-D. Additionally, the staff compared the independence requirements of the PMS as they relate to ensuring the protection system was developed in a SDOE. The evaluation of the system being constructed and operated in a SDOE is discussed in Section 7.9.

Based upon information provided in the Common Q topical report and its appendices, the NRC approved the Common Q platform, which includes the BPLs, the LCLs, the interface and test processor (ITP), and the MTP. While the physical and electrical independence aspects of the Common Q have been demonstrated, several issues remained. One issue concerns the inter and intra-divisional data communications independence requirements of the Common Q platform. Section 7.9 discusses this issue.

As previously stated, within the layout of the PMS, yet external to the previously approved Common Q platform, the NRC evaluated the RNC, the SRNC, and the CIM against the independence requirements for physical separation and electrical, functional and communications independence (covered in Section 7.9) in Clause 5.6 of IEEE Std. 603-1991. GDC 13, 20, 21, 22, 23, and 24 contain other requirements affecting CIM independence.

IEEE Std. 603-1991, which the NRC endorsed in 10 CFR 50.55a(h), defines "associated circuits" as non-Class 1E circuits that are not physically separated or are not electrically isolated by acceptable separation distance, safety class structures, barriers, or isolation devices.

IEEE Std. 384-1981, "IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits," defines the acceptance criteria for the associated circuits. The RNC, which serves as an interface between the non-safety-related PLS Ovation® platform and the safety-related CIM, serve as part of the communications isolation function, according to Section 5.5.2 of WCAP-16674-P, "Non-Safety Manual Component-Level Control of Safety Components (Case E)," Revision 2 (ADAMS Accession Number ML1000500344) (Use ADAMS Accession Number ML1000500342 for the publically available, nonproprietary version). This information also appears in Section 3.3.5 of WCAP-16675-P, "AP1000 Protection and Safety Monitoring System Architecture Technical Report," Revision 3 (ADAMS Accession Number ML100050345, ML100050343 for the publicly available, nonproprietary version).

According to the description in the TRs, electrical and physical isolation between the RNC and the safety-related CIM is achieved by the use of fiber-optic cabling between the RNC and the remote input/output (I/O) bus, which connects to the PLS side of the RNC. Westinghouse commits to ensuring that the RNC will undergo qualification testing that meets or exceeds the guidance in IEEE Std. 384-1981. Thus, the device will undergo the qualification requirements placed on Class 1E circuits to ensure that the Class 1E circuits are not degraded below an

acceptable level, even in the presence of a failure of the associated circuit. The NRC acknowledges that the RNC will be qualified as an associated circuit, since the fiber-optic cable providing electrical isolation is between the non-safety-related PLS and the RNC.

The staff understands the subcomponent performing communications conversion is located physically on the CIM and that it creates the functional isolation between the RNC and CIM by performing the communications protocol or language conversion from the Emerson Ovation® programming language to discrete digital signals that will be provided to the priority logic, also located on the CIM. This type of arrangement also creates the functional isolation required to satisfy NRC requirements by ensuring that a failure, degradation, or corruption of the information being received by the CIM will not disable the ability of the PMS to execute or complete its function through the priority module, in accordance with IEEE Std. 603-1991, Clauses 5.2 and 5.6.1. Specifically, the priority logic of the CIM provides the PMS priority over the non-safety-related control system if a safety-related plant component needs to actuate to its safe state in all cases. This issue was addressed adequately in Westinghouse's response to RAI-SRP7.0-ICE-03 providing additional information regarding how the PMS has priority over the PLS, even when failure conditions are present. Its incorporation into WCAP-17179-P, Revision 2 will be captured under **CI-SRP7.2-ICE-05.**

Section 7.9 contains the staff's full evaluation, covering non-safety-related-to-safety-related data communications of the PMS, via the RNC and CIM, and other I&C systems.

7.2.2.3.7 Capability for Test and Calibration

The staff evaluated the Common Q system against the requirements of IEEE Std. 603-1991, Clause 5.7, "Capability for Test and Calibration," and the guidance contained in the following documents:

- SRP, BTP 7-17, "Guidance on Self-Test and Surveillance Test Provisions"
- SRP Appendix 7.1-D, "Guidance for Evaluation of the Application of IEEE Std. 7-4.3.2"
- Regulatory Guide 1.22, "Periodic Testing of Protection System Actuation Functions," issued 1972
- Regulatory Guide 1.118, "Periodic Testing of Electric Power and Protection Systems," issued 1995, which endorses IEEE Std. 338-1987, "IEEE Standard Criteria for the Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems"

The staff finds that Westinghouse meets the physical requirements that describe how testing and calibration will be performed administratively, through appropriate procedural guidance for both operational and maintenance personnel, as well as by the design of the Common Q platform and CIM subsystem which provide various interlocks within the Common Q portion and CIM subsystem within the PMS. Based upon a review of all information within the DCD and referenced TRs, Westinghouse does not credit any self-testing features with the PMS as replacements for periodic technical specification surveillance tests. The staff finds Westinghouse's approach acceptable. The staff will continue to validate this finding through the ITAAC process in later development stages (implementation, integration, and factory acceptance testing) of the developmental lifecycles for the Common Q platform and CIM subsystem within the PMS as a whole to ensure the actual system meets the requirements described in the planning activities and requirements activities developmental stages.

Westinghouse stated that each individual RTCB would be opened during a trip actuation device operational test once per year. In current licensed plants, the maximum length of time between openings of RTCBs (or equivalent) is typically 92 days. This issue is discussed in Chapter 16 of NUREG-1793 and this supplement. This issue was determined to be adequately addressed in Revision 15 of the DCD and no changes were made to RTCB layout or design, including the periodicity of RTCB testing. Therefore, OI-SRP7.2-ICE-03 is considered resolved.

7.2.2.3.8 Information Displays

Clause 5.8 of IEEE Std. 603-1991 requires information displays for manually controlled actions, safety-system status, and indication of bypasses. Additionally, the information displays should be accessible to operators. The staff used the guidance in RG 1.47, "Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems," issued 1973, during the review.

The information displays used by the PMS remain unchanged since they were found to be acceptable in the "Closeout of Category 1 Open Items for the Common Q Systems" (ADAMS Accession Number ML011690170), with the caveat that the flat panel display systems (FPDS) be qualified. Specifically, the NRC safety evaluation report (SER), "Safety Evaluation for the Closeout of Several of the Common Qualified Platform Category 1 Open Items Related to Reports CENPD-396-P, Revision 1, and CE-CES-195, Revision 1 (TAC Number MB0780), dated June 22, 2001, contains the following statement:

> PSAI 6.3 has been resolved generically and may be closed as a requirement in the SE. In connection with its resolution, the staff also found that the FPDS, subject to its successful performance during scheduled qualification testing, to be acceptable for use in Common Q designs as a Class 1E HMI device.

Therefore, a licensee incorporating by reference the AP1000 certified design would need to specifically address the equipment qualification of the FPDS when closing out ITAAC identified in AP1000 DCD Tier 1, Table 2.5.2-8, Design Commitments 2, 3, and 4. The staff finds the AP1000 information display design acceptable as it relates to Clause 5.8 of IEEE Std. 603-1991. Section 7.5 of this FSER supplement contains further discussion of information displays important to safety. Chapter 18, "Humans Factors Engineering," evaluates the adequacy of display information presented to operators.

7.2.2.3.9 Control of Access

Clause 5.9, "Control of Access," of IEEE 603-1991 requires control of access to the PMS. The staff judged the physical capability of the PMS to provide for access control to be acceptable with regard to its system design and administrative controls prior to the removal of the Planning Activities and Requirements Activities ITAAC. Section 7.9 of this FSER supplement contains the evaluation of the ability of the Common Q platform and CIM subsystem within the PMS to meet these requirements to ensure that the PMS is planned and constructed within a SDOE and a protected data communications standpoint. Additionally, Section 7.2.7 discusses the access controls to restrict the alteration of setpoints.

7.2.2.3.10 Repair

The staff compared the information Westinghouse presented in WCAP-16675-P regarding the

capability of the PMS to undergo repair activities both online and offline to meet the requirements of IEEE Std. 603-1991; Clause 5.10, “Repair”; and adequately address the guidance contained in BTP 7-17. The staff finds that, although online self-diagnostics may aid the operator, maintenance, or engineering team to diagnose a fault condition, they do not replace the need for surveillance testing as discussed in Section 7.2.2.3.7.

7.2.2.3.11 Automatic and Manual Control

Clauses 6.1 and 7.1 of IEEE Std. 603-1991 require provisions for automatic control of safety functions. Specifically, Clause 6.1 requires, in part, that means be provided to automatically initiate and control all protective actions except as justified in Clause 4.5. The safety-system design shall be such that the operator is not required to take any action before the time and plant conditions specified in Clause 4.5. Clause 7.1 requires the execute features to receive and act upon automatic controls.

Sections 1.1 and 1.2 of WCAP-16675-P identify the automatic reactor trip and ESF actuations. Westinghouse did not identify any manual controls for reactor trip or ESF actuations for the PMS in place of automatic controls. Additionally, the reactor trip breakers and ESF equipment are designed to accept and act upon automatic commands from the PMS. Therefore, the staff finds that the PMS design meets Clauses 6.1 and 7.1 of IEEE Std. 603-1991.

Clauses 6.2 and 7.2 of IEEE Std. 603-1991 require provisions for manual actuation of safety functions. Specifically, Clause 6.2 requires, in part, system-level manual actuation of safety functions that minimize the number of discrete operator manipulations and depend on the operation of a minimum amount of equipment, consistent with the constraints of Clause 5.6.1, “Independence Between Redundant Portions of the Safety System.” Position C.4 of RG1.62, “Manual Initiation of Protective Actions,” issued October 1973, states that equipment common to both the automatic and manual initiation should be kept to a minimum. The action-sequencing logic may be common, as long as component-level control of safety equipment is provided in the control room. Figure 2-2 of WCAP-16675-P identifies the voting logic, as well as the action-sequencing logic, common to the automatic and manual ESF initiation paths. The staff finds that, while this departs from the guidance in RG1.62, the design is acceptable for the following reason. In the event there is a failure that would disable common portions of the automatic and manual initiation paths in all divisions, a DAS is provided that is not common to the safety-related PMS. The point at which the system-level manual actuation is brought into PMS architecture minimizes the use of equipment and therefore reduces the complexity associated with implementing the system-level manual actuation. From a single-failure standpoint, both the automatic and manual initiation paths are designed for single-failure protection. For the RTS-level manual actuation, the switches in the MCR are hardwired to the reactor trip breakers. The staff finds the system-level manual actuation of the reactor trip and ESF to be acceptable.

Section 3.4.2 of WCAP-16675-P describes manual component-level control. The proposed design provides safety-related component-level control of components having onerous consequences, using the soft controls on the safety displays in the MCR and from the CIMs in the equipment rooms. Onerous consequences are defined as those that cause a breach of the reactor coolant system pressure boundary or cause a need to shut down the plant to cold conditions to effect repairs. Component-level control of equipment not having onerous consequences is provided through the non-safety-related workstations in the MCR or the RSR in the event of a condition requiring evacuation of the MCR. The staff finds the proposal to be acceptable, since there is no regulatory requirement for component-level control as it relates to

the AP1000 design. Specifically, the plant design does not credit component-level control of equipment to perform safety functions; all safety functions are performed at the system level. Westinghouse has defined the components having onerous consequences in Table A-1 of the FMEA of AP1000 PMS, WCAP-16438-P, Revision 2 (ADAMS Accession Numbers ML090790514, ML0907900513 for publicly available documents) and the staff finds this list acceptable. Although Westinghouse considers it proprietary, it will make the component information available to operations, engineering, and maintenance personnel in a licensed power plant using the AP1000 design, thus making the information's classification acceptable.

7.2.2.3.12 Operational and Maintenance Bypasses

Clauses 6.6, 6.7, 7.4, and 7.5 of IEEE Std. 603-1991 address the requirements as they relate to the operating and maintenance bypass of the sense and command and execute features of the safety I&C system. In part, the clauses require that operating bypasses automatically prevent the activation of an operating bypass or initiate the safety function if the applicable permissive conditions are not met. The capability of a safety system to accomplish its safety function shall be retained while equipment for sense and command and execute features is in maintenance bypass. Additionally, the guidance of RG 1.47 must be addressed to ensure the system responds appropriately in the presence of operational or maintenance bypasses.

The staff evaluated several sections of WCAP-16675-P regarding the PMS bypass capabilities. The four-division system has a high level of redundancy, which allows a division to be bypassed, placing the PMS logic function affecting a reactor trip or ESF actuation into a 2oo3 condition. Additionally, WCAP-16675-P, states that the design does not allow bypassing of two or more redundant channels or divisions. However, placing a given channel into a partial trip condition, if warranted, occurs automatically and does not require the "Function Enable" key switch on the MTP. The AP1000 DCD also commits to the prevention of the operating bypasses when permissive conditions are not met. This aspect of the design would be verified in the ITAAC described in AP1000 DCD Tier 1, Table 2.5.2-8, Design Commitments 9a–d and 11. Thus, based upon the information described above and that found in Section 7.5 of this report, the NRC finds the methodology described in WCAP-16675-P to bypass a given division of the PMS, for maintenance or operational conditions, to be acceptable.

7.2.2.3.13 Integrated Logic Processor Technical Evaluation

The ILPs serve as the action-sequencing logic in the ESFAS portion of the PMS; they distribute the activate signal to the various CIMs, via their respective SRNCs. Based on the design information in WCAP-16675-P, the ILP acts as an intradivisional interface device between the comparative logic device (e.g., LCL) and the SRNC. The SRNC then forwards its output to the priority module (CIM). The ILP uses a design previously approved by the NRC (i.e., Common Q equipment). The staff identified this design information through examination of docketed material within Section 2.2.3.2.2 of WCAP-16775, which revealed the ILP uses an AC160 programmable logic controller to operate. As the AC160 is the processor within the Common Q platform, and the staff has previously approved its use, the staff finds the ILP design acceptable provided the remainder of its components function identically to that of a Common Q based module. The NRC staff previously identified this issue as OI–SRP–7.2–ICE–04 and, based upon the review of the information in Section 2.2.3.2.2 of WCAP-16775, the staff finds the design of the ILP acceptable.

7.2.2.3.14 Component Interface Module Technical Evaluation

The CIM serves as a transitional device that receives its safety-related input signal from the output of its respective SRNCs and delivers its output signal to the respective final actuation device of a given safety-related component. The CIM also serves as an interface device that receives input signals from the non-safety-related PLS, in addition to the input signal it receives from the SRNC. The non-safety-related communications (control) signal is applied to the CIM through the non-safety-related RNC, which serves as a transitional device from the non-safety-related to the safety-related systems.

The CIM System comprises the following major components:

Component Interface Module	(CIM)
Safety Remote Node Controller	(SRNC)
Double Wide Transition Panel	(DWTP)
Single Wide Transition Panel	(SWTP)
CIM Base Plates	
SRNC Base Plates	

The dual-redundant field programmable gate array (FPGA) based SRNCs receive their [ ] input from their respective ILP within the PMS via a high speed link (HSL). The SRNCs process the PMS signal [ ] prior to the safety-related PMS signal being presented to the CIM. Upon the completion of the signal conditioning being performed by the SRNC, the PMS signal is transmitted to the DWTP, which serves as a connection panel for various signals, and then to the CIM.

The DWTP connects the SRNC base plates and the incoming non-safety-related Ovation® signal to the input of the respective CIM. The DWTP also serves as the connection point for the 24 Vdc power feeds that provide power to the SRNC and CIM base plates, the non-safety-related RNC, and the SWTPs, if any are utilized. The SWTPs serves as extender modules that connect to the DWTP and allow additional CIMs to be connected to the given configuration of CIMs.

The SRNC and CIM base plates serve as physical mounting sockets to which a given SRNC or CIM can be attached.

The output signals from the DWTP or, if utilized, the SWTP, are presented to CIMs, namely the non-safety-related Ovation® signal from the PLS and the dual redundant, safety related PMS signal.

The CIM also utilizes FPGA programmable technology, which serves to evaluate and prioritize which of the two signals are present, and position the safety-related component accordingly.

IEEE Std. 603–1991 requires the CIM System satisfy all applicable criteria to ensure the device meets safety system requirements.

To address the single failure criterion in Clause 5.1 of IEEE Std. 603-1991, Westinghouse submitted WCAP-16438-P, “FMEA of AP1000 Protection and Safety Monitoring System,” Revision 2, and WCAP-16592-P, “Software Hazards Analysis of AP1000 Protection and Safety Monitoring System,” Revision 1. The AP1000 FMEA discusses the possibility of individual SRNCs and CIM failure modes and their effect upon the system. Sections 7.1.5, I&C

Architecture and 7.2.2.3.2, Single-Failure Protection, discuss the findings related to the PMS SHA and FMEA respectively. The forthcoming FMEA for the CIM System will capture bounding failure types and the anticipated MTBF analysis for the components of the CIM System. Due to the forthcoming CIM System FMEA being bounded by the PMS FMEA (WCAP- 16438-P) the staff finds the approach of addressing the different failure modes of the CIM System adequate. Although both devices do not use software during their operational modes, the use of programming languages along with synthesizers, simulators and other testing tools being used during their lifecycles for both the SRNC and CIM require they be treated as software-based devices. Based upon the updated response to RAI-SRPSHA-01, Revision 1, dated June 28, 2010, which discusses the CIM System within the SHA, the staff finds the CIM System satisfies the single failure criterion. The update to the AP1000 SHA is captured under **CI-SRP7.1-ICE-01** and the update to the AP1000 FMEA is captured under **CI-SRP7.2-ICE-02**.

IEEE Std. 603–1991, Clause 5.2, requires the CIM System to be designed such that once the system has been actuated the executable features of the protective system continue to completion. Based upon the discussion in the WCAP-16438-P the AP1000 PMS FMEA, upon a failure of the SRNCs, such as through a loss of system power or overt module failure, the device will latch in its last command, such that if a failure occurs, the SRNC will continue to provide the actuate command. In the case of the CIM, should a single communication bus fail on the safety-related bus, the redundant bus will carry the signal through to completion. If a singular CIM fails outright, the system is designed with either a redundant CIM or another system design characteristic, such as a check valve in line with the valve actuator affected by the CIM failure to ensure the system is not adversely impacted by the component failure. These system design characteristics were verified during the April 20-22, 2009 audit conducted at the Westinghouse facility in Cranberry, Pennsylvania (ADAMS Accession Number ML091560352).

IEEE Std. 603–1991, Clause 5.3, along with 10 CFR Part 50 Appendix B requires the CIM System to be designed with a sufficient measure of quality to ensure a high level of component and system reliability consistent with low failure rates. SRP Appendix 7.1-D, “Guidance for Evaluation of the Application of IEEE Std. 7-4.3.2”; Section 5.3; and BTP 7-14 specifically address the criteria for a quality software development process. Additional regulatory guidance discussing acceptance criteria related to protective system quality are discussed in Section 7.2.2.3.3, Quality. The staff found several areas of technical information to be lacking either a sufficient level of detail to satisfy BTP 7-14 or a proposed alternative method of providing adequate CIM System developmental detail in order for the staff to find the CIM development process of sufficient breadth and technical depth. As such, the final disposition of this issue related to CIM development, previously addressed as OI-SRP7.2-ICE-05, will be covered in Section 7.2.5.

IEEE Std. 603-1991 Clause 5.4, “Equipment Qualification,” states, in part, that 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. Based upon a review of the ITAAC in Table 2.5.2-8, particularly Design Commitments 2, 3, 4, 5a and 5b. The listed commitments address the protective system’s and therefore the CIM System’s ability to withstand the necessary seismic, electromagnetic/radio-frequency and electrostatic discharge loads or transients. Additionally, the CIMs must be able to withstand additional environmental conditions such as qualified temperature and humidity profiles. As a result of the requirements placed upon the protective system, and therefore the CIM System, in the Tier 1 ITAAC of Section 2.5.2 of the AP1000 DCD, the staff finds the CIM System meets the environmental

qualifications as required by IEEE Std. 603-1991.

Safety systems must also be capable of accomplishing their safety functions under the full range of applicable conditions specified in the design basis in accordance with Clause 5.5 of IEEE Std. 603-1991, System Integrity. Additionally, the staff used the guidance within Appendices 7.1-C and 7.1-D of the SRP to review the CIM System and the manner by which it meets the requirements of system integrity.

Of particular concern when dealing with computer-based or programmable technology-based systems is the system's ability to complete its function in an actual or real time period that would ensure that any design basis limits are not exceeded. The system must be left in a known state after an event condition has been resolved to satisfy Information Bulletin 80-06; thus ensuring that it is the operator, not the system, that controls the repositioning of equipment during recovery from an event. Additionally, a digital system should be able to detect, alert the operator, and take appropriate action, perhaps by taking a component, channel or division to trip or bypass, once a failure is detected.

Based upon a review of WCAP-16674-P, WCAP-16675-P, and Section 2.3.1.2.8 of WCAP-17179-P, the staff determined the CIM subsystem portion of the PMS system functioned in a deterministically-based manner. This information is also captured in lower level proprietary Westinghouse documents, thus helping to ensure safety-system timing requirements are validated. Based upon Section 6.0, Component Interface Module, of WCAP-16674-P, Westinghouse commits that, after the completion of an event scenario, the PMS components will remain in their actuated state until they can be repositioned by an operator. This commitment adequately addresses the guidance of Information Bulletin 80-06. In relation to the guidance of Appendix 7.1-C of the SRP detailing a protection system's response in the presence of a detected failure of a component, channel or division, the staff finds the information in Section 2.1 of WCAP-17179-P adequately addresses the system's self-identification and reporting of system faults. In addition, the FMEA for the PMS (WCAP-16438-P) discusses the overall system response in the presence of known component, channel or system faults in Section 4.4 ILC (Integrated Logic Cabinet) Process Station. Based upon a review of the docketed information presented by Westinghouse, related to System Integrity, the staff concludes the CIM System operates in a manner consistent with Clause 5.5 of IEEE Std. 603-1991.

IEEE Std. 603-1991, Clause 5.6, Independence, along with 10 CFR Part 50, Appendix A, GDCs 21, 22, and 24, require, in part, that safety-related protection systems be designed with sufficient physical, electrical, functional, and communications independence. The communications independence of the CIM will be discussed in Section 7.9. Electrical isolation of the CIM System is provided through the use of fiber optic connections from the PLS to the DWTP within the ILC, in which the CIM System resides. Physical independence is provided by housing all CIM system safety-related components separately from the non-safety-related PLS components with one notable exception. The RNC is housed in the ILC with the CIM System. Although not classified as a Class 1E component, Westinghouse committed to qualify the RNC as an associated circuit in accordance with IEEE Std. 384-1981. Although the functionality of the RNC cannot be guaranteed during or after a design basis event, Westinghouse's commitment to qualify the RNC to serve as an associated circuit prevents its loss of function and will not permit the safety-related function of the CIM from being diminished or prevented. As such, the interaction of the PLS and PMS within the CIM also addresses functional isolation in that a loss of function within the RNC or another PLS-based component will not inhibit the

CIM from carrying out its safety-related function in accordance with 10 CFR Part 50, Appendix A, GDC 24. For further information related to PMS independence, refer to Section 7.2.2.3.6, Independence.

Based upon a review of the information contained in WCAP-16674-P, Revision 2, WCAP-16675-P, Revision 3, and WCAP-17179-P, Revision 1, the staff finds the CIM System meets the criteria related to physical, electrical and functional independence requirements between the safety-related and non-safety-related systems. A discussion related to the findings on communications independence of the CIM System is provided in Section 7.9.

IEEE Std. 603-1991, Clause 5.7, and 10 CFR Part 50, GDC 21, require the protection system be capable of testing and calibration during all anticipated modes of operation. In addition, the guidance in Appendix 7.1-D and BTP 7-17, of the SRP, as well as RG 1.22, state how a system designed for high reliability will be able to be tested in various configurations while simultaneously ensuring the protection system stays in service. Based upon a review of all applicable information in Chapter 7 of the AP1000 DCD and associated TRs, Westinghouse credits no self tests that mitigate or replace the need to conduct periodic surveillance testing of the CIM or protection systems. After reviewing the CIM system TR, the system conducts periodic diagnostic self-tests and transmits the information via the CIM and SRNC to the ILP within the PMS, at which point the Common Q portion of the system alerts the operator to any condition outside of normal system operation. This topic is discussed further in Section 2.5 of the CIM TR. The staff finds that based upon a review of the information in WCAP-16674-P, Revision 2; WCAP-16675-P, Revision 3; and WCAP-17179-P, Revision 1; the CIM System satisfies Clause 5.7 of IEEE Std. 603-1991 and 10 CFR Part 50, Appendix A, GDC 21.

Clause 5.9, Control of Access, in IEEE Std. 603-1991, stipulates appropriate levels of control be required to access the safety system. The PMS is typically accessed from either the PDSP in the MCR or via the division specific MTP. The CIM System components can be accessed when required, such as is the case when safety-related components with non-onerous consequences cannot be controlled via the PLS via the local controls on the CIM itself, but the cabinets in which the CIMs are housed are locked and administrative controls will be in place to prevent unwanted access of the CIM System. A more detailed analysis concerning the control of access to the CIM and PMS is provided in Section 7.9.5, which evaluates Westinghouse's requirements to ensure the PMS is constructed in an SDOE.

Based upon a review of the material within WCAP-17179-P, Revision 1, in particular Section 2.12, Human Factors and Maintenance Considerations, the staff finds the CIM System adequately addresses Clause 5.10, "Repair," of IEEE Std. 603-1991.

In relation to the use of automatic and manual control the CIM System is not designed for routine manual control. However, in the event of the failure of a safety-related component with non-onerous consequences that does not have individual safety-related controls on the safety-related PDSP in the MCR (as defined by the PMS FMEA in WCAP-16438-P, Revision 2), the CIM possesses local safety-related controls that can be utilized to position the safety-related component as the situation requires. It should be noted these non-onerous components are typically soft-controlled from the PLS, however as the PLS is non-safety-related, its actions are not credited in accordance with IEEE Std. 603-1991. For further discussion regarding how the PMS executes automatic and manual controls refer to Section 7.2.2.3.11 of this report. Based upon its review of WCAP-17179-P, Revision1, the staff finds the CIM System meets the requirements of IEEE Std. 603-1991, Clauses 6.1 and 6.2, Automatic and Manual Control

respectively.

IEEE Std. 603-1991, Clause 5.15 requires the protection system operate in a reliable manner. To facilitate this requirement as it relates to the CIM System, appropriate analyses shall be conducted to ensure that reliability goals have been achieved. Westinghouse has committed to present to the staff a formal CIM development process, in which it will demonstrate what quality measures, processes, policies, procedures and analyses will be completed in order to satisfy the requirements of IEEE Std. 603-1991, Clause 5.15. For additional discussion of the staff's understanding of the Westinghouse commitments made related to CIM System reliability as a byproduct of the CIM development process, refer to Section 7.2.5 of this report.

The staff conducted an engineering review with Westinghouse technical personnel on October15 - 16, 2008, and January 29 - 30, 2009, and conducted two audits, one on April 20-22, 2009 and the other on April 12 -16, 2010 to discuss the PMS development process, of which the CIM is a critical part. Previously through the use of OI-SRP7.2-ICE-05 the staff raised the issue of an inadequate CIM development process and the staff restated this conclusion to Westinghouse after the April 12 -16, 2010 audit and transmitted RAI-SRP7.0-ICE-11 to Westinghouse on May 17, 2010. After reviewing the updated response to the RAI in WCAP-17179, the staff found Westinghouse did not provide sufficient planning or design information related to the CIM priority module. The following provides a topical breakdown of the required information:

- Section 5.1.5 of WCAP-16675-P describes the CIM as a non-software-based Class 1E device that is not considered to be susceptible to a software common-cause failure. However, as the CIM is FPGA-based (programmable technology), Westinghouse did not provide sufficient information for the staff to determine that the CIM is not susceptible to a software common-cause failure (SWCCF). Westinghouse commits to updating all TRs by removing all text stating the CIM is not susceptible to a SWCCF. This is **CI-SRP7.2-ICE-06.**
- Westinghouse has not described the programmable development plans for the CIM logic development.

Westinghouse has not provided sufficient information on these topics, previously requested under RAI-SRP7.1-ICE-21, RAI-SRP7.1-ICE-22, and RAI-SRP7.1-ICE-23. Additionally, after conducting two audits, one in Scottsdale, Arizona (at the CIM and DAS supplier's facility) and the other in Warrendale, Pennsylvania (Westinghouse location) and reviewing the information contained within WCAP- 17179, the required information, in both depth and breadth, was determined not to be present for the CIM or its peer components in the AP1000 Component Interface Module TR. The NRC staff previously identified this issue as OI-SRP7.2-ICE-05 and based upon Westinghouse's commitment to develop an adequate CIM development process, this open item will be closed out as discussed in Section 7.2.5.

7.2.2.3.15 Safety-Related Remote Node Controller Technical Evaluation

The staff conducted an audit that dealt with the review of Westinghouse Phase 1 and Phase 2 proprietary documents for the AP1000 PMS SLC on April 20–22, 2009, in Cranberry, PA (ML091560352). During the demonstration of a "test" system, the staff learned of a new device that Westinghouse would add to the PMS. Westinghouse demonstrated the use of an SRNC that would serve as the interface device from the ILP to the CIM. Under previous revisions of

TRs, no intermediary device existed between the ILP and the CIM. Additionally, the staff reviewed WCAP-17179-P, the AP1000 Component Interface Module Technical Report that discussed the use of the SRNC within the CIM System. Based upon the review of the report, questions regarding the use of and quality design process built into the SRNC device remain. Therefore, the issue was captured under the open item related to the CIM. The issue previously identified as OI-SRP7.2-ICE-06 pertaining to the quality development process of the SRNC will be captured by the response to OI-SRP7.2-ICE-05 which discusses quality development process of the CIM, of which the SRNC is a part. This open item is discussed in Section 7.2.5.

7.2.3 Common Qualified Platform Design and COL Action Items

In APP-GW-GLR-017, Westinghouse stated its position on what current and future activities it will complete through the ITAAC process. In some cases, the closeout activities either point to more than one ITAAC for closure, or Westinghouse requested closure of a given PSAI when it had not met all the acceptance criteria for a PSAI. The information in APP-GW-GLR-017 is not entirely consistent with the staff's position regarding the disposition of the GOIs and PSAIs.

To identify Westinghouse's position regarding currently open and previously closed PSAIs and GOIs through the ITAAC process, the NRC asked Westinghouse, in RAI-SRP7.1-ICE-01, to provide a detailed road map showing which I&C design items remain open and which have already been closed, as well as the method of closure through the ITAAC or DAC process.

On December 12, 2008, the NRC received the Westinghouse response to RAI-SRP7.1-ICE-01 in DCP/NRC2319 (ADAMS Accession Number ML083510079). However, several of Westinghouse's conclusions were not consistent with the staff's findings, which is based on a review of the information contained in the following documents:

- "Safety Evaluation by the Office of Nuclear Regulation CE Nuclear Power Topical Report CENPD-396-P Common Qualified Platform Project 692" (ADAMS Accession Number ML003740165), and its supporting future documents regarding the closeout of GOIs and PSAIs, also known as Category 1 and Category 2 Closeout Items (ADAMS Accession Number ML011690170 and ML030550776)

- APP-GW-GLR-017

- Response letter to RAI-SRP7.1-ICE-01, dated December 12, 2008

The staff determined that GOIs 7.1, 7.2, 7.3, 7.5, and 7.6 are closed, based on the findings in "Acceptance of the Changes to Topical Report CENPD-396-P, Rev. 01, 'Common Qualified Platform,' and Closeout of Category 2 Open Items (TAC No. MB2553)," filed under ADAMS Accession Number ML030550776. The NRC closed out GOIs 7.4 and 7.7 generically, as well as PSAI 6.3. The NRC closed GOI 7.9 and 7.10 in acceptance of "design concept only," based on findings in "Safety Evaluation for the Closeout of Several of the Common Qualified Platform Category 1 Open Items Related to Reports CENPD-396-P, Revision 1, and CE-CES-195, Revision 1 (TAC No. MB0780)" (ADAMS Accession Number ML011690170).

The following provides the staff's position with regard to the remainder of the open GOIs and PSAIs:

- GOI 7.8

  The staff reviewed WCAP-16674, Revision 1. The staff determined the methodology used by Westinghouse that the staff understands to be a "safe state, system-based" approach, which typically used the non-safety-related PLS to control a safety-related component, was acceptable, in that the system first attempts to activate the given safety-related component using the PLS and, failing that, the system then activates using the safety-related PMS. In the event of a SWCCF of the PMS, the AP1000 compensates by activating the DAS to meet the diversity requirements in BTP 7-19. Although other issues related to the development process of the priority device, known as the CIM System in the AP1000 design, still remain, the mechanism by which the safety-related component actuates, either by a non-safety-related or safety-related system means, is deemed acceptable. Therefore, the staff considers GOI 7.8 closed. However the issue of overall CIM System quality, planning and development processes continues to be a concern previously captured under OI-SRP7.2-ICE-05 and, based upon Westinghouse's commitment to adequately address a high quality CIM development process. This action is discussed in Section 7.2.5.

- GOI 7.9

  The applicant stated, in APP-GW-GLR-017, that the NRC can close GOI 7.9, regarding the specific use of the ITP and the Advant Fieldbus (AF) 100 buses to provide separation of safety and non-safety signals, since the AP1000 I&C system differs in some details from the integrated solution described in Appendix 4, "Common Qualified Platform Integrated Solutions." Additionally, this TR provides other plant-specific implementations of safety-to-non-safety communications.

  Thus, the staff considers GOI 7.9 closed. The staff evaluated the other plant-specific implementations of safety-to-non-safety communications in Section 7.9 of this FSER supplement.

- GOI 7.10

  Westinghouse committed to alter the characteristics of the AP1000 Common Q platform so that the AP1000 design no longer uses multichannel operator stations. Therefore, the NRC considers GOI 7.10 closed.

- PSAI 6.1

  The staff agrees with Westinghouse's conclusion in APP-GW-GLR-017 that it uses its quality assurance program to determine the suitability of all I/O devices, by following the requirements of the Westinghouse QMS, which the NRC approved in August 2002 (ADAMS Accession Number ML022390672). The NRC considers PSAI 6.1 closed.

- PSAI 6.2

The staff agrees with Westinghouse's conclusion in APP-GW-GLR-017 that, since the AP1000 does not use a hardware user interface, PSAI 6.2 is not valid in the AP1000 specific application. Therefore, the NRC considers PSAI 6.2 closed.

- PSAI 6.3

  The NRC closed out this issue (ADAMS Accession Number ML011690170) (see above discussion).

- PSAI 6.4

  The staff agrees with Westinghouse's conclusion in the RAI response letter dated December 12, 2008 (see above), as well as the information in "Resolution of Common Q NRC Items for AP 1000," Revision 0, also referred to as TR-42 (ADAMS Accession Number ML061440346), that this PSAI will not be closed until the completion of the testing phase for hardware and software for the PMS. This commitment to test the system's components to appropriate levels of environmental qualification appears in AP1000 DCD Tier 1, Chapter 2, Section 2.5.2, ITAAC Table 2.5.2-8, Design Commitment No. 4.

- PSAI 6.5

  The staff agrees with Westinghouse's conclusion in the RAI response letter dated December 12, 2008 (see above), that this PSAI will be addressed in the testing phase for PMS hardware and software. The commitment to verify the implementation of the SLC appears in AP1000 DCD Tier 1, Chapter 2, Section 2.5.2, ITAAC Table 2.5.2-8, Design Commitment No. 11.

- PSAI 6.6

  The staff agrees with the approach Westinghouse selected regarding the AP1000 setpoint methodology in WCAP 16361-P, "Westinghouse Setpoint Methodology for Protection Systems—AP1000" (APP-PMS-JEP-001), Revision 0. AP1000 DCD Tier 1, Chapter 2, Section 2.5.2, ITAAC Table 2.5.2-8, Design Commitment No. 10, addresses the actual setpoint accuracy and response time of AP1000 safety systems. Since the DCD provides an acceptable setpoint methodology and ITAAC to verify setpoints and response time, the NRC considers PSAI 6.6 closed. Section 7.2.7 contains further discussion of setpoints.

- PSAI 6.7

  The staff agrees with Westinghouse's conclusion in the RAI response letter dated December 12, 2008 (see above), that this PSAI will be addressed during the human factors engineering testing phase for the PMS. AP1000 DCD Tier 1, Chapter 3, ITAAC Table 3.2-1, includes the design commitments for verifying the human factors engineering. Further information is provided in Chapter 18 of the FSER.

- PSAI 6.8

The staff agrees with Westinghouse's conclusion in the RAI response letter dated December 12, 2008 (see above), that this PSAI is applicable to existing NPPs, not new power plants incorporating new designs. Therefore, the NRC considers this PSAI closed.

- PSAI 6.9

  The staff agrees with Westinghouse that the plant procedures and/or technical specifications due to installation of the Common Q system will be dealt with at the plant-specific level. Chapter 16 of NUREG-1793 and this supplement address the technical specifications.

- PSAI 6.10

  Previously, the staff reviewed but had not approved the generic FMEA, and submitted several RAIs to Westinghouse to offer a more detailed technical response or to clarify several statements within the FMEA document that were unclear. Section 7.2.2.3, "Single-Failure Protection," which discusses the technical information required of Westinghouse related to its FMEA. As a result, the NRC considered this PSAI open. Based upon the submission of Revision 2 of WCAP 16438-P, "FMEA of AP1000 Protection and Safety Monitoring System" and Westinghouse's commitments to update the next revision of the FMEA, the PSAI is considered closed. For further information, regarding this topic and the accompanying CI, refer to Section 7.2.2.3.2, Single Failure Protection.

- PSAI 6.11

  PSAI 6.11 states that an applicant using the Common Q platform would need to address D3 to prevent a SWCCF. In Sections 7.1 and 7.7 of the AP1000 DCD, Westinghouse describes the functional requirements of the DAS. The DAC in Revision 17 of AP1000 DCD Tier 1, Table 2.5.1-4, Item 4, includes the design and analysis of the DAS. As described in Section 7.8 of this FSER supplement, Westinghouse modified Item 4. The staff found that Westinghouse provided sufficient design information to justify the modifications. Therefore, this PSAI is closed.

- PSAI 6.12

  AP1000 DCD Tier 1, Chapter 2, Section 2.5.2, ITAAC Table 2.5.2-8, Design Commitment No. 10, defines the commitment to verify proper response times of circuits. Since Westinghouse has provided an acceptable ITAAC to address this action item, the NRC considers PSAI 6.12 closed. The time response of the CIM System is addressed in Section 7.2.2.3.14, Component Interface Module Technical Evaluation of this report.

- PSAI 6.13

  The staff agrees that this PSAI will remain open until the completion of integration and preoperational testing. AP1000 DCD Tier 1, Chapter 2, Section 2.5.2, ITAAC Table 2.5.2-8, Design Commitment No. 11, includes the commitment to verify load capacity and sharing of communications resources for the PMS.

- PSAI 6.14

  PSAI 6.14 states implementation of the Common Q must not render invalid any previously accomplished TMI [Three-Mile Island] action items. In NUREG-1793, the staff found the AP1000 design addresses the TMI action items. The staff did not find any information in Revision17 to the AP1000 DCD that would invalidate that conclusion. Since the AP1000 design meets the I&C-related TMI action items described in 10 CFR 50.34(f)(2), the staff finds this PSAI closed.

Based upon the discussions above, the staff considers all GOIs closed. The open PSAIs listed above will continue to remain open until they are resolved.

7.2.5 Protection and Safety Monitoring System Design Process Review

In Revision 17 of AP1000 DCD Tier 1, Section 2.5.2, Westinghouse describes its entire SLC process related to the development of the Common Q portion of the PMS, which it will implement during the planning, design, construction, testing, and operational phases for the AP1000 I&C safety systems. In Revision 17 of AP1000 DCD Tier 1, Section 2.5.2, Design Commitment No. 11, Westinghouse deleted the design requirements phase and system definition phase. Westinghouse based this removal on the cumulative amount of both docketed and audited documentation made available to the staff as of this date.

The staff reviewed the information on the docket and conducted several site visits related to the review of the PMS design process at Westinghouse's Twinbrook facility, and in both Monroeville and Cranberry, PA. The primary purpose of the Twinbrook visits (April 8–10, 2008, October 15–16, 2008, January 29–30, 2009 and July 30, 2009) was to conduct an engineering review of the documents for the design requirements and system definitions phases (described as the conceptual phase and system definition phase by the Common Q SPM and WCAP-15927, and the planning activities and requirements activities phases of SRP BTP 7-14 SLC Process).

Additionally, the NRC staff conducted three audits, the first was conducted on April 20–22, 2009, examining the Phase 1 and Phase 2 AP1000 PMS SLC proprietary material at the Westinghouse facility in Cranberry, PA (ADAMS Accession Number ML091560352). The second audit was conducted on March 8 – 11, 2010 at CS Innovations, in Scottsdale, AZ. CSI serves as the designer and supplier of the CIM subsystem (as well as the DAS – Section 7.8 provides further discussion of how adequate diversity is maintained between the two systems) within the PMS. The more recent audit was conducted in Warrendale, PA at the Westinghouse Automation Services (formerly Repair, Replacement, and Automation Services) facilities on April 12 – 16, 2010. The more recent of the two audits was in order to determine whether an adequate demonstration of documentation had been presented to conclude that all requirements for the planning activities phase and requirements activities phases for both the PMS and the DAS would be considered complete. The October 3–5, 2006, trip report (Enclosure 4 of ADAMS Accession Number ML062910491) lists the design requirements phase documents associated with the staff's visit to the Monroeville, PA, facility as of October 2006.

Westinghouse based its conclusion that its design requirements and systems definition phases were complete on the proprietary information listed in the April 2009 audit report and the docketed information related to the AP1000 I&C safety systems design process. Westinghouse desired to close these two phases as part of its DAC closure process.

The staff finds that, once the requirements for each phase of the PMS (SLC) are met, "completion" rather than "elimination" of these and all phases described in the text of Section 2.5.2, Item 11, is appropriate, provided the staff finds the information contained within those phases to be sufficient. When the staff arrives at that conclusion for each given design process phase, Westinghouse may remove the given SLC phase(s) in AP1000 DCD Tier 1, Table 2.5.2-8, Item 11. Those tables describe specific ITAAC activities that will be completed during the given facility's inspection process, rather than the process undertaken to ensure that Westinghouse has included sufficient quality in the overall design process for AP1000 I&C safety systems. However, Westinghouse may not remove the design process description from the text-based portion of the design process description in Section 2.5.2, Item 11. Westinghouse agreed to restore all AP1000 PMS design process phases to the text-based portion of Section 2.5.2, Design Commitment No. 11. On February 23, 2010, Westinghouse submitted a response to open item OI-SRP7.2-ICE-07 that dealt with the removal of the text based descriptions within Tier 1, Chapter 2, Section 2.5.2. Westinghouse's commitment to re-insert the text-based portions of the PMS design process with the addition of the word "complete" to those given phases, once the staff finds a given developmental phase for the PMS to be adequately addressed is an approach acceptable to the staff. However, although not specifically addressed by this OI, the staff's expectation would be that this process would be carried out in the Tier 1 information, Chapter 2, Section 2.5.1 for the DAS in a similar fashion. The NRC staff previously identified this as OI-SRP7.2-ICE-07, and based upon Westinghouse's reply and the staff's determination of adequacy, this issue will be captured as **CI-SRP7.2-ICE-07** until this Tier 1 text-based restoration process has been undertaken in a future revision of the AP1000 DCD.

Based on the review of all audited and docketed documentation provided to the NRC that relates to the design requirements, system definition, and remaining developmental phases of the SLC for the PMS, as well as the series of audits conducted and their conclusions, the staff has not concluded that Westinghouse adequately completed or addressed the system definition phase, both from a lack of technical adequacy and a lack of completeness of the given subject matter. After reviewing Section 7.1.2.14.1 Design Process, of the AP1000 DCD, the staff was unable to locate additional information adequately describing all developmental phases of the Common Q SLC and the programmable technology lifecycle for the CIM System within Tier 2 of the AP1000 DCD. Additionally, based upon discussions held during the April 2009, March 2010, and April 2010 audits and conclusions drawn in the respective audit reports, Westinghouse stated they had "split" the System Definition phase of development for the Common Q and CIM System portion of the PMS. However, based upon the documents made available for review, it appears Westinghouse has "split" the System Definition phase of development in a discussion-based format only, as no alteration to the Common Q SPM, the Tier 2* document, WCAP 15927, or Tier 2 information has been made. Westinghouse did not provide sufficient technical information in Revision 17 of the AP1000 DCD, its associated TRs, or its proprietary documentation (to be made available for audit or inspection) to demonstrate satisfactory completion or alteration of the System Definition phase of Common Q development.

Westinghouse must provide adequate information regarding a programmable technology development plan for the CIM and SRNC**,** previously addressed by OI-SRP7.2-ICE-05 and

OI-SRP7.2-ICE-06, respectively. Westinghouse must restore the listing of the System Definition phase in AP1000 DCD Tier 1, Chapter 2, Section 2.5.2, Design Description 11, and within ITAAC Table 2.5.2-8, Design Commitment 11, until the staff finds that Westinghouse has completed that group of activities. Once those activities have been completed, the staff requires Westinghouse comply with its commitment as delineated in its response to open item OI-SRP7.2-ICE-07, now captured as **CI-SRP7.2-ICE-07** that dealt with the removal and restoration of the text-based descriptions within Tier 1, Chapter 2, Section 2.5.2. Additionally, the staff requires Westinghouse to restore information in Tier 1, provide additional, sufficient information in Tier 2, and Tier 2* documentation, especially WCAP 15927, that accurately describes all developmental phases and processes associated with the Common Q portion of the PMS. The NRC staff previously identified this issue as OI-SRP7.2-ICE-08. Based upon Westinghouse's commitment to restore the System Definition phase of the PMS SLC in Revision 18 of the AP1000 DCD and based upon Westinghouse's commitment to add ITAAC Design Description 14, within Tier 1, Chapter 2, Section 2.5.2, and Design Commitment 14 in Table 2.5.2-8, in which Westinghouse describes how it will meet the requirements related to the development of the CIM subsystem within the PMS, the staff determined that OI-SRP7.2-ICE-05 and OI-SRP7.2-ICE-08 were closed.

Since Westinghouse chose to add a more specific ITAAC related to the CIM Development process (Tier 1, Chapter 2.5.2, Design Description 14 and Design Commitment 14 in Table 2.5.2-8, ITAAC), and based upon the additional language added to the System Integration and Test phase acceptance criteria within Design Commitment 11, as discussed in Section 7.9.2.3.2 of this report, the staff finds the Design Requirements, or Planning Activities phase (per HICB BTP 14), of development for the PMS to be complete. However, the staff's expectation related to the forthcoming CIM Development process is that it will sufficiently address and describe all phases of development for the CIM subsystem of the PMS, including the Planning Activities phase of development.

Furthermore, since Westinghouse submitted, and the staff approved critical licensing documents within the System Definition phase related to PMS development (such as the FMEA for the AP1000 PMS (WCAP-16438-P) and the Software Hazards Analysis of the AP1000 PMS (WCAP-16592-P)), the staff does not consider the remaining development activities listed as part of the System Definition Phase of the PMS SLC to be DAC, as future development activities are not anticipated to impact licensing basis information such as the AP1000 DCD Tier 2 or AP1000 technical reports referenced in the DCD. However, if design detail from future development activities impacts the licensing basis information, the staff expects that information to be incorporated into the licensing basis information.

In Revision 16 of the AP1000 DCD, Westinghouse asked to remove the reference to WCAP 15927, which Westinghouse submitted to the NRC in addition to the SPM, to resolve RAI 420.001 and RAI 420.023. The staff issued these RAIs during the certification of the original AP1000 FSER in 2002. Westinghouse had to demonstrate the measures it would take to ensure critical information contained in this report is not removed. In July 2009, Westinghouse decided not to remove the report and submitted Revision 2 of WCAP 15927, which explained which organization, in this case the separate and independent IV&V organization, has the exclusive responsibility for IV&V activities, including testing activities. The staff considers the issue resolved, since WCAP-15927 elaborates on the organization that performs the software verification and validation activities. Specifically, Section 3 of the document states that "…testing activities are defined as part of the V&V process." The statement indicates that the

IV&V group is responsible for testing the PMS, as discussed in the Common Q SPM. Therefore, the staff finds that RAI-SRP7.1-ICE-10 is resolved.

7.2.7 Protection Systems Setpoint Methodology

On May 30, 2006, Westinghouse submitted WCAP-16361-P (APP-PMS-JEP-001), "Westinghouse Setpoint Methodology for Protection Systems—AP1000," Revision 0 (ADAMS Accession Number ML061530485). The following regulatory requirements and guidance documents apply to the staff's review of WCAP-16361-P:

- GDC 13 and 20
- 10 CFR 50.36(c)(ii)(A) (requires that the technical specifications include limiting safety-system settings)
- Regulatory Guide 1.105, "Setpoint for Safety-Related Instrumentation" (describes a method acceptable to the NRC staff for complying with the NRC's regulations for ensuring that setpoints for safety-related instrumentation are initially within, and remain within, the safety limit)

The Westinghouse setpoint methodology combines the AP1000 uncertainty components to determine the overall channel statistical allowance for the functions of the RTS/ESFAS. All appropriate and applicable uncertainties, as defined by a review of the AP1000 baseline design input documentation, have been considered for each RTS/ESFAS function. The methodology used to combine the uncertainty components for a channel is an appropriate combination of those groups that are statistically and functionally independent. Those uncertainties that are not independent are conservatively treated by arithmetic summation and then systematically combined with the independent terms. It includes instrument (sensor and process rack) uncertainties and non-instrument-related effects (process measurement accuracy). The methodology used the square-root-of-the-sum-of-the-squares technique, which the NRC has approved. Also, the American National Standards Institute, the American Nuclear Society (ANS), and the International Society of Automation (ISA) approve the use of the same probabilistic and statistical techniques for the various standards that determine safety-related setpoints.

The staff reviewed WCAP-16361-P and found that the allowable values (AVs) are equal to the rack calibration accuracy, which is the acceptable "as-left" value. This methodology ensures that the purpose of the AV is satisfied by providing a large enough allowance to account for those uncertainties not measured during the surveillance tests to protect the safety limit. Also, the difference between the AV and the nominal trip setpoint is as large as the calibration tolerance, and the AVs, along with the nominal trip setpoint, are included in the plant technical specifications as the associated criteria, in accordance with 10 CFR 50.36. Therefore, the staff concludes that the proposed WCAP-16361-P is acceptable. However, due to proposed changes in the inputs to the OPΔT and OTΔT as discussed in Section 7.2.2.1.1 of this report, Westinghouse committed to revise the WCAP 16361-P report to address these changes. This Westinghouse commitment will be captured as **CI-SRP7.2-ICE-08**.

Section 7.1.6.1 of Revision 17 of the AP1000 DCD states that all requested information on the

subject of setpoint methodology and final setpoint calculations has been completely addressed and requires no further action by the COL applicant. This statement is not in agreement with WCAP 16361-P, in which Westinghouse concludes that it cannot determine the final setpoint calculations until it completes the final design of the power plant. The staff issued RAI-SRP7.2-ICE-08, requesting that Westinghouse demonstrate how it intends to meet the final calculation requirements, given that it has not completed the protection system design. Westinghouse submitted DCR/NRC2315 (ADAMS Accession Number ML083470287) to the NRC on December 9, 2008, declaring that the COL applicant will determine the setpoint adequacy, in accordance with AP1000 DCD Tier 1, Table 2.5.2-8, Item #10. In a response to OI-SRP7.2-ICE-09, dated March 8, 2010, Westinghouse committed to restore the language in Section 7.1.6.1, stating that the COL applicant or licensee will be responsible for the final determination of setpoints, in accordance with AP1000 DCD Tier 1, Chapter 2, Section 2.5.2, ITAAC Table 2.5.2-8, Design Commitment 10. The NRC staff previously identified this is as OI-SRP7.2-ICE-09 and based upon the commitments within the March 8, 2010 response, the issue will be captured as **CI-SRP7.2-ICE-09**.

Section 2.2.6 of WCAP 16675-P states that Westinghouse uses the MTP to alter setpoints and addressable constants. The MTP provides a dedicated display interface for each division and is used to bypass the channel before changes are made. The staff evaluated the access controls on the MTP to control the alteration of addressable constants, setpoints, parameters, and other settings to meet the requirements of IEEE Std. 603-1991, Clause 5.9. This clause required the design to provide administrative control of access to safety-system equipment. Section 1, Point 10, of the digital I&C Interim Staff Guidance (ISG) Document #4, "Highly-Integrated Control Rooms—Communications Issues (ISG #4-HICRc)," Revision 1, clarifies this requirement by making the following statement:

> A workstation (e.g., engineer or programmer station) may alter addressable constants, setpoints, parameters, and other settings associated with a safety function only by way of the dual-processor/shared-memory scheme described in this guidance, or when the associated channel is inoperable. Such a workstation should be physically restricted from making changes in more than one division at a time. The restriction should be by means of physical cable disconnect, or by means of keylock switch that either physically opens the data transmission circuit or interrupts the connection by means of hardwired logic.

The staff finds the use of the MTP acceptable to bypass the channel in addressing the guidance in ISG No. 4-HICRc. Specifically, since the MTP serves as a dedicated display interface system for each division, the NRC does not require physical means to prevent the MTP from making changes to more than one division at a time.

7.2.8 Protection and Safety Monitoring System Evaluation Findings and Conclusions

The staff evaluated the revisions made to Chapter 7 of the AP1000 DCD, Revision 17, against the regulatory requirements stipulated in SRP Table 7-1. Below is a summary of the staff's findings as they relate to the AP1000 PMS.

The staff finds that the AP1000 DCD, Revision 17, meets the requirements of 10 CFR 50.55a(a)(1). Specifically, the staff found that the applicant incorporated quality standards into the design of the AP1000 I&C systems.

Regulations in 10 CFR 50.55a(h) require compliance with IEEE Std. 603-1991 and the correction sheet dated January 30, 1995. The staff compared the PMS in the amendments to the AP1000 I&C systems design with the applicable clauses of IEEE Std. 603-1991 and has the following findings:

- Westinghouse satisfied Clause 5.1 of IEEE Std. 603-1991, as documented in Section 7.2.2.3.1.1 of this FSER supplement. Specifically, the applicant has demonstrated how the PMS met the criteria presented in Clause 5.1 and GDC 21. The FMEA provided to the staff adequately demonstrates how the PMS will operate with a single failure under all postulated operating conditions, as discussed in Section 7.2.2.3.2 of this report.

- IEEE Std. 603-1991, Clause 5.3: Westinghouse satisfies the requirement of quality for the PMS, as documented in Section 7.2.2.3.3 of this FSER supplement. Specifically, the applicant has not demonstrated how it meets the criteria in Clause 5.3 with regard to the design of the CIM and the SRNC, which would then provide reasonable assurance that it had developed a high-quality product for all components within the PMS. Sections 7.2.2.3.14 and 7.2.2.3.15 of this report discuss these issues. The NRC staff previously identified these issues as OI-SRP7.2-ICE-05 and OI-SRP7.2-ICE-06, respectively. Based upon the Westinghouse commitment to add an ITAAC relating to the development of a programmable technology lifecycle for the CIM System consistent with the requirements of IEEE Std. 603-1991 and the guidance of BTP 7-14 of the SRP, the staff considers the open items closed.

- 10 CFR Part 52, “Licenses, Certifications, and Approvals for Nuclear Power Plants,” Appendix D, “Design Certification Rule for the AP1000 Design,” Section II.D, defines Tier 1 information as that information explaining design descriptions, along with ITAAC information. Based upon Westinghouse’s commitment to restore all phases of the PMS SLC design process in the text-based portion of Item 11 in SRP Section 2.5.2, “Protection and Safety Monitoring System,” the issue the NRC staff previously identified OI-SRP7.2-ICE-07, be captured as **CI-SRP7.2-ICE-07.**

- 10 CFR 52.47(b)(1) describes the ITAAC. Westinghouse provided sufficient information to satisfy the completion of the design requirements or conceptual phase of the PMS SLC, with the commitment to add the CIM Development Process ITAAC discussed above. Based upon its review of the documentation presented and based upon conclusions drawn in several audits, the staff will not approve the removal of the system definition phase of the PMS SLC until such time as Westinghouse provides satisfactory information to the staff for review and approval.

- IEEE Std. 603-1991, Clause 6.8: The staff found the proposed setpoint methodology acceptable. Additionally, the Westinghouse commitment to restore the text in Section 7.1.6.1 of the AP1000 DCD stating that the COL applicant or licensee will be responsible for the final determination of setpoints was found acceptable to the staff. The issue the staff previously identified as OI-SRP7.2-ICE-09 will be captured as **CI-SRP7.2-ICE-09.**

The staff finds that due to the addition of the ITACC related to the information that will be provided for the CIM Development Process, (Design Description and Design Commitment 14 within Tier 1, Chapter 2.5.2 and Table 2.5.2-8 respectively) the Design Requirements or Planning Activities phase of development for the PMS is considered complete.

The staff finds that the changes proposed in Revision 17 of the AP1000 DCD did not affect the remaining requirements of IEEE Std. 603-1991. Therefore, the staff's original conclusions in NUREG-1793 for these requirements are still valid.

The staff finds that Revision 17 of the AP1000 DCD did not present changes that would invalidate the staff's conclusions in NUREG-1793 regarding the requirements in 10 CFR 50.34(f)(2).

Appendix A to 10 CFR Part 50 provides specific criteria for I&C systems. The staff found that the PMS design continues to comply with the specific GDC for I&C systems in SRP Table 7-1, as described in NUREG-1793.

Regulations in 10 CFR 52.47(a)(9) require that applications for light-water-cooled NPPs evaluate the standard plant design against the SRP revision in effect 6 months before the docket date of the application. The evaluation required by this section shall include an identification and description of all differences in design features, analytical techniques, and procedural measures proposed for the design and those corresponding features, techniques, and measures given in the SRP acceptance criteria. SRP Chapter 7 provides the design considerations for safety, including criteria for performance and reliability considerations. The staff evaluated the information presented for AP1000 safety systems in the AP1000 DCD against the guidance provided in SRP Chapter 7. With the exception of the items listed above, the staff finds the PMS design descriptions to be acceptable.

7.3 Engineered Safety Features Actuation Systems

7.3.1.4.1 Automatic Depressurization System Valve Block

The AP1000 design uses Automatic Depressurization Valves (ADS) in certain accident conditions to depressurize the reactor coolant system (RCS) and allow passive safety systems to inject coolant to the reactor core. However, a potential common-cause failure of the PMS could initiate the ADS and simultaneously cause the PMS to not appropriately respond to the condition. As a result, the plant would need to respond to the spurious actuation of the ADS valves using back-up systems such as the DAS, non-safety systems, and operator action. While the scenario is beyond design basis, the consequences of such a scenario would be similar to that of up to a large-break loss-of-coolant accident. In addition, the staff did not identify analyses demonstrating the capability of the plant to mitigate the scenario of a spurious actuation of the ADS valves.

To address the potential spurious actuation of ADS valves due to a common-cause failure of the PMS, Westinghouse added an ADS valve block feature to prevent the spurious actuation of any of the ADS valve paths in each of the four stages of valve sets. The blocking feature prevents one valve in each of the two-valve valve sets from opening without deactivation of the block signal. For ADS Stages 1-3, the blocking feature is applied to the depressurization valve, and regarding ADS Stage 4, the blocking feature is applied to the squib valve. For ADS Stage 4, Westinghouse will determine whether the "arm" or "fire" signal within the squib valve will have the blocking feature applied. However, the staff believes the use of either signal is acceptable. Section 7.3.1.2.4.1 of the AP1000 DCD describes the need for a confirmatory process condition that is separate from the PMS actuation logic to serve as the input to the blocking signal circuit. The DCD describes the use of redundant CMT Level switches, one in each CMT, to serve as

the permissive that removes the block signal. Each of the respective level switches act to clear the block signal upon a lowering level in a given CMT once the tank level has reached or surpassed its setpoint. The DCD further states the blocking device will be a Class 1E module that will satisfy the requirements of safety-related I&C equipment. On a divisional basis, the interface between PMS and the blocking device will be the CIM for the each affected ADS valve in the division. The CIM resides in the PMS circuitry after the logic function has taken place. Additionally, the AP1000 DCD states that there are no interdivisional connections between the blocking devices nor will there be any coincidence voting between the blocking devices thus satisfying the independence requirements of IEEE Std. 603-1991. Section 7.3.1.2.4.1 of the AP1000 DCD also discusses the use of manual switches to enable the operator to manually clear the block signal as required. Since this action affects a component with onerous consequences the staff expects, that beyond the commitment in the AP1000 DCD for this switch to reside in the main control room (MCR), the given switches will be separate, hardwired switches in the primary dedicated safety panel or another safety-related panel in the MCR. In addition, Westinghouse updated Figure 7.2-1 noting that an ADS valve block signal is utilized via the CMT level switches' signal.

Beyond the redundancy created through the use of two CMT level switches to prevent a single level switch from causing a blocking circuit failure as described in the AP1000 DCD, per the description in the FMEA for the AP1000 PMS, WCAP-16438-P, the text explains that should an ADS Block signal within a division fail to remove the block signal, only a single division of PMS is affected. For stages 1-3 ADS valves the other division's ADS valves will actuate and as Stage 4 ADS valves utilize signals from two divisions, the "other" PMS division's signal will actuate the given Stage 4 ADS valve.

Based upon a review of the information related to the ADS Valve Blocking Circuit provided in the AP1000 DCD and the AP1000 FMEA for the PMS, the staff finds the addition of the ADS Valve Block circuit to be acceptable. The action of incorporating the information into Revision 18 of the AP1000 DCD and the next revision of the FMEA of the AP1000 PMS, WCAP-16438-P, will be captured as **CI-SRP7.3-ICE-01.**

7.3.4 ESFAS Evaluation Findings and Conclusions

The ESFAS is a portion of the PMS. Section 7.2 of this FSER supplement discusses the additional design information associated with the PMS and the staff's evaluation. The staff identified no changes of substance in Section 7.3 of the AP1000 DCD, Revision 17 other than those described below.

To prevent spurious actuation in of any of the valve paths for any and all of the stages of the ADS valves, Westinghouse chose to implement an ADS valve blocking circuit that prevents the given depressurization valve (for Stages 1-3 ADS valves) or the squib valve (for Stage 4 ADS valves) from opening unless system conditions warrant. Based upon a review of the information contained in the AP1000 DCD, Section 7.3.1.2.4.1 and the FMEA for the AP1000 PMS, WCAP-16438-P, the staff finds the addition of the ADS valve block circuit to be acceptable. The action of incorporating the information into Revision 18 of the AP1000 DCD and the next revision of the FMEA of the AP1000 PMS, WCAP-16438-P, will be captured as **CI-SRP7.3-ICE-01.**

7.4 Systems Required for Safe Shutdown

7.4.3 Evaluation Findings and Conclusions

Westinghouse changed the fifth bullet of Section 7.4.3.1.3 within the AP1000 DCD to clarify that the remote shutdown workstation is designed, not for a single failure, but with redundancy. However, when a random event other than fire causes an MCR evacuation, a coincident single failure in the safety systems controlled from the remote shutdown workstation is considered.

The staff finds the change acceptable, since Regulatory Guide 1.189, "Fire Protection for Operating Nuclear Power Plants," establishes the bases for safe shutdown with respect to fire protection. These limits do not require consideration of an additional, random, single failure in the evaluation of the capability to safely shut down because of fire. SRP Section 9.5.1 addresses conformance to Regulatory Guide 1.189. Therefore, the application of the single-failure criterion to remote shutdown is applicable only to other events that could cause the control room to become uninhabitable. These events would not result in consequential damage or unavailability of systems required for safe shutdown. The AP1000 design does consider events other than fire, coincident with a single failure in the safety system, for the remote shutdown workstation.

7.5 Safety-Related Display Information

7.5.3 Network Gateway (Real Time to Protection and Safety Monitoring System)

The applicant removed the communications description from Revision 17 of AP1000 DCD Tier 2, Section 7.1.2.8, and added a reference to Section 3 of WCAP-16675-P, Revision 3 (ADAMS Accession Numbers ML100050345, ML100050343 for the publically available version). WCAP-16675-P, as supplemented by WCAP-16674-P, Revision 2 (ADAMS Accession Number ML100050344, ML100050342 for the publically available version) provides a comprehensive description of the communications within the safety system, between safety and non-safety systems, and within the non-safety systems. Section 7.9 of this FSER supplement documents the review of the modifications made to the AP1000 safety and non-safety communications system, and provides additional information on the communications system.

7.5.5 Qualified Data Processing System

Revision 17 of the AP1000 DCD upgraded several variables in Table 7.5-1, "Post-Accident Monitoring System," to add seismic qualification to some instruments and to add a qualified data processing system (QDPS) indication. The staff accepts this change, which increases safety with more highly qualified instruments and controls, as well as improved information to support MCR operations.

Revision 17 of the AP1000 DCD changed the information given for several variables in Table 7.5-1 and added Note 7 indicating, "This instrument is not required after 24 hours."

The staff finds the addition of Note 7 acceptable for these variables because AP1000 DCD, Section 7.5.4, contains the statement below.

> Class 1E position indication signals for valves and electrical breakers may be

powered by an electrical division with 24-hour battery capacity. This is necessary to make full use of all four Class 1E electrical divisions to enhance fire separation criteria. The power associated with the actuation signal for each of these valves or electrical breakers is provided by 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. Once the position indication is lost, there is no need for further monitoring since the operator does not have any remote capability for changing the position of these components.

7.5.5.1 Combined License Information and Tables 7.5-1 and 7.5-8

Section 7.5.5 of the AP1000 DCD, Revision 17, states: "This section has no requirement for information to be provided in support of the Combined License (COL) application." Section 7.5, Tables 7.5-1 and 7.5-8, indicate that the meteorological parameters and environs radiation and radioactivity variables are "site specific." The staff requested clarification of this inconsistency in RAI-SRP7.5-ICE-02. The Westinghouse response (ADAMS Accession Number ML0833600440) states: "The words 'site specific' for environs radiation and radioactivity parameters indicate that these variables are site-related and are to be addressed by the COL applicant in the site emergency response plan identified in DCD Tier 2, Chapter 13, Section 13.3.1. Therefore, each COL applicant is to provide information for monitoring the meteorological parameters and environs radiation and radioactivity as appropriate." In a letter dated May 26, 2010 (ML101480129), Westinghouse provided a revised response to OI-SRP7.5-ICE-01 stating that Westinghouse commits to update Tier 2 Tables 1.8-1 and 1.8-2 in the next revision to the DCD. Westinghouse plans to modify Section 7.5.5 to indicate a COL action item regarding meteorological parameters and environs radiation and radioactivity instrumentation is required by the COL applicant. The NRC staff previously identified this as OI-SRP7.5-ICE-01 and, based upon the commitment within the Westinghouse response to the open item, the open item is considered resolved. The staff will continue to capture this issue as **CI-SRP7.5-ICE-01**.

7.5.6 Bypass and Inoperable Status Information

The applicant removed the description of the bypass and partial trip in AP1000 DCD Tier 2, Section 7.1.2.9, and provided a reference to Section 6 of WCAP-16675-P, Revision 3. Section 6.4 of WCAP-16675-P describes the design requirements for the bypass and partial trip conditions.

This section establishes the use of the Common Q network to provide bypass status indication in the MCR, in accordance with Regulatory Guide 1.47.

Technical Evaluation

Regulations in 10 CFR 50.34(f)(2)(v) require the safety-system design to provide an automatic indication of the bypassed and inoperable status of safety systems. As applied to data communications systems, SRP Section 7.9 states that the bypassed and inoperable status indications for data communications systems should be consistent with those of the systems of which they are part. The bypassed and inoperable status indication should conform to the guidelines of Regulatory Guide 1.47.

The staff finds the AP1000 DCD, as supplemented by WCAP-16675, sufficiently demonstrated how the PMS design provides bypass indications of protection channels used in the reactor trip and/or ESF actuation path to meet the requirements of 10 CFR 50.34(f)(2)(v). Specifically, the staff concludes the applicant provided adequate information that describes how the indications of bypassed channels or components on the MTP and MCR conform to Regulatory Guide 1.47, as specified in the guidance provided in SRP Section 7.9. The NRC staff previously identified this issue as OI-SRP-7.5-ICE-02 and, based upon the information contained in Section 6.4 Bypass and Partial Trip Condition within WCAP-16675, the staff finds the design of the system's ability to inform the operators of bypassed and inoperable safety channels within the PMS to be acceptable.

7.5.7 In-Core Instrumentation System

7.5.7.1 In-Core Instrumentation Interaction with Core Exit Thermocouples

WCAP-17226, "Assessment of Potential Interaction between the Core Exit Thermocouple Signals and the Self-Powered Detector Signals in the AP1000™ In-core Instrumentation System," Revision 2, describes how the AP1000 In-core Instrumentation System (IIS) design satisfies the requirements of IEEE Std. 384-1981 such that any credible single fault in the Non-Class 1E self-powered detector (SPD) signals will not reduce the number of valid Class 1E Core Exit Thermocouple (CET) inputs to the Post Accident Monitoring System (PAMS) below the required minimum number. The CET signal wires used by the Class 1E PAMS and the non-Class 1E SPD signal wires used by the On-line Power Distribution Monitoring System (OPDMS) are in very close proximity, and do not satisfy the separation distances identified in IEEE Std. 384-1981. In addition, the required separation distance identified in IEEE Std. 384-1981 between safety and non-safety signals is not met in the In-core Instrument Thimble Assemblies (IITA) and in the Mineral Insulated (MI) cable assembly hardware that route the CET and SPD signals from the Reactor Vessel head (RVH) penetrations to the Refueling Disconnect Panel (RDP). Furthermore, four of the AP1000 IITA contain Non-class 1E CET sensors that provide input to the non-Class 1E DAS.

Within the IITA, the active portions of the Class-1E CET elements and the non-Class 1E SPD elements are placed inside individual steel outer sheaths that share a common ground to provide electrical isolation between the CET and SPD elements. The presence of two commonly grounded metallic barriers within the IITA probe assembly and in the MI cables makes it incredible for an SPD emitter signal to short directly to the CET element signal leads.

From the Quickloc flanges on the RVH to the RDP, the CET signals and SPD signals share a common Class 1E design and post-accident environmentally qualified MI cable assemblies. The MI cable assemblies consist of individual flexible steel-sheathed cable sub-assemblies, which contain the separate CET and SPD signal lead MI cables, routed together in a flexible steel outer sheath that serve as conduits for individual CET and SPD cables in the cable assembly.

From the Class 1E connector panels on the RDP, the SPD signals are split and sent to two Signal Processing System (SPS) cabinets that are powered by non-Class 1E power supplies. The CET signals are also split at the RDP Class 1E connector panels, where most of the CET signals are sent to the PMS; the remaining 4 CET signals are sent to the DAS. The CET

signals sent to the PMS are split into two corresponding trains and sent to the corresponding PMS divisions via separate qualified Class 1E MI cables. The CET signals sent to the DAS are routed through post accident environmentally qualified MI cables.

An analysis was performed to determine whether the non-Class 1E power supplies that power the SPS cabinets can have an over-voltage or surge voltage that propagate backwards to the SPD inputs signals through the SPS circuitry without attenuation or shorting to ground. The analysis showed that it is credible that a sufficiently large over-voltage or a voltage surge at the SPS cabinet power supply inputs could cause at least a momentary loss of all Class 1E CET signals associated with the affected SPS cabinets via shorting between the SPD and CET wires in the backshell of the IITA or MI cable electrical connectors. If the over-voltage or transient surge condition were to occur on both SPS cabinets, then the result could be that all of the CET signals needed by the PAMS become inoperable.

To mitigate this concern, the applicant performed an analysis to determine the maximum sustained over-voltage value for low voltage circuits in Westinghouse Nuclear Power Plant designs that run cable per nuclear industry standards. The staff requested the applicant to describe how the maximum credible over-voltage generated by the SPS cabinets is established. In response, the applicant proposed to modify WCAP-17226 with the following explanation:

> "AP1000 requires that low voltage systems be installed in a separate raceway system from medium voltage systems. As such, the maximum credible sustained overvoltage condition which can occur in a low voltage power or control circuit routed in this (these) low voltage raceway system(s) can be determined conservatively by considering nominal system operating voltages and maximum preferred system voltage range as defined in ANSI C84.1-2006. The system voltage at the low voltage system will remain balanced when the medium voltage system is supplied from normal or reserved source of power during the normal plant operation. During the abnormal plant operation when the normal and reserve sources of power are not available, the low voltage system will continue to function by receiving power from the standby diesel generators. The system voltage will also remain balanced even when the medium voltage continues to operate in the presence of a single line to ground fault indefinitely.
>
> As the neutral of the load center transformers secondary windings are solidly (or effectively) grounded there will be no increase in the maximum credible sustained overvoltage of the low voltage system whether a ground fault is present at the medium voltage system or not. As such, the maximum credible sustained overvoltage numerical value, when the transformer is lightly loaded, can simply be derived from consideration of the nominal low voltage system of 480VAC plus a 10% multiplier (480VAC)(1.10) = 528 VAC for an maximum sustained system voltage during both normal full load and light load operation. The high voltage taps of the load center transformer is set such that the maximum allowable voltage at the terminals of the loads and the secondary winding of the load center transformers is not exceeded.
>
> For purposes of defining a value for design of isolation devices a margin of 10% will be used yielding (528VAC)(1.10) = 580VAC. This value is developed specifically for use as a bounding design value for isolation devices and, as described above, is conservative beyond the actual design operating conditions of the plant."

This established maximum credible over-voltage value allows for the identification of operating characteristics of the IITA and MI cable hardware used in the IIS to be specified to withstand a peak over-voltage beyond the identified historical maximum over-voltage value. The design requirements for the MI Cable and IITA electrical connector hardware require that manufacturing or proof testing be performed to demonstrate compliance with a 600 VAC peak voltage CET functional interaction exclusion requirements. This hardware testing requirement satisfies the requirements for testing or analysis of associated circuit interaction with Class 1E circuits contained in IEEE Std. 384-1981 for over-voltage conditions. To further mitigate the possibility of a transient surge voltage condition in the SPS cabinet's input power supply in excess of the identified maximum over-voltage value that may disable both Divisions of the CET signals used by the PAMS, different divisions of safety power are supplied to the IIS SPS cabinets, with the power cables routed in separate shielded conduits.

The applicant also identified the DAS as another non-Class 1E system that can cause a surge or over-voltage faults to propagate to the IIS. The applicant's analysis found that the maximum credible surge voltage output from the DAS to the DAS CET signal leads that could produce an interaction with the IIS is the same as the IIS IITA and CET cable. The identified maximum credible voltage output from the DAS to the CET signal leads are also equivalent to the electrical connector hardware voltage environmental electromagnetic interference qualification limit requirements contained in Tier 2, Appendix Section 3D.4.1.2 of Revision 17 of the API000 DCD. The DCD hardware requirements specifically require that the IIS IITA and associated cables be qualified to meet Reg. Guide 1.180, "Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference for Safety-Related Instrumentation and Control Systems," peak surge voltage pulse levels. This result ensures that if there is a voltage surge from DAS that propagates down through the DAS CET signal leads to the associated SPD cables, there will be no credible, systematic shorting of DAS CET signals to the associated SPD signal leads, which contain the CET signals that are sent to the PMS.

IEEE Std. 603-1991, Clause 5.6.3 requires that equipment in other systems that is in physical proximity to safety system equipment but that is neither an associated circuit nor another Class 1E circuit be physically separated from the safety system equipment to the degree necessary to retain the safety systems' capability to accomplish their safety functions in the event of the failure of non-safety equipment. Physical separation may be achieved by physical barriers or acceptable separation distance. The separation of Class 1E equipment shall be in accordance with the requirements of IEEE Std. 384-1981.

The NRC issued RG 1.75, "Criteria for Independence of Electrical Safety Systems" to endorse IEET Std. 603-384 with exceptions. RG 1.75 identifies the underlying separation criteria: (1) physical separation and (2) electrical isolation are provided to maintain the independence of safety-related circuits and equipment so that the safety functions required during and following any design-basis event can be accomplished. Section 5.6(3) of IEEE Std. 384-1992 provides general criteria for independence between safety-related and non-safety-related circuits. When minimum separation cannot be met, it allows an analysis of non-safety-related circuits to demonstrate that the safety-related circuits are not degraded below an acceptable level. If the analysis is successful, the non-safety-related circuits can remain as non-safety-related circuits. RG 1.75 clarifies that (1) non-safety-related circuits that are not separated from safety-related circuits through the minimum separation or barriers must be treated as "associated circuits," and (2) the cables that are associated because they are powered from a safety-related source serving non-safety-related loads or share the safety signal must also be treated as associated circuits. This regulatory guide defines "associated circuits" as "non-safety-related circuits that

are not physically separated or not electrically isolated from safety-related circuits by acceptable separation distance, safety class structures, barriers, or isolation devices."

Based on the staff's evaluation of the information presented in WCAP-17226, the staff finds that the associated circuit analysis performed and the ensuing design requirements adequately ensure that the Class 1E CET elements cannot be degraded below an acceptable level by over-voltage or surges from non-Class 1E SPD elements or other connected non-safety systems. The specific evaluation of portions of this analysis is documented below:

- Within the IITA, the staff finds that placing the active portions of the Class-1E CET elements and the non-Class 1E SPD elements inside individual steel outer sheaths that share a common ground provides adequate electrical isolation between the CET and SPD elements. The staff finds that since the steel outer sheaths share a common ground, it can adequately protect the CET element from a potential overload of the SPD element.

- From the Quickloc flanges to the RDP, the staff finds the MI cable assembly adequately ensures the isolation of Class-1E CET elements from SPD elements through the use of separate individual flexible steel-sheathed cable sub-assemblies for the CET and SPD signal leads. The individual steel-sheathed cables provide adequate electrical isolation to prevent faults within the SPD signal leads from propagating to the CET signal leads.

- The staff finds adequate the analysis provided to evaluate the maximum credible over-voltage or surge voltage that can propagate backwards from the non-class 1E power supplies in the SPS cabinets to the SPD input signals. Specifically, the staff finds that the applicant's analysis, which specifies that, for 3-wire low voltage AP1000 systems, the maximum sustained over-voltage will incorporate a 10% margin (which is above the 5% margin specified in ANSI C84.1-2006) for a solidly grounded system is consistent with the criteria found in IEEE Std. 141-1993, "IEEE Recommended Practice for Electric Power Distribution for Industrial Plants." IEEE Std. 141-1993, Clause 7.2.5 states there are three levels of conductor insulation for medium-voltage cables that are permitted: 100, 133, and 173%. The solidly grounded system permits the use of 100% insulation level, which indicates that the maximum sustained over-voltage is at 100% of the Line-to-Ground voltage during a single line to ground fault. Thus the 10% additional margin sufficiently bounds the anticipated maximum sustained over-voltage. Ultimately, the cable insulation selection for a nominal low voltage system of 480 VAC will be rated at a minimum of 600 V, which encompasses the anticipated maximum sustained over-voltage value of 528 VAC. Incorporation of the proposed change to WCAP-17226 to include a discussion of how the maximum credible over-voltage value is derived is tracked as **CI-SRP7.5-ICE-02**.

- Westinghouse proposed to specify design requirements for the MI Cable and IITA electrical connector hardware to be tested to withstand the identified maximum credible voltage values. This approach is acceptable to the staff in that it meets the associated circuit requirements of IEEE Std. 384-1981 for over-voltage conditions. In addition, assigning each SPS cabinet and its corresponding PAMS Division to a different Class 1E power bus, the staff finds this approach ensures any fault on the SPS cabinets' safety input power supplies will only occur on one SPS cabinet and can therefore only disable one Division of the CET signals used by PAMS. The staff finds this acceptable.

- Furthermore, the staff finds adequate the identified maximum credible overvoltage that can be generated from the DAS that could produce an interaction with IIS. The staff finds that by qualifying the IIS IITA and associated cables in accordance with RG 1.180, the design characteristics ensure that a potential voltage surge from the DAS will not be able to cause systematic shortening of the DAS CET signal to SPD signal leads. Therefore, the staff finds that the PAMS CET coverage is adequately protected against failures of the DAS.

7.5.9 Evaluation Findings and Conclusions

Appendix D.II, "Definitions," to 10 CFR Part 52, defines COL action items (COL license information) as items that identify certain matters that applicants must address in the site-specific portion of the FSAR. Westinghouse selected the site-specific parameters required to meet 10 CFR 50.34(f)(2)(xvii) regarding accident monitoring instrumentation as a COL action item and updated Tier 2 Tables 1.8-1 and 1.8-2 accordingly. Therefore, the staff finds the above requirements have been satisfied via the commitment in the Westinghouse response dated May 26, 2010. This issue will be captured as **CI-SRP7.5-ICE-01**.

Regulations in 10 CFR 50.34(f)(2)(v) require Westinghouse to provide for automatic indication of the bypassed and inoperable status of safety systems. The staff finds that Westinghouse has sufficiently addressed this requirement in the AP1000 DCD and the supporting TRs, as documented in Section 7.9.2.6 of this FSER supplement. Specifically, the applicant has demonstrated how the indication of bypassed and operable status of safety systems in the MCR conforms to Regulatory Guide 1.47. The NRC staff previously identified this issue as OI-SRP7.5-ICE-02, and, based upon the discussion within Section 6.4 of WCAP 16675, the staff finds the issue has been satisfactorily resolved.

Based upon the staff's review of WCAP-17226-P, the interaction between the IIS and other safety-related systems is deemed acceptable provided the proposed change to WCAP-17226-P to include a discussion of how the maximum credible over-voltage value is derived is included in the next revision of the document. This issue will be tracked as **CI-SRP7.5-ICE-02.**

Additionally, the staff finds that the accident monitoring instrumentation meets the applicable requirements of GDC 13 and 19, "Control Room."

7.6 Interlock Systems Important to Safety

7.6.5 Evaluation Findings and Conclusions

In Section 7.3.1.4.1 of this report it describes Westinghouse's commitment to add an Automatic Depressurization System (ADS) valve blocking circuit to prevent the spurious actuation of any of the valve paths in any of the stages for the ADS. As this circuit is described as a blocking circuit rather than an interlock, (in which a block may be cleared or overridden but an interlock must not), the circuit's operation is not captured in Section 7.6 of this report. As such, the changes in Section 7.6 of the AP1000 DCD did not affect any conclusions regarding regulatory compliance in NUREG-1793. Therefore, the staff finds the applicant continues to meet the requirements identified in NUREG-1793 for Section 7.6.

7.7 Control and Instrumentation Systems

7.7.1 System Description

7.7.1.1 Reactor Power Control System

The applicant revised the second paragraph of Section 7.7.1.1.1, "Power Control," to remove the term "lead/lag compensated." Westinghouse is revising the AP1000 design to apply the lead/lag compensation after the high auctioneer, versus before it. The applicant claims that this design does not require compensation to be factored into signal quality check acceptance criteria in the auctioneer. Westinghouse described this justification in APP-GW-GLR-080, Revision 0, "Mark-up of AP1000 Design Control Document Chapter 7." The staff's review confirms that this design change does not affect any staff conclusions in NUREG-1793.

The applicant also revised the description of the T_{ave} reactor control band for the various plant modes of control (i.e., load follow, load regulation, base load). The applicant claims that there is no advantage to increasing the deadband during load follow operations. The applicant further states that doing so would erode margins to reactor trip setpoints. Westinghouse also stated this justification in APP-GW-GLR-080, Revision 0. The staff's review confirms that this change does not affect any staff conclusions in NUREG-1793.

The applicant removed the "time weighted average" or "smoothing" compensation to the nuclear flux and the axial offset signals while the plant is in a load regulation mode of control. The applicant states that this current transient specification does not require complex "time weighted average" nuclear flux and axial offset signal compensation on the inputs to the axial offset control band calculation and that simple lag compensation is adequate. Westinghouse also stated this justification in APP-GW-GLR-080, Revision 0. The staff's review confirms that this change does not affect any staff conclusions in NUREG-1793.

7.7.1.2 Rod Control System

The applicant revised the interlock and "low" and "low-low" alarms associated with control rod insertion limits. The revision will move the automatic activation of the rod insertion interlock from the "low" rod insertion alarm setpoint to the "low-low" rod insertion alarm setpoint. In moving the activation of the rod insertion interlock from the "low" to the "low-low" rod insertion alarm, rod insertion will be prevented, at the "low" alarm setpoint, by following appropriate plant operating procedures and will be prevented at the "low-low" setpoint by automatically actuating the rod insertion interlock and terminating automatic AO bank insertion (or withdrawal to prevent further M bank insertion).

By moving the rod insertion interlock to the "low-low" alarm setpoint, continued rod insertion (and thus, a continued reduction in control rod shutdown margin) is automatically terminated by plant controls versus "appropriate plant operating procedures."

Furthermore, removing the interlock from the "low" alarm setpoint does not reduce any plant protection function or increase the risk of reducing protection against a reduction in control rod shutdown margin caused by the margin built into the difference between the "low" and the "low-low" rod insertion setpoints. Therefore, the staff's review confirms that this design change does not affect any staff conclusions in NUREG-1793, including Supplement 1.

7.7.1.3 Pressurizer Pressure Control

The applicant changed the description of the pressurizer variable heating control by stating that it is not sensitive to the rate of change in pressure and that it will respond in the same manner to small, fast, or slow small changes in pressure. The staff's review confirms this change does not affect any staff conclusions in NUREG-1793.

7.7.1.5 Feedwater Control

In Section 7.7.8.1 of the AP1000 DCD, Revision 17, the low-range feedwater flow measurement is no longer used in the low-power mode, and it is not used in the integration (reset) action of the low-power mode feedwater flow controller. This means that only feedwater temperature (low-power mode) and steam flow (high-power mode) are used to tune the integrator setpoints.

In both Sections 7.7.8.1 and 7.7.8.2, the control of the lift on the main and startup feedwater control valves is no longer determined by the ΔP available across the feedwater control valve, and the flow coefficient (C_v) characteristic of the valve. Therefore, in high-power control mode, the feedwater flow is regulated in response to changes in steam flow and proportional plus integral (PI)-compensated steam generator narrow-range water level deviation from setpoint. In the low-power control mode, the feedwater flow is regulated in response to changes in steam generator wide-range water level and PI-compensated steam generator narrow-range water level deviation from setpoint.

The startup feedwater control subsystem regulates the flow of feedwater in a manner similar to the way the (main) feedwater is controlled in the low-power control mode. Feedwater flow is regulated in response to changes in the steam generator wide-range water level and PI-compensated steam generator narrow-range water level deviation from setpoint. The staff's review confirms that this design change does not affect any staff conclusions in NUREG-1793.

7.7.2 Diverse Actuation System

Section 7.8 of this FSER supplement contains detailed evaluation regarding the DAS design changes.

7.7.3 Signal Selector Algorithms

The applicant has not demonstrated what specific actions are taken by the signal selector algorithms in the event that one of the multidivisional or multichannel inputs is deemed faulty or of "bad" quality. The staff requires all outputs of the device, whether they are in the form of control, alarm, interlock, or indications, to be identified and addressed. The staff issued this request to Westinghouse as RAI-SRP7.7-ICE-01. Westinghouse responded to the RAI in a letter, "AP1000 Response to Request for Additional Information (SRP 7)," dated July 7, 2008 (ADAMS Accession Number ML081910138). However, the staff found the response inadequate. Westinghouse submitted Revision 1 to address this issue on May 6, 2009, and subsequently Westinghouse submitted Revision 2 of RAI-SRP7.7-ICE01. In the Revision 2 response, submitted on January 27, 2010, Westinghouse states it will update the forthcoming Revision 18 of the AP1000 DCD so that it is clear that the SSAs are executed in the PLS and additionally that PMS and DAS performance are independent of the SSA. The NRC staff

previously identified this as OI-SRP7.7-ICE-01. Revision 2 of RAI-SRP7.7-ICE-01 adequately addresses this issue. The staff created **CI-SRP7.7-ICE-01** to track its incorporation into Revision 18 of the DCD.

7.7.4 Evaluation Findings and Conclusions

The staff finds the conclusions described in NUREG-1793 still valid, based on the staff's review of the changes proposed in Revision 17 of the AP1000 DCD. Specifically, the staff required additional information on how the signal selector algorithms would affect the PMS and the DAS. Information on such impacts could affect the degree of independence between the control system and the protection system, as required in GDC 24. Also, such impacts could affect the degree of diversity and quality of the DAS as required in GDC 22. The response discussed in Section 7.7.3 above adequately addressed the issue. The NRC staff previously identified this as OI-SRP7.7-ICE-01 and, based upon the Westinghouse commitment to add the requested information in the response into the forthcoming revision of the AP1000 DCD, the issue is captured as **CI-SRP7.7-ICE-01**.

Section 7.8 contains further evaluation of the DAS.

7.8 Diverse Instrumentation and Control Systems

7.8.1 System Description

The I&C systems reviewed in this section include the diverse Instrumentation and Control (I&C) systems and equipment that provide a diverse backup to the safety-related Protection and Safety Monitoring System (PMS) and the defense against postulated common-cause failures in the PMS and the non-safety-related Plant Control System (PLS) concurrent with postulated transients.

The review ensured that the applicant, Westinghouse designed and installed the anticipated transient without scram mitigation systems and equipment in accordance with the requirements of 10 CFR 50.62, "Requirements for Reduction of Risk from Anticipated Transients without Scram (ATWS) Events for Light-Water-Cooled Nuclear Power Plants", and 10 CFR Part 50, Appendix A, GDC 22..

The Diverse Actuation System (DAS) in the AP1000 DCD is a non-safety related I&C system and provides a diverse and independent method for tripping the reactor and performing several engineering safety features (ESF) in order to meet the requirements of 10 CFR 50.62 and 10 CFR Part 50, Appendix A, GDC 22. In addition, a set of dedicated and independent displays of selected plant indications and manual controls is provided in the Main Control Room (MCR) to address the criteria in Branch Technical Position (BTP) 7-19, "Guidance for Evaluation of Diversity and Defense-in-Depth in Digital Computer-Based Instrumentation and Control Systems."

The scope of the safety evaluation in the following section of this FSER supplement is limited to the changes that have been made to the approved DAS system since the AP1000 DCD, Revision 15, was certified.

7.8.2 Diverse Actuation System Assessment

The staff's FSER related to certification of the AP1000 standard design (NUREG-1793) is based upon WCAP 15775, "AP1000 Instrumentation and Control Defense-in-Depth and Diversity Report," (APP-GW-J1R-004), Revision 0, issued April 2002 (ADAMS Accession Number ML021220228). The applicant submitted Revision 2 of its D3 assessment on April 3, 2003 (ADAMS Accession Number ML030980037). The applicant revised its D3 assessment based on the response to the NRC's RAI 420.013, Revision 1, in a letter dated February 21, 2003 (ADAMS Accession Number ML030560120). The applicant referred to the Revision 2 of the D3 assessment in the certified AP1000 DCD, Revision 15. In the certified AP1000 design the hardware of the DAS is microprocessor based and its operating systems or programming languages are different from those used in the PMS.

In the original FSER (NUREG-1793), Section 7.1.6, the staff concluded that "the proposed design satisfies the Commission's position on I&C system diversity." The NRC based its conclusion on the proposed DAS design, as stated in Revision 15 of the applicant's DCD, which included the ITAAC listed in AP1000 DCD Tier 1, Section 2.5.1.

In the second paragraph of Section 7.7.2 of NUREG-1793 the staff concluded that based on the design commitments of Revision 15 of the AP1000 DCD:

> 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 applicant submitted APP-GW-GLN-022, Revision 1, "AP1000 Standard Combined License Technical Report DAS Platform Technology and Remote Indication Change," dated May 2007. In technical report APP-GW-GLN-022, Revision 1, the applicant changed the DAS design commitments and DAS ITAAC in Revision 15 of the AP1000 DCD to allow non-microprocessor-based implementations, added the DAS instrumentation cabinet, added an electrical penetration to the containment, and relocated a portion of the DAS to another area of the plant.

The following evaluation focuses on the modification to allow non-microprocessor-based implementations of the DAS and the addition of the DAS instrumentation cabinet. The relocation of DAS equipment within the plant has no impact upon the I&C review. Additionally, the installation of another electrical penetration to the containment is beyond the scope of the Chapter 7 review.

For the purposes of the Chapter 7 I&C review, the following areas of the DCD are affected:

Tier 1
Section 2.5.1
Table 2.5.1-4
Table 2.5.1-5
Table 3.7-1
Tier 2

Section 7.7.1.11
Figure 7.2-1
Section 9A.3.1.3.1.1
Table 14.3-3
Table 14.3-6
Table17.4-1
Table 19.59-18

The applicant discussed the change to the I&C technology utilized for the DAS throughout Tier 1 and Tier 2 in Revision 16 of the AP1000 DCD by substituting language, as appropriate, where it used the terms “microprocessor” and “software” to describe DAS technology. The applicant replaced the term “microprocessor” with “microprocessor or special purpose logic processor,” and the term “software” with “any software.” The addition of the DAS Instrument Cabinet, DAS-JD-004 will contain the 4-20 mAdc loop transmitters and power supplies necessary to complete the DAS instrumentation requirements. The DAS-JD-004 cabinet mounts next to the DAS Squib Valve Control Cabinet, DAS-JD-003. This is acceptable. The applicant revised Section 7.7.1.11 of the AP1000 DCD Tier 2, Revision 16 by replacing the terms “microprocessor-based” and “microprocessor” with “logic”, “software” with “any software” from several design change descriptions in APP-GW-GLR-080, “Mark-up of AP1000 Design Control Document Chapter 7”, Revision 0, which describes all changes to the AP1000 I&C systems in the certified AP1000 DCD.

This proposed change to use non-microprocessor-based technology is intended to increase reliability and was found to be acceptable. However, a discussion concerning the diversity between the PMS and the DAS is provided later in this section.

In Revision 17 of the AP1000 DCD, the applicant removed DAS DAC from Tier 1, Section 2.5.1, “Diverse Actuation System (DAS) Design Description,” Items 4a and 4b, as well as from Tier 1, Table 2.5.1-4, ITAAC Items 4a and 4b. Items 4a and 4b are the design requirements and system definition phases of the DAS hardware and software design process. The applicant removed portions of the DAC, and also provided the corresponding design information in WCAP-17184-P, “AP1000 Diverse Actuation System Planning and Functional Design Summary Technical Report,” Revision 1, which addresses those two phases. However, the applicant failed to provide a description in Chapter 7 of the AP1000 DCD, Tier 2, regarding completion of those two phases found in AP1000 DCD Tier 1. 10 CFR 52.47(a)(2) requires standard design certification applications to provide a level of design information sufficient to enable the Commission to reach a final conclusion on all safety issues associated with the design before the certification is granted. In the proposed amendment to the AP1000 DCD, Tier 1, ITAAC Items 4a and 4b are removed based on design work accomplished. In Chapter 7 of the AP1000, Tier 2, DCD, the applicant should provide a summary and justification for why the ITAAC found in Items 4a and 4b of AP1000, Tier 1, Table 2.5.1-4, can be removed. The staff issued RAI-SRP7.8-DAS-12 requesting the applicant to describe the completeness of the above two phases in Chapter 7 of AP1000 DCD, Tier 2. In response to this RAI, the applicant provided a detailed description about the two completed life cycle phases as a markup for the AP1000 DCD Tier 2, Section 7.7.1.11, which is found acceptable. In addition, the applicant

added an ITAAC item to Table 2.5.1-4 of AP1000 DCD Tier 1 to address the ITAAC for DAS manual actuations. The staff finds the above changes to AP1000 DCD Tier 1 and Tier 2 acceptable and finds the response to RAI-SRP7.8-DAS-12 acceptable. The committed changes will be tracked as **CI-SRP7.8-ICE-01**.

In the initial submittal of WCAP-17184-P, Revision 0, the staff found that the applicant failed to address the DAS setpoint methodology. GDC 13, **"**Instrumentation and Control," requires, among other things, that appropriate controls be provided to maintain variables and systems within prescribed operating ranges. The guidance in BTP 7-19, Section B, Item 3, Positions 1 and 2, acceptance criteria address confirmation that an anticipated operational occurrence (AOO) and postulated accidents are mitigated in the presence of common-cause failure.

In technical report WCAP 17184-P, Revision 0, the applicant did not identify how the DAS actuation setpoints and timing delays would be established. DAS must be able to perform its functions to ensure the potential release of radioactive material for postulated accidents and anticipated operational occurrences fall within acceptable limits in the event of a software common-cause failure of the safety-related protection system. The staff issued RAI-SRP7.8-DAS-02 requesting the applicant to describe the DAS setpoint methodology. To address this RAI, the applicant provided technical report WCAP-17184-P, Revision 1, to add the DAS setpoint methodology description as a new appendix to this technical report. After reviewing the DAS setpoint methodology description, the staff found that the DAS allowances for automatic actuation signals, "Containment Temperature High" and "Pressurizer Water Level Low" are outside of the typical ratio of 1.15**σ** /2**σ**. The staff issued RAI-SRP7.8-DAS-10 requesting the applicant to provide the design basis to support the deviation. In response to this RAI, the applicant proposed a revision to WCAP-17184-P in which it described why the DAS channel statistical allowances for "Containment Temperature High" and "Pressurizer Water Level Low" do not conform to the typical ratio of 1.15σ/2σ when comparing a 75% probability/75% confidence level to 95% probability/95% confidence level for determination of the random and independent terms of the square-root-sum-of-the-squares calculation. Additionally, the applicant also provided a justification for the use of a 75% probability/75% confidence level. After reviewing the revised report, the staff found that the applicant adequately addressed the DAS setpoint methodology and found it acceptable. Therefore, the staff finds the responses to RAI-SRP7.8-DAS-02 and RAI-SRP7.8-DAS-10 acceptable. The staff created **CI-SRP7.8-ICE-02** to track the revision to WCAP 17184-P.

In AP1000 DCD, Revision 17, the applicant changed the microprocessor-based implementation of the DAS to be a special purpose logic processor-based system. This special purpose logic processor-based DAS is further described as a Field Programmable Gate Array (FPGA) digital platform-based system in technical report WCAP 17184-P. The applicant also made changes to use the FPGA technology for the Component Interface Module (CIM) in the safety-related PMS in WCAP 17179-P, "AP1000 Component Interface Module Technical Report" and APP-GW-GLR-071 (WCAP 16775-P), "AP1000 Protection and Safety Monitoring System Architectural Technical Report." According to the above reports, the CIM and DAS systems will be designed and manufactured by the same company at a common design and manufacturing facility. 10 CFR Part 50, Appendix A, GDC 22, "Protection System Independence," requires, among other things, 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. BTP 7-19 provides guidance for evaluating an applicant's D3 assessment to ensure conformance with the NRC position on D3 for digital I&C systems. NUREG/CR-6303, "Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems"

provides diversity analysis methods and strategies to demonstrate that adequate and sufficient diversity should be included within the design. The staff found that the applicant did not provide design descriptions that can demonstrate adequate and sufficient diversity between the DAS and CIM systems in accordance with the guidance listed above. Hence, the staff issued RAI-SRP7.8-DAS-04 requesting the applicant to describe in detail how the DAS equipment (i.e., hardware, software) will be diverse from the safety-related CIM in PMS. The staff also issued another RAI-SRP7.8-DAS-05 requiring the applicant to identify the criteria, practices, and processes that will ensure adequate diversity in the development of the CIM and the DAS at the common design and manufacturing facility, including the diversity with respect to human, software, and equipment diversity.

In response to the above RAIs, the applicant states, in part, that diversity is a principle in instrumentation of sensing different variables, using different technology, using different logic or algorithm, or using different actuation means to provide different ways of responding to postulated plant conditions. The applicant also revised WCAP 15775, the AP1000 Instrumentation and Control Defense-in-Depth and Diversity Report, to Revision 4 to address the specific requirement of diversity between CIM and DAS. The applicant demonstrated in Section 2.11 of Technical Report WCAP 17179-P, draft Revision 2, and Section 9 of Technical Report WCAP 17184-P, draft Revision 2, how the requirements of diversity are met between CIM and DAS. For example, for the human diversity, the applicant states in the two technical reports that different designers are used for the CIM and DAS designs. In addition, the different design teams and different test teams will be used to test the CIM and DAS designs. In order to achieve the software diversity between the DAS and PMS (i.e. CIM), the applicant will use different algorithms, logic, program architecture, executable operating system and executable software/logic. The staff concludes that the applicant has provided sufficient information demonstrating conformance with regulatory policies and criteria concerning diversity. The AP1000 DCD Tier 1 and Tier 2 will also be updated accordingly to address the software diversity. Therefore, the staff finds the responses to RAI-SRP7.8-DAS-04 and RAI-SRP7.8-DAS-05 acceptable and the commitments to modify the technical reports will be tracked as **CI-SRP7.8-ICE-03**.

The staff found inconsistencies between Chapter 7 of the AP1000 DCD, Tier 2, Revision 17 and WCAP-17184-P, Revision 1, regarding DAS manual actuations. 10 CFR 52.47(a)(2) requires that an application must contain a sufficient description and analysis of the structures, systems, and components of the facility, with emphasis upon performance requirements, the bases, with technical justification therefore, upon which these requirements have been established, and the evaluations required to show that safety functions will be accomplished. The description shall be sufficient to permit understanding of the system designs and their relationship to the safety evaluation. The design information provided for the design basis items, taken alone and in combination, should have one and only one interpretation. Therefore, the staff issued RAI-SRP7.8-DAS-06 to request the applicant to provide correct and unambiguous design descriptions for the list of DAS manual actuations. The applicant clarified that the list in the AP1000 DCD is all-inclusive of any manual actuation performed by DAS. The tripping of the reactor coolant pumps is only done in conjunction with the core makeup tank actuation and therefore not separately listed in the DCD. The list in Section 2.3 of WCAP-17184-P, Revision 1, is the list of manual actuations that are cited in the PRA for enabling AP1000 to meet its Large Release Frequency (LRF) goal for beyond design basis events. Therefore, this list would be different from the list in the DCD because not all of the DAS manual actuations are needed to meet the LRF goal for beyond design basis events. Table B-1 in WCAP-17184-P is also not intended to be a complete list of all of the manual actuations. This table is modified to only

include those manual actuations that do not have automatic DAS actuations. To incorporate the above clarification, the applicant proposed a revision to WCAP-17184-P, which the staff found acceptable. Therefore, the staff finds the response to RAI-SRP7.8-DAS-06 acceptable and opened **CI-SRP7.8-ICE-04** to track the proposed revision to WCAP-17184-P.

The staff found Appendix B, Table B-1, in WCAP 17184-P, Revision 1, includes the manual actuation of the hydrogen control system or igniters, but it is not credited in Section 2.3 of WCAP-17184-P for the DAS manual operator action and/or a DAS automatic function. The applicant did not provide a technical basis for this non-credited DAS manual operator action. BTP 7-19 states where operator action is cited as the diverse means for response to an event, the applicant should demonstrate that adequate information (indication) and sufficient time is available for operator action. The staff's review of Section 10.2.1.1 in WCAP-17184-P, Revision 1, determined that the stated design descriptions do not provide an explanation of how the manual action is used in the DAS design beyond listing the manual actions. From the PRA evaluation the staff found that there is a 19-minute window for accomplishing this action. The applicant failed to provide a clear technical basis that will permit sufficient understanding of credited DAS manual actuations and their conformance with the applicable regulatory requirements. The staff issued RAI-SRP7.8-DAS-07 to request the applicant to provide the technical basis for the hydrogen igniter manual action as a non-credited DAS function.

In response, the applicant states, in part, that for this manual actuation of the hydrogen control system or igniters, PRA analysis techniques show acceptable results even if the act of manually actuating the hydrogen igniters is not accomplished (operator fails to act with 100% certainty). For this reason, manual actuation of the hydrogen igniters is not a credited manual operator action nor is it required (or credited) for hydrogen igniters to operate automatically. The 19-minute window as described in the PRA analysis is for a beyond design basis event. The PRA analysis was used to provide insights into this particular scenario. Hydrogen igniters were added to the AP1000 design even though they are not credited in the design basis. In response to this RAI, the applicant proposed a revision to technical report WCAP-17184-P to provide the reasoning behind installation of hydrogen igniters. After evaluating the response, the staff found that the applicant's response to this RAI is acceptable. Therefore, the staff finds the response to RAI-SRP7.8-DAS-07 acceptable and opened **CI-SRP7.8-ICE-05** will track the revision to WCAP-17184-P.

In Appendix B, Table B-1, in technical report APP-GW-GLR-145, Revision 1, the staff found that there is a 20-minute window for accomplishing the manual actuation of the Automatic Depressurization System (ADS). However, after reviewing the above technical report, the staff found that the stated design descriptions do not provide an explanation of how the ADS manual actions are used in the DAS design beyond listing them. According to BTP 7-19, the applicant should demonstrate that adequate information (indication) and sufficient time is available for manual operator actions. The staff issued RAI-SRP7.8-DAS-08 to request the applicant to provide clear technical basis description in the technical report that permits sufficient understanding of ADS manual operator action as credited DAS manual actuations and the basis for why the 20-minute window is sufficient for completing the ADS manual actuation. In response to this RAI, the applicant proposed a revision to technical report WCAP 17184-P to provide clarification for this manual actuation of ADS.

The DAS credits manual actions to depressurize the RCS during anticipated operational occurrences or postulated accidents following a software common-cause failure in the protection system. Branch Technical Position HICB-19, "Guidance for Evaluation of Defense-in-

Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems," Revision 4, states that where operator action is cited as the diverse means for response to an event, the applicant should demonstrate that adequate information (indication) and sufficient time is available for operator action. The staff reviews acceptability of these manual actions using guidance in DI&C-ISG-05, "Highly-integrated Control Rooms – Human Factors Issues" (ISG-5).

Manual actions that can be initiated from DAS are listed in the following places:

- AP1000 Design Certification, Revision 17, Tier 2, Section 7.7.1.11
- WCAP-17184-P (APP-GW-GLR-145), "AP1000™ Diverse Actuation System Planning and Functional Design Summary Technical Report" , Revision 1, Section 2.3
- WCAP-17184-P, Revision 1, Appendix B, Table B-1

The manual actions listed in WCAP-17184-P, Section 2.3, were not consistent with the other two lists. The staff initiated RAI-SRP7.8-DAS-06 to resolve the differences. In the Westinghouse response of June 22, 2010, Westinghouse explained that the Design Certification described all manual actions that can be performed by DAS. WCAP-17184-P, Section 2.3, described the manual actions that are cited in the PRA for enabling AP1000 to meet its LRF goal for beyond design basis events. The lists are different because not all of the DAS manual actions are needed to meet the LRF goal for beyond design basis events. Appendix B, Table B-1, provided a list matching the DCD. Westinghouse will modify Table B-1 to include only those manual actions that do not have corresponding automatic DAS actuations. For these manual actions, Westinghouse provided specific information describing whether the manual action is credited as part of the DAS response to a common cause failure or whether the manual action is part of the defense in depth strategy for severe accident management thus providing a clearer communication of why the manual actions are included in the DAS design. These changes were provided in Revision 2 of WCAP-17184-P. The staff found the changes acceptable**.** **CI-SRP7.8-ICE-04** has been established to verify the proposed changes are implemented in the next revision of WCAP-17184-P.

Appendix B of WCAP-17184-P now lists the following 4 manual actions:

Manual action 1: *Manual initiation of IRWST recirculation/IRWST drain for in vessel retention support*

The DAS provides this capability as part of the defense in depth strategy for severe accident management. It is an action needed to address anticipated operational occurrences or postulated accidents following common-cause failures in the protection systems. Therefore the regulatory guidance in BTP 7-19 and ISG-05 do apply.

Manual action 2: *Manual initiation of the Hydrogen control system*

The DAS cabinet presents a convenient and reliable location for the manual hydrogen control system switches because it is in the main control room and has a diverse battery-backed power supply. It is not an action needed to address anticipated operational occurrences or postulated accidents following common-cause failures in the protection systems. Therefore the regulatory guidance in BTP 7-19 and ISG-05 does not apply.

Manual action 3: Manual Depressurization of the RCS

This action is credited in the DAS response to a common cause failure. In summary, ISG-05 states that an analysis must be completed that demonstrates:

- The time available to perform the required manual actions is greater than the time required for the operator(s) to perform the actions.

- The operator(s) can perform the actions correctly and reliably in the time available

No information was provided to the staff to explain how this guidance was addressed. The staff initiated RAI-SRP7.8-DAS-8 requesting this information. In the Westinghouse response of June 22, 2010 (DCP NRC 002927), Westinghouse committed to include a new ITAAC in Tier 1 Chapter 2, Section 2.5.1, Diverse Actuation System, Table 2.5.1-4. This commitment was provided in the response to RAI-SRP7.8-DAS-12 and reads as follows:

Table 2.5.1-4
Inspections, Tests, Analyses, and Acceptance Criteria

Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
5. The DAS manual actuation of ADS, IRWST injection, and containment recirculation can be executed correctly and reliably.	An evaluation to confirm that the operator actions can be performed within the specified times.	b) A report exists and concludes that DAS manual operator action verification was conducted.

The staff finds the proposed ITAAC to be an acceptable way to develop the information needed to address the regulatory guidance in ISG-05, provided the commitment is also included as a separate "Design Description" in the text-based portion of Section 2.5.1 . **CI-SRP7.8-ICE-06** has been established to verify the proposed ITAAC is included in Revision 18 of the DCD.

The staff notes that APP-GW-GL-011, "AP1000 Identification of Critical Human Actions and Risk Important Tasks", Revision 0, Table 3-1 and 3-2 identify risk-important human actions. Table 3-2, Basic Event ID: AND-MAN01 identifies failure to actuate the ADS for RCS depressurization as recovery from failure of automatic actuation or for manual ADS actuation as a risk-important human action. As such this manual action is already included in the HFE program described in Chapter 18 of this report. In summary, that program includes all risk important human actions as priority items in the task analysis, the Human-System Interface (HSI) design, the HFE design verification and validation, and human performance monitoring elements. By being included within the HFE program the regulatory guidance provided in ISG-05 is either met or exceeded.

Manual action 4: Manual initiation of IRWST gravity injection.

The DAS provides this capability as part of the defense-in-depth strategy for severe accident management. It is an action needed to address anticipated operational occurrences or postulated accidents following common-cause failures in the protection systems. Therefore, the regulatory guidance in BTP 7-19 and ISG-05 do apply.

Operator manual actions credited within the DAS design have not yet been evaluated to verify they are viable. The applicant provided an acceptable DAS ITAAC in Section 2.5.1 of Tier 1, Chapter 2 information that will track completion of this evaluation. A similar evaluation is required within the HFE program described in DCD Chapter 18. Together or independently these commitments will ensure the regulatory guidance in BTP 7-19 and ISG-05 is implemented. This in turn will provide reasonable assurance that the operator manual actions to depressurize the RCS are an effective element of the DAS design for coping with anticipated operational occurrences or postulated accidents following common-cause failures in the protection systems.

Additionally, by the applicant adding a new ITAAC item to Table 2.5.1-4 of AP1000 DCD Tier 1 to address the design commitment and ITAAC for DAS manual actuations, the staff found that the applicant's response to this RAI is acceptable. Therefore, the staff considered that RAI-SRP7.8-DAS-08 is closed, but it will be tracked as confirmatory item **CI-SRP7.8-ICE-06** listed above.

The staff found in Appendix B, Table B-1, in technical report APPP-GW-GLR-145/ WCAP 17184-P, Revision 1 that the applicant includes In-containment Refueling Water Storage Tank (IRWST) gravity injection as an DAS manual actuation. From the PRA evaluation in the table, there is a 20-minute window for accomplishing this manual action. However, the applicant failed to provide the technical basis for the sufficiency of this manual operator action. The applicant should demonstrate that adequate information and sufficient time is available for manual operator actions based on the guidance in BTP 7-19. Therefore, the staff issued RAI-SRP7.8-DAS-09 to request the applicant to identify a clear technical basis description that permits sufficient understanding of this credited DAS manual actuation and its basis for why the 20-minute window is sufficient for this DAS manual action. In response to this RAI, the applicant states, in part, that for this particular scenario, PRA analysis techniques show acceptable results even if the act of manually actuating IRWST gravity injection is not accomplished (operator fails to act with 100% certainty). For this reason, manual actuation of IRWST gravity injection is not a credited manual operator action nor is it required (or credited) for automatic operation. The 20-minute window as described in the PRA analysis is for a beyond design basis event. The PRA analysis was used to provide insights into this particular scenario. The capability to manually actuate IRWST gravity injection from DAS was added to the AP1000 design out of caution, even though it is not credited in the design basis. The applicant proposed to revise WCAP-17184-P to Revision 2 to provide further clarification of the reasoning behind the manual initiation of IRWST gravity injection. The applicant committed to add a new ITAAC item to Table 2.5.1-4 of AP1000 DCD Tier 1 to address the design commitment and ITAAC for DAS manual actuations, which include the manual actuation of the IRWST gravity injection. The staff found that the applicant's response and changes related to this RAI are acceptable. The staff finds the response to RAI-SRP7.8-DAS-09 acceptable and it will be tracked as **CI-SRP7.8-ICE-07**.

In WCAP-17184-P, Revision 1, which Westinghouse submitted to justify the removal of ITAAC Items 4a and 4b from AP1000 DCD Tier 1, Table 2.5.1-4, the staff found that the applicant addressed the requirements of cyber security. The requirements of cyber security was also addressed in technical report WCAP 17184-P, Revision 1. However, the staff's position related to cyber security issues is that cyber security is addressed by 10 CFR 73.54 and is not a 10 CFR Part 50 review item. As such, the reference to cyber security in the above technical reports should be modified and/or replaced with a docketed technical report describing the SDOE in which the applicant chooses to develop its software-based and programmable

technology based DAS and CIM, paying particular attention to IEEE 603-1991, Clauses 5.3, 5.6.3, and 5.9. The staff issued RAI-SRP7.8-DAS-11 which requested the applicant remove the discussion of cyber security from the two technical reports. In response to this RAI, the applicant deleted the mention of cyber security requirements in the revised WCAP 17184-P and WCAP-17179-P. The applicant also made corresponding changes to the AP1000 DCD Tier 2, Table 1.6-1 and Section 7.1 to address the requirements of this RAI. The staff found the response to RAI-SRP7.8-DAS-11 acceptable and opened **CI-SRP7.8-ICE-08** to track the changes described above. In addition, the applicant submitted a new, separate technical report APP-GW-J0R-012, Revision 0, "AP1000 Protection and Safety Monitoring System (PMS) Computer Security Plan" to address the secure development and operational environment for the AP1000 PMS. Section 7.9 of this FSER supplement provides evaluation of this new technical report.

The staff found that the following issues in WCAP-17184-P, Revision 1, need to be addressed by the applicant:

- Section 6.1.2.2 references the Wolf Creek license amendment request regarding self-test features of the DAS. However, the Wolf Creek license amendment request is not part of the AP1000 DCD licensing basis. Therefore, self-test features should be identified in the technical report for the AP1000 DAS.

- The statement in Section 8.1 currently states that the "two-out-of-two logic … lends itself to reliability." However, this configuration is less reliable than a single train configuration, although the PRA-based DAS design and two-out-of-two actuation logic were approved in the certified AP1000 DCD, Revision 15, and the applicant has not made changes to the DAS logic in the applicant's DCA application. Hence, the above statement is not accurate and should be modified to reflect the approved DAS design feature.

- Section 8.1 states that "The use of FPGAs results in a hardware-based design that is not subject to software common cause failures. The only software involved in the process is that used to burn-in the required logic design into the FPGA." These two statements are inaccurate and should be removed because the FPGA-based systems are developed with software tools and can have programming errors similar to microprocessor-based digital systems, although FPGA-based systems do not run any system or application software during operation. Therefore, evaluation for common cause failures within FPGA development process and software programming shall be conducted. A high quality and well documented life-cycle design process should be provided according to BTP 7-14, "Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems."

During the review of technical report WCAP-17184-P, Revision 1, the staff identified the above issues and issued RAI-SRP7.8-DAS-13 to request the applicant to correct those statements for technical and regulatory accuracy. In response to this RAI, the applicant proposed to modify technical report WCAP-17184-P to Revision 2 to make the necessary corrections. After reviewing the draft revised technical report, the staff found that the applicant's response is acceptable. The staff finds the response to RAI-SRP7.8-DAS-13 acceptable and opened **CI-SRP7.8-ICE-09** to track the committed revisions.

The staff finds the DAS is properly credited for providing a diverse backup to the safety-related protection system; however, the ATWS mitigation systems actuation circuitry (AMSAC) system should not have been credited with providing diverse protection upon a postulated common-cause failure (CCF) of the safety-related PMS. During the evaluation of the changes made to the certified AP1000 DCD, Revision 15 for the DAS, the staff found that the applicant provided ambiguous descriptions for the DAS circuitry and the AMSAC. 10 CFR 52.47(a)(2) requires, in part, a description of structures, systems, and components to be of sufficient detail to permit understanding of the systems designs. Section 15.8 of the AP1000 DCD, Revision 17, states that the DAS provides AMSAC functions. It also states that for Westinghouse plants the ATWS rule (10 CFR 50.62) requires the installation of AMSAC, which consists of circuitry separate from the reactor protection system to trip the turbine and initiate decay heat removal. The applicant failed to provide a description of the AMSAC or the relation between the DAS and the AMSAC system in Section 7.7 of the AP1000 DCD Tier 2, Revision 17. The applicant also failed to clearly describe if the DAS circuitry and the AMSAC system circuitry are the same system or if they are separate systems. The staff issued RAI-SRP7.8-DAS-01 to request the applicant to clarify the design descriptions for DAS and AMSAC. In response, the applicant states that for Westinghouse plants the ATWS rule requires the installation of equipment that is diverse from the reactor protection system to automatically trip the turbine and initiate decay heat removal. This equipment must be designed to perform its function in a reliable manner and be independent from sensor output to final actuation device from the existing reactor protection system. The AP1000 is designed with a DAS, which provides the functions required by the ATWS rule. In response to this RAI, the applicant also provided a markup for Section 15.8 of the AP1000 DCD to clarify the description of DAS and AMSAC. The staff found the response to RAI-SRP7.8-DAS-01 acceptable and opened **CI-SRP7.8-ICE-10** to track the committed revisions.

When evaluating the changes to the certified AP1000 DCD, Revision 15, the staff issued RAI-SRP-7.8-DAS-03 requesting the applicant to identify design descriptions that demonstrate how the 2-out-of-2 (2oo2) DAS actuation logic would meet the applicable regulatory criteria. 10 CFR 50.62 requires ATWS mitigation equipment to perform its functions in a reliable manner. The guidance of BTP 7-19, Point 3, on D3 states that 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. The applicant states in Revision 17 of the AP1000 DCD, Tier 2, Section 16.3-2 that, “when a required channel is unavailable, the automatic DAS function is unavailable.”

In response, the applicant explained that there are two actuation logic modes, automatic and manual. The automatic actuation logic mode functions to logically combine the automatic signals from the two redundant automatic subsystems in a 2oo2 basis. The combined signal operates a power switch with an output drive capability that is compatible, in voltage and current capacity, with the requirements of the final actuation devices. The 2oo2 logic is implemented by connecting the outputs in series. The manual actuation mode operates in parallel to independently actuate the final devices. Actuation signals are output to the loads in the form of normally de-energized, energize-to-actuate signals. The normally de-energized output state, along with the dual, 2oo2 redundancy reduces the probability of inadvertent actuation. The staff found the applicant’s response to RAI-SRP-7.8-DAS-03 acceptable.

The 2oo2 DAS actuation logic was included in the approved DAS design in the certified AP1000 DCD, Revision 15. Specifically, 10 CFR 50.62 requires that ATWS mitigation equipment must be design to perform its function in a reliable manner. As described in Section 15.8.3 of the AP1000 DCD, Tier 2, Revision 18, the AP1000 is equipped with a DAS, which provides the functions required by the ATWS rule (10 CFR 50.62). The ATWS core damage frequency for the AP1000 is below the SECY-83-293 goal of 10^{-5} per reactor year. In NUREG-1793, the staff reviewed and approved the AP1000's basis for meeting the ATWS core damage frequency goal.

Reliability of digital systems can be achieved through various means including redundancy, fault detection and management, quality of design, and use of reliable components. Reliability can be defined as the likelihood that a given component or system will be properly functioning when needed, as measured over a given period of time. Reliability, in itself, does not account for any repair actions that may take place. Availability can be defined as the percentage of time that a given system will be functioning as required. In other words, availability is the probability that a system is not failed or undergoing a repair action when it needs to be used.

The AP1000 DAS design addresses reliability from a design/component approach and by fault detection and management. From a design/component reliability approach, Section 8.1 of WCAP-17184-P states that a failure modes and effects analysis, mean-time-between-failure analysis, and a reliability block diagram analysis will be performed on the DAS at the component level. Since the DAS detailed design is not complete at the design certification stage, nor required to be complete per 10 CFR 52.47, those analyses were not part of the staff's review. However, sufficient criteria in the AP1000 DCD are available to guide the detailed design analysis, such as the use of MIL-HDBK-217F for component failures and hardware reliability analysis. From a fault detection/management approach, Section 6.1.2.2.1 of WCAP-17184-P states that the DAS will include self-diagnostic features to identify failures of the processor and supporting circuitry. The self-diagnostic features provide real-time indication to operators of a DAS failure, limiting the fault exposure time and improving DAS availability.

As part of the determination for meeting the ATWS core damage frequency goal, the AP1000 PRA assumed an availability goal for DAS, as described in Section 8.2 of WCAP-17184-P. As committed in WCAP-17184-P, the detailed reliability analysis performed on the DAS would be consistent with the availability goal. Specifically, the reliability analysis will determine an expected failure rate based on hardware failures. Both the failure rate and expected repair time will be calculated and compared to the availability goal for consistency. By utilizing self-diagnostic features, the operators are given real-time indication of a DAS failure, which will allows maintenance to be performed in a timely manner. By using the self-diagnostic features, the fault exposure time is reduced on the DAS, thus improving DAS availability as it relates to latent, undetected faults.

Given the commitments in WCAP-17814-P regarding the reliability analysis and self-diagnostics, the staff finds that the DAS will operate reliably. DAS may be taken out of service

for maintenance, or be subjected to a failure, but would meet the committed availability target, which is part of the overall basis for meeting the ATWS core damage frequency goal. NRC regulations such as 10 CFR 50.65, "Requirements for monitoring the effectiveness of maintenance at nuclear power plants," would provide verification that the availability goal is being achieved while the plant is in operation.

As part of the AP1000 DCD, Tier 2, Revision 18, design changes (DCN 63), Westinghouse proposed the addition of a new DAS High Hot Leg Temperature Reactor and Turbine Trip. The reason for the design change is that in the original DAS design, which is modeled in PRA, a reactor trip and turbine trip should occur for ATWS sequences with main feedwater available. Because feedwater is still available, the DAS Low Steam Generator Water Level signal will not initiate the reactor or turbine trip. The DAS High Hot Leg Temperature signal is needed to perform this function.

The staff evaluated ATWS for the AP1000 as documented in the FSER for Rev 15 (NUREG-1793). For that evaluation, the applicant analyzed a number of cases that included scenarios with and without normal feedwater operating. The most limiting case was confirmed to be the loss of normal feedwater event with turbine bypass operable, resulting in the highest RCS pressure. Addition of the hot leg temperature DAS trip would not alter that conclusion. The additional trip provides additional margin for the limiting case, and hence, is a conservative change that is acceptable for ATWS response. With respect to DAS reliability, quality, qualification, and independence from the primary protection system, the staff finds that the addition of a new function would not impact any of these design characteristics. Specifically, the function can be added into the current DAS architecture without changes to the DAS architecture described in the certified AP1000 design. Therefore, the staff finds the new DAS High Hot Leg Temperature Reactor and Turbine trip meets the requirements of 10 CFR 50.62.

7.8.3 Evaluation Findings and Conclusions

After reviewing WCAP-17184-P, Revision 2; technical report APP-GW-GLN-022, Revision 1; WCAP-15775, Revision 4; changes to AP1000 DCD, Tier 1 and Tier 2; and responses to related RAIs, the staff concludes that the applicant provides sufficient information to support the changes made to the DAS in Revision 17 of the AP1000 DCD.

The staff found the AP1000 DCD, Revision 17, meets the requirements of 10 CFR 50.62 and 10 CFR Part 50, Appendix A, GDC 22. The proposed changes between Revisions 15 and 17 of the AP1000 DCD did not affect the design commitments regarding an anticipated transient without scram. The staff also found that the applicant provided sufficient information to support the removal of the two completed lifecycle phases and other changes for DAS. Therefore, the staff concludes the changes the applicant made to the DAS design meet regulatory requirements and criteria.

7.9 Data Communication Systems

7.9.1 System Description

The AP1000 I&C systems consist of the PMS safety system, which contains four independent divisions, four non-safety systems, the plant control system (PLS), data display and processing system (DDS), main turbine control and diagnostic system, and special monitoring system (SMS)), and two systems that perform both safety and non-safety functions (in-core instrumentation system (IIS) and operations and control centers system (OCS)). AP1000 DCD, Section 7.1.2.8, references WCAP-16675, Revision 2 (ADAMS Accession Number ML091600142), for AP1000 data communications systems design. This TR provides an overview of the design of data communications within the PMS and communications between the PMS and non-safety systems. Section 3 of WCAP-16675 references WCAP-16674, Revision 2 (ADAMS Accession Numbers ML100050344), for a more detailed description of data communications in the AP1000 I&C systems design.

WCAP-16675, as supplemented by WCAP-16674, describes the use of the Common Q platform for data communications within the internal PMS safety functions (nuclear instrumentation system – NIS, QDPS, RTS, ESFAS, and the component logic system) and the safety portions of the IIS and OCS. This TR also describes the use of the Emerson Ovation® Network for data communications within the non-safety systems, the non-safety portions of IIS and OCS, and outputs from the safety system data (via the Advant-Ovation Interface (AOI) gateways).

7.9.2 Communication within Safety Systems

7.9.2.1 Common Q Communications Subsystems

The NRC evaluated WCAP-16097, "Common Qualified Platform Topical Report" (ADAMS Accession Numbers ML031830959), and issued safety evaluations approving the Common Q platform on August 11, 2000; June 22, 2001; and April 2, 2003. WCAP-16097 described the communications subsystems of the Common Q system. The SER for the Common Q platform (ADAMS Accession Numbers ML003740165) provided an evaluation of the following three types of communications subsystems:

(1) AF100 bus communication for intrachannel communications and a separate AF100 bus for interchannel communications in the DDS

(2) high-speed link (HSL) serial communications for interchannel communications

(3) external communications for communications between the Common Q platform and external computer systems

The Common Q platform topical report SER concluded that these three types of communications subsystems met the requirements of IEEE Std. 603-1991, as supplemented by IEEE Std. 7-4.3.2-1993. The staff's review of these communications subsystems supplements the conclusions made in the SER of the Common Q platform topical report. Specifically, the staff evaluated the application of these communications subsystems for data communications within the AP1000 I&C systems. Sections 7.9.2.2, 7.9.2.3, and 7.9.3 of this FSER supplement document the evaluation of the application of these communications subsystems to the PMS design.

7.9.2.2 Intradivisional Communication via the AF100 Bus

7.9.2.2.1 Functional Description of the AF100 Bus

Section 3 of WCAP-16775 describes the use of the AF100 bus for intradivisional communications between the AC160 controllers and the safety and QDPS display systems within the same division. This section states that, within each PMS division, the internal functions and the safety portions of both IIS and the OCS are integrated using an intradivisional AF100 bus.

Specifically, the AF100 bus is used to allow the various AC160 controllers and FPDS within a division to exchange information for maintenance, test, diagnostic, communication (to the non-safety system), display, and manual control. The majority of the dataflow is from the AC160 controllers to the FPDS (for display and for communication to the non-safety system). Therefore, the AF100 bus is used to integrate information exchange among the AC160 controllers performing the ESFAS and reactor trip functions and the FPDS. The AF100 is not in the sensor-to-reactor trip path or sensor-to-ESFAS-actuation path. The ESFAS and reactor trip functions do not require information from each other to perform their safety functions.

The AF100 bus is a deterministic communication bus with a transmission rate of 1.5 megabit (Mbit)/second or faster. Section 4.1.2 of WCAP-16674 describes the two types of data communication that occur within the AF100 bus. The real-time data distribution communication provides a scheduled periodic broadcast of real-time data (process data transfer) pertaining to the plant processes. The general purpose communication provides a periodic exchange of data (message transfer) for other purposes, such as system operation, diagnostics, and maintenance. As described in Section 3.1 of WCAP-16675, message transfer does not influence process data transfer in any way. This is accomplished by reserving bandwidth for process data transfer and using the remaining bandwidth for message transfers. In addition, Section 3.1.1 of WCAP-16675 describes how the application program configuration tool is used to limit the maximum number of process data transfer packets that can be transferred over the AF100 bus to prevent overloading it. Process data packets are transferred with fixed packet size and cycle time to ensure deterministic communications.

Section 2.2.6.2 of WCAP-16675 states that software changes can be accomplished in the AC160 in two ways. One way is to program the AC160 over the AF100 bus. Even though this network and the only programming source (the MTP) are totally contained within a division of the PMS, this mode of programming is prevented. This is accomplished by using the AC160 Function Chart Builder tool to configure the equipment to not accept AF100 bus programming. The other way to load software into the AC160 is by a serial connection between the division's MTP and the AC160. Within a division, a separate cable is permanently routed from the maintenance and test cabinet (MTC) to each cabinet containing an AC160 processor module. This configuration allows for software loading to any processor module within a division from the MTP. The software loading cable is normally disconnected on each end. To perform a software update, the cable (coming from the cabinet containing the target processor module) in the MTC is connected to the MTP. The opposite end of the software loading cable is connected to the target AC160 processor module and the software update is performed from the MTP.

Section 3.1 of WCAP-16675 states that an AF100 bus is totally contained within each division of the safety system. The physical extent of each AF100 bus is limited to its corresponding I&C equipment room, the MCR, and the raceways between the two. On-site access is not provided in any other location. Offsite access to the four PMS intradivisional Common Q networks is not available. This section also states that, within the PMS, security is maintained, since the ability to remotely program the AC160 controllers and safety and QDPS display systems over the

AF100 bus has been disabled in the PMS. Access to the PMS intradivisional Common Q network is only available from the MCR. Access is not available in any of the other operation and control centers.

7.9.2.2.2 Technical Evaluation of the AF100 Bus

The staff finds the use of the Common Q AF100 bus acceptable for intradivisional communication within each PMS division. The AF100 bus only serves one division in each PMS division, with no direct connections to other divisions or non-safety systems. Data from other divisions and non-safety systems can only reside on the AF100 bus via the other components within the same division (e.g., integrated communications processor (ICP) through HSLs). In such cases, electrical and communications isolation is provided by the fiber-optic connection between the given component and other divisions, and the communications processor of that particular component, respectively. IEEE Std. 603-1991, Clause 5.6.1, requires independence between redundant portions of safety systems to the degree necessary to retain the capability to accomplish the safety function during and following any design-basis event requiring that safety function. In addition, IEEE Std. 603-1991, Clause 5.6.3, "Independence Between Safety Systems and Other Systems," requires independence between safety and non-safety systems such that credible failures in, and consequential actions by, non-safety systems shall not prevent the safety system from accomplishing its intended safety function. Based on the communications and electrical isolation present in the Common Q AF100 bus, the staff finds the independence requirements of IEEE Std. 603-1991, Clauses 5.6.1 and 5.6.3, are met.

The staff evaluated the access controls to the AF100 bus against the requirements of IEEE Std. 603-1991, Clause 5.9, as clarified by the guidance provided in DI&C ISG #4-HICRc. IEEE Std. 603-1991, Clause 5.9, requires the design to permit the administrative control of access to safety-system equipment. DI&C ISG #4-HICRc, Section 1, Point 10, states that safety division software should be protected from alteration while the safety division is in operation. Hardwired interlocks or physical disconnection of maintenance and monitoring equipment should prevent online changes to safety-system software. The staff has evaluated the access controls described in Section 3.1 of WCAP-16675, as discussed in the above section.

The staff finds the use of the AC160 Function Chart Builder tool to configure the equipment so that it does not accept programming over the AF100 bus to be acceptable in meeting the requirements of IEEE Std. 603-1991, Clause 5.9, by addressing Section 1, Point 10, of DI&C ISG #4-HICRc regarding restrictions to the online programmability of safety equipment. In addition, the staff finds that the access control provided for programming the AC160 controller over the serial software loading cable to the equipment provides additional assurance that unauthorized software modifications to the AC160 controller and to the safety and QDPS displays are prevented. Specifically, the staff finds the physical disconnection of the software load cable between scheduled software updates meets Section 1, Point 10, of DI&C ISG #4-HICRc.

The staff evaluated how the design of the AF100 bus addressed the system integrity requirements of IEEE Std. 603-1991, Clause 5.5, which requires in part that safety systems be designed to accomplish their safety functions under the full range of applicable conditions enumerated in the design basis. Branch Technical Position (BTP) 7-21, "Guidance on Digital Computer Real-Time Performance" states that risky design practices such as non-deterministic data communications, non-deterministic computation, use of interrupts, multitasking, dynamic

scheduling, and event-driven design should be avoided. Based on the deterministic nature of the process data transfer on the AF100 bus, as described in Section 3.1 of WCAP-16675, and the limitations on maximum allowed process data transfer packets, the staff finds that the design of the AF100 bus adequately addresses the deterministic communications criteria provided in BTP 7-21 to meet IEEE Std. 603-1991, Clause 5.5.

7.9.2.3 Interdivisional and Intradivisional Communication via the High-Speed Link

7.9.2.3.1 Functional Description of the High-Speed Link

Section 3 of WCAP-16775 describes the use of the HSL for interdivisional and intradivisional communication within the PMS. This section states that the PMS uses HSLs, which are point-to-point, to communicate certain data within and across PMS divisions. The HSL is a serial RS 422 link using High-level Datalink Control protocol with a 3.1 M_{bits}/second transfer rate. The HSL is used for planned data exchanges of predefined data packets between two Common Q processor modules in the sensor-to-reactor trip path or sensor-to-ESFAS actuation path.

As stated in Section 6.2.1 of the SER to WCAP-16097, the PM646 function processor is divided into two sections, the Process section and the Communications section. The communications section in the PM646A processor module is used for HSL communications. Each processor module has one independent transmit link (output to two ports) and two independent receive links. The receivers of each HSL are independent and can receive different data independently, in accordance with the guidance of DI&C ISG #4-HICRc. As specified in Section 5.1 of the SER to WCAP-16097, these ports are used with fiber-optic cables for interchannel communications. Section 6.4 of this TR states that the integrity of data transmitted is monitored by using a cyclic redundancy check (CRC). The receiving processor module calculates the CRC of the received data and compares it with CRC bits received with the data. If the CRC comparison fails three consecutive times, the processor module declares the link has failed and reports the failure to the application software, which takes appropriate action. The processing section and the communication section of each PM646A processor module communicate with each other, in accordance with DI&C ISG #4-HICR, such that the communication and function processors operate asynchronously, sharing information only by means of dual-ported memory or some other shared memory resource that is dedicated exclusively to this exchange of information. This allows the two sections to share data between them while preventing either from affecting the operation of the other. The specific implementation, as described in Section 6.2.1 of the SER to WCAP-16097, is proprietary.

Based upon the specification listed in Section 4.1.1.4 of WCAP-16097, to ensure deterministic behavior of the Common Q platform, the measured load of the application programs on a single PM646 processor has to be less than 70 percent. To verify that safety systems meet the response time requirement, WCAP-16097 states that Westinghouse committed to perform a throughput analysis and a response time analysis. This topical report stated that, during the testing phase of the Common Q application, Westinghouse will perform response time tests to validate the design's compliance with both the system response and the display response requirements. In the SER for the WCAP-16097, the staff concluded that the design features, the operation of the AC160 PLC system, and CENP's commitments to perform timing analyses and tests provide sufficient confidence that the AC160 will operate deterministically to meet the recommendations in BTP HICB-21 and is, therefore, acceptable in that regard. However, the staff issued Plant Specific Action Item (PSAI) 6.6 to ensure that timing analysis and validation

tests for applications of Common Qualified Platform system verify that the design satisfies the plant-specific requirements for accuracy and response time presented in the accident analysis in Chapter 15 of the safety analysis report. The resolution of PSAI is documented in NUREG-1793 for the Certified AP1000 Design, which states: "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."

Section 3.2 of WCAP-16675 describes the functional use of the HSL for interdivisional and intradivisional communication within the PMS. Below is a summary of how the HSL is used for data communications between equipment within the PMS.

Bistable Processor Logic to Local Coincidence Logic Communication

The PMS uses the Common Q HSLs to transmit certain data for partial trip, partial actuation, and related status information calculated in the BPL controllers to the LCL controllers. In addition, these serial links are used to transmit voting information between divisions. Fiber-optic cables provide electrical isolation and the communications processor in the PM646 module provides communications isolation.

Local Coincidence Logic to Integrated Logic Processor Communication

The PMS uses Common Q HSLs to transfer ESF system-level actuation and related status information calculated in the LCL controllers to ILPs that actually control the safety components. These links are only used locally within a division.

Integrated Logic Processor Communication to Integrated Communication Processor Communication

The PMS uses Common Q HSLs to transfer data to support the QDPS function and data to support cross-division diagnostics between divisions. Cross-division diagnostics are completed outside the PMS, using outputs from the ICP to the PLS. For communications across divisions of the PMS, fiber-optic media converters and fiber-optic cables provide electrical isolation and the communications processor within each PM646 module provides communications isolation. Section 3.3 of WCAP-16775 states that qualified isolation devices maintain electrical isolation and communications independence between the ICP and the PLS.

Integrated Test Processor

The PMS uses Common Q HSLs to transfer data to the ITP to support testing and monitoring the PMS system. The ITP compares information from within the division via the AF100 bus to information received via HSLs from the other divisions for fault detection. Fiber-optic media converters and fiber-optic cables provide electrical isolation and the communications processor within each PM646 module provides communications isolation.

7.9.2.3.2 Technical Evaluation of the High-Speed Link and PM646 Deterministic Performance

Clause 5.5 of IEEE Std. 603-1998 requires safety systems be designed to accomplish their safety functions under the full range of applicable conditions enumerated in the design basis. In

addition, Clause 4.10 of IEEE Std. 603-1998 requires, as a part of the design basis, identification of the critical points in time or the plant conditions, after the onset of a design basis event.

To meet IEEE Std. 603-1991, Clause 5.5 and Clause 4.10, data communications systems in support of the protection system should demonstrate real-time performance in accordance with SRP Branch Technical Position (BTP) 7-21, "Guidance on Digital Computer Real-Time Performance." SRP BTP 7-21 stipulates that:

1. Time delays within the data communications systems and measurement inaccuracies introduced by the DCS should be considered when reviewing setpoints,

2. Data rates and data bandwidths should be reviewed including impact by environmental extremes, and

3. Sufficient excess capacity margins should be available to accommodate future increases.

In addition, limiting response times should be consistent with safety requirements. Digital computer timing should be consistent with the limiting response times and characteristics of the computer hardware, software, and data communications systems.

As stated above, in the SER for the Common Q Topical Report and NUREG-1793, the staff concluded that the HSL communications and the PM646 processor design is adequate to address the deterministic performance criteria in HICB BTP 7-21 in the Common Q Topical Report, and the resolution of PSAI 6.6 in NUREG-1793. Westinghouse included ITAAC acceptance criteria to verify the PMS response time under maximum CPU loading meets Chapter 15 response time limits. Specifically, Westinghouse committed to modify the acceptance criteria in Item 11 b) the System Integration and Test phase of ITAAC Table 2.5.2-8 in Tier 1, Chapter 2, Section 2.5.2 of the AP1000 DCD to state "Performance of system tests and the documentation of system test results, including a response time test will be performed under maximum CPU loading to demonstrate the PMS can fulfill its response time criteria." The staff finds this proposed update to Item 11 b) of ITAAC Table 2.5.2-8 acceptable. However, based upon the commitment made in an RAI response by Westinghouse to restore all development phases of the PMS under Design Description 11 in the text based portion of Section 2.5.2, listed as CI-SRP7.2-ICE-07 in Section 7.2.5 of this report, the 11b) designator may be altered to another alpha-numeric designator in Revision 18 of the AP1000 DCD. This is **CI-SRP 7.9-ICE-01**.

IEEE Std. 603-1991, Clause 5.6.1, requires independence between redundant portions of safety systems to the degree necessary to retain the capability to accomplish the safety function during and following any design-basis event requiring that safety function. SRP BTP 7-11, "Guidance on Application and Qualification of Isolation Devices," states that fiber-optic cables are acceptable isolation devices. Based on the guidelines in BTP 7-11, the staff finds that optical media converters with optical fiber cabling in the HSL provide adequate electrical isolation. In addition, DI&C ISG #4-HICRc clarifies existing guidance on acceptable methods to meet the communications independence requirements of IEEE Std. 603-1991, Clause 5.6. Section 1 of this ISG specifies that communications between redundant divisions of safety systems should adhere to the points presented in that section. Table 7.9-1 documents the staff's evaluation of interdivisional communications using the HSLs against each criterion in DI&C ISG #4-HICRc.

Table 7.9-1 Evaluation of the PMS Interdivisional Communication via HSL

Point	Acceptability	Basis
1	The staff finds Point 1 of DI&C ISG #4 has been satisfied.	Aside from voting purposes, the components within the PMS do not receive any information from outside their division that will be used for accomplishing any safety functions.
2	The staff finds Point 2 of DI&C ISG #4-HICRc has been satisfied.	Except for voting purposes, the information received from other divisions is not used for initiating a protective function. Information received from other divisions for display and signal comparison purposes is validated through CRC checks. A communications fault in which the information is delayed, incorrect, or missing will be handled by the communications processor of each PM646 module.
3	For Point 3 of DI&C ISG #4, the applicant provided an alternative method to the guidance. The staff finds the alternative method is acceptable.	Aside from voting purposes, the information shared across divisions of the PMS does not meet DI&C ISG #4-HICRc interdivisional communication Point 3. In the PMS design, information received from other divisions for display and cross-divisional diagnostic purposes does not enhance the safety function. However, since (1) the received information is not used for reactor trip and ESF actuation function, (2) it is communicated on a separate communication medium (AF100 bus), and (3) failure of such communication would not affect the safety functions, the staff finds the proposed alternative method acceptable.
4	The staff finds Point 4 of DI&C ISG #4 has been satisfied.	Within the PM646 module, the communications processor is separate from the function processor, and data transmission between the two processors can only be accomplished using dual port-RAM. As such, any communications errors will not propagate from the communications processor to the function processor within each PM646 module.
5	The staff finds Point 5 of DI&C ISG #4 has been satisfied.	As stated above, in the SER for the Common Q Topical Report and NUREG-1793, the staff concluded that the HSL communications and the PM646 processor design is adequate to address the deterministic performance criteria in HICB BTP 7-21 in the Common Q Topical Report, and the resolution of PSAI 6.6 in NUREG-1793. The PMS is designed to meet the Chapter 15 overall response requirements. The proposed response time testing in ITAAC Item 11b of Table 2.5.2-8 in the AP1000 DCD will verify that the as-built PMS fulfills the response time criteria under maximum CPU loading.

6	The staff finds Point 6 of DI&C ISG #4 has been satisfied.	The safety processor operates asynchronously to the communications processor within the PM646 module, and the operation does not perform any communication handshaking or accept interrupts from other divisions.
7	The staff finds Point 7 of DI&C ISG #4 has been satisfied.	The communication section of PM646 module only accepts predefined data sets and uses a CRC check to ensure the integrity of the data.
8	The staff finds Point 8 of DI&C ISG #4 has been satisfied.	The received information from other divisions is only used for display, diagnostic, and voting purposes. The use of predefined data sets and CRC checks ensures that the integrity of the data prevents any communications errors from affecting the safety functions.
9	The staff finds Point 9 of DI&C ISG #4 has been satisfied.	Section 2.1 of WCAP-17201 describes how the incoming messages are pre-allocated memory in static locations in the communications portion of the AC-160 controller. Additional features are implemented to ensure that any software faults in the application data will be detected. Based on the storage of incoming messages in pre-allocated memory space and the use of error detection features to identify any software faults, the staff finds that Point 9 has been satisfied.
10	The staff finds Point 10 of DI&C ISG #4 has been satisfied.	As stated in Section 7.9.2.2.2 of this SER, there only two methods to load software to the AC160 controllers. One is via the AF100 bus, which has been disabled during the software programming. The other way to load software into the AC160 is by a serial connection between the division's MTP and the AC160. This loading cable is normally disconnected on each end to prevent inadvertent programming during operations. As such, the staff finds Point 10 has been satisfied.
11	The staff finds Point 11 of DI&C ISG #4 has been satisfied.	The information received from other divisions is only used for display, diagnostic, and voting purposes. The design does include using the information for any other functions, including functions that allow the safety function to receive software instructions. The implementation of the design will be evaluated in the review of the specific design specifications.
12	The staff finds Point 12 of DI&C ISG #4 has been satisfied.	WCAP-17201, Section 2.2 discusses how messages will be checked to ensure validity of the message (e.g., repeated messages or messages out of sequence.) The specific features implemented to ensure the validity of the messages are proprietary. However, based on the information presented in technical report WCAP-17201, Section 2.2, the staff finds that Point 12 of ISG-04 has been satisfied.

13	The staff finds Point 13 of DI&C ISG #4 has been satisfied.	As described in technical report WCAP-17201, Section 2.3 the HSL protocol does not support error detection; only error detection is implemented to detect data communication failures. Once a message is detected as bad, it is flagged, and the application software will respond accordingly. The staff finds the use of error detection for HSL data communications acceptable to ensure received messages are correct and correctly understood. Therefore, the staff finds that point 13 has been satisfied.
14	The staff finds Point 14 of DI&C ISG #4 has been satisfied.	The HSL is a point-to-point serial link; thus, Point 14 of DI&C ISG #4 is satisfied.
15	The staff finds Point 15 of DI&C ISG #4 has been satisfied.	Although the Common Q topical report states that the communication section of the PM646 is event driven, and does not communicate a fixed set of data at regular intervals, the processing section of PM646 is cyclic. As such, as discussed in Section 2.4 of WCAP-17201, at the end of every execution cycle, the application program store data from the processing section into the dual-ported memory for the communication section to transmit. Since the communication section transmits the data whenever there is a message in dual-ported memory, this communication is thus linked to the cyclic operation of the process section. Therefore, although the communication section is event driven, the communications are really cyclic and deterministic, and thus the staff finds that Point 15 has been satisfied.
16	The staff finds Point 16 of DI&C ISG #4 has been satisfied.	The watchdog timer feature of the PM646 module ensures message and link liveliness.
17	The staff finds Point 17 of DI&C ISG #4 has been satisfied.	The AP1000 DCD and the supporting TRs, along with the Common Q topical report, and Tier 1 ITAAC have committed to completing equipment qualification.
18	The staff finds Point 18 of DI&C ISG #4 has been satisfied.	The AP1000 DCD and the supporting TRs, along with the Common Q topical report, have committed to providing the FMEA and the SHA.

19	The staff finds Point 19 of DI&C ISG #4 has been satisfied.	As stated above, in the SER for the Common Q Topical Report and NUREG-1793, the staff concluded that the HSL communications and the PM646 processor design is adequate to address the deterministic performance criteria in HICB BTP 7-21 in the Common Q Topical Report, and the resolution of PSAI 6.6 in NUREG-1793. The PMS is designed to meet the Chapter 15 overall response requirements. The proposed response time testing in ITAAC Item 11b of Table 2.5.2-8 in the AP1000 DCD will verify that the as-built PMS fulfills the response time criteria under maximum CPU loading.
20	The staff finds Point 20 of DI&C ISG #4 has been satisfied.	As stated above, in the SER for the Common Q Topical Report and NUREG-1793, the staff concluded that the HSL communications and the PM646 processor design is adequate to address the deterministic performance criteria in HICB BTP 7-21 in the Common Q Topical Report, and the resolution of PSAI 6.6 in NUREG-1793. The PMS is designed to meet the Chapter 15 overall response requirements. The proposed response time testing in ITAAC Item 11b of Table 2.5.2-8 in the AP1000 DCD will verify that the as-built PMS fulfills the response time criteria under maximum CPU loading.

Based on the staff's evaluation of the HSL design against the 20 criteria presented in Section 1 of DI&C ISG #4-HICRc, the staff finds that this design has addressed all criteria within Section 1 of DI&C ISG #4-HICRc, as shown in Table 7.9-1. Thus, the staff finds that the PMS design meets the independence requirements of IEEE Std. 603-1991, Clause 5.6.1. The staff requests that the applicant demonstrate how the HSL design fully conforms to the guidance of DI&C ISG #4-HICRc to meet the requirements of IEEE Std. 603-1991, Clause 5.6.1.

IEEE Std. 603-1991, Clause 5.6.3, requires independence between safety and non-safety systems, such that credible failures in, and consequential actions by, non-safety systems shall not prevent the safety systems from accomplishing their intended safety function. Section 7.9.3 of this SER supplement discusses communications independence between the ICP and the PLS to meet the requirements of IEEE Std. 603-1991, Clause 5.6.3.

The staff has evaluated the access controls to HSLs against requirements of IEEE Std. 603-1991, Clause 5.9. Clause 5.9 required the design to provide administrative control of access to safety-system equipment. Since the HSLs are point-to-point dedicated serial links that are only used within safety systems of the PMS, access control is maintained by the physical security controls in the MCR. The staff finds that access controls to the HSLs meet the requirements of IEEE Std. 603-1991, Clause 5.9.

7.9.2.4 CIM Communication

WCAP-17179, "AP1000 Component Interface Module Technical Report," Revision 1, provides a description of the data communications for the CIM. Section 2.1 of this technical report states that the CIM is designed to interface a field component to the PMS and the PLS. Communication with the PMS is accomplished with the Safety Remote Node Controller (SRNC) assembly. The SRNC module accepts a HSL connection. The SRNC communicates with each CIM through a safety bus known as the X bus. The X-bus is an independent, bidirectional link between the CIM and the SRNC. The PMS communication link is known as the X port. The CIMs communicate with the PLS through an Ovation Remote Node Controller (RNC). The Ovation RNC bus is known as the Y bus.

Section 2.3.1.2.8 of WCAP-17179 states that the CIM has design features to provide for deterministic operation of the CIM. Communication between the PMS to the SRNC via the HSL is designed to be deterministic as described in Section 2.4.1.1 of this technical report. Furthermore, the communication between the SRNC and the CIM via the X bus is designed for deterministic communications as described in Section 2.4.1.2 of this technical report. Messages received from the PLS via the Y bus is translated to discrete digital signals prior to input into the CIM.

Technical Evaluation of the CIM Communications

The staff evaluated how the CIM communications design addressed the system integrity requirements of IEEE Std. 603-1991, Clause 5.5, which requires in part that safety systems be designed to accomplish their safety functions under the full range of applicable conditions enumerated in the design basis. BTP 7-21 states that risky design practices such as non-deterministic data communications, non-deterministic computation, use of interrupts, multitasking, dynamic scheduling, and event-driven design should be avoided. Based on the design commitments for deterministic operation and communications for the CIM, as stated in WCAP-17179 and summarized above, the staff finds that the applicant has adequately

addressed the deterministic communications criteria provided in BTP 7-21 to meet IEEE Std. 603-1991, Clause 5.5.

The evaluation of the interface between the CIM and the PLS with respect to communications independence requirements, as stipulated in IEEE Std. 603-1991, Clause 5.6.3 is provided in 7.9.3 of this SER.

7.9.2.5 Main Control Room Multiplexers

Section 7.1.2.6 of the AP1000 DCD removed the use of multiplexers in the protection and safety monitoring to provide a signal path between the protection system equipment and the MCR. This section states that each division's safety and QDPS display will communicate with the protection system equipment via the dedicated AF100 communications network within each division. In addition, Section 3.4.1 of WCAP-16675 states that the MCR system-level actuation switches are cabled directly from the switches in the MCR to the LCL located in the bistable coincidence cabinets in each instrument room.

Since the switches in the MCR are directly connected to the LCL, the staff finds the justification for removal of the multiplexers in the MCR acceptable.

7.9.2.6 Testing of Communications Modules

Westinghouse removed the description of the fault tolerances, maintenance, test, and bypass from the DCD, and replaced it with references to WCAP-16675. Section 6.1 of WCAP-16675 describes the test features of communications modules within the PMS.

Sections 6.1.2 of WCAP-16675 states the AF100 bus communication modules provide communications between subsystems (e.g., BPL, LCL, ILP, MTP, and ITP). These communications include transferring data in support of system diagnostics. The AF100 bus supports two types of communications: process data and message transfer. Process data are dynamic data used to monitor and control the process, while message transfer is used for program loading and system diagnostics.

The AF100 bus communications modules are individually supervised by their own internal diagnostics and additional run-time diagnostic. In addition, the processor module performs continuous background diagnostics of the communications modules and automatically detects errors during operation. The process module contains the error messages in the error buffer for system troubleshooting.

Technical Evaluation for Testing of Communications Modules

IEEE Std. 603-1991, Clause 5.7, requires the design to provide the capability to test and calibrate safety-system equipment, while retaining the capability of the safety systems to accomplish their safety functions. As applied to data communications systems, SRP Section 7.9 states that data communications systems should be designed to support self-testing and surveillance testing. The design of automatic self-test features should maintain channel independence. The staff finds that the self-testing of the AF100 bus communications modules, including the internal diagnostics and additional runtime diagnostics, demonstrate conformance with the self-testing criteria in SRP Section 7.9 and thus meets the requirements of IEEE Std. 603-1991, Clause 5.7. However, the staff notes that these self-test features are not to

replace the requirements for surveillance testing. In addition, since self-testing of the AF100 bus does not traverse multiple divisions or go outside the safety system, these testing features meet the independence requirements of IEEE Std. 603-1991, Clause 5.6.

7.9.3 Communication between Safety and Non-safety Systems

Section 5 of WCAP-16674 describes the data communications between the safety system and non-safety system within the AP1000 design. This TR also describes the changes made to the certified AP1000 design regarding data communications between the safety and non-safety systems. This TR states that the certified AP1000 design had the following data flow between the safety and non-safety systems:

(1) data flow from PMS to PLS for control purposes
(2) data flow from PMS to DDS for information system purposes
(3) data flow from DDS to PMS for safety-system actuation purposes
(4) data flow from PLS to PMS for component control purposes

In addition, the certified design establishes the following ITAAC in AP1000 DCD Tier 1, Section 2.5.2, regarding the implementation of these data flows:

7.a The PMS provides process signals to the PLS through isolation devices.

7.b The PMS provides process signals to the DDS through isolation devices.

7.c Data communications between safety and non-safety systems does not inhibit the performance of the safety function.

7.d The PMS ensures that the automatic safety function and the Class 1E manual controls both have priority over the non-Class 1E soft controls.

In the certified design, the data flow between safety and non-safety systems is primarily implemented using divisionalized bidirectional gateways. Section 5 of WCAP-16674 states that the data communications between the PMS and the non-safety system have been modified in the PMS design. These modifications have the following effects:

- Reduce the dependence on the gateways.
- Make the gateways [ ].
- Create segmentation and network independence of the nuclear steam supply system (NSSS) control functions within the PLS.
- Make a clear delineation of the points of electrical, communication, and functional isolation.

In the modified design, the PMS implements data flows between safety and non-safety equipment using divisionalized, [ ] gateways and individual analog and digital signals. Five cases of safety-system-to-non-safety-system communication are identified within

the AP1000 design. WCAP-16674 provides an analysis of the ITAAC in the AP1000 DCD Tier 1, Section 2.5.2 for compliance for each of the cases, including the following requirements:

- There are isolation devices between the PMS and PLS, and between the PMS and the DDS.
- Data communications between safety and non-safety systems do not inhibit the performance of the safety function.
- PMS ensures that the automatic safety function and the Class 1E manual controls both have priority over the non-Class 1E soft controls.

7.9.3.1 Description of the Five Cases of Communication between Safety and Nonsafety Systems

Below is a summary of the five cases of safety-system-to-non-safety-system communication.

Case A and Case B

Section 5 of WCAP-16674 states that Case A and Case B communications allow the PMS to communicate with the non-safety control system (PLS) via qualified isolation devices. Case A involves transferring safety-related input signals that are isolated in the PMS cabinets and sent to the PLS as individual hardwired analog signals. This is identical to the type of interface in existing plants. Case B allows the PMS to transfer analog and discrete digital signals calculated within the PMS to the PLS using qualified isolation devices. Section 5 of WCAP-16674 states that the qualified isolation devices used in both Case A and Case B communications provide electrical isolation between the systems as required by IEEE Standard 603-1991. They also provide functional isolation by preventing the non-safety system from adversely affecting the safety function.

Case C

Case C communication allows various process-related signals (analog input signals, analog signals calculated within the PMS, and digital signals calculated within the PMS) to be sent to the DDS for information system (plant computer) purposes. Non-process signals, such as cabinet entry status, cabinet temperature, and direct current power supply, are also provided to the DDS for information system purposes. As described in Section 5.1.2 of WCAP-16674, the AOI Gateway in each PMS division connects that division's internal network to the non-safety real-time data network. The sole purpose of the AOI Gateway is to provide data from the safety system to the non-safety system for non-safety applications. The AOI Gateway has no protection function in the PMS. The reliability of the PMS to perform its safety function is not dependent on the AOI Gateway's being functional.

The gateway has two subsystems: one is the safety subsystem that interfaces with the AF100 bus, and the other is the non-safety subsystem that interfaces with the non-safety Emerson Ovation® network. The AOI safety subsystem is implemented within the PMS to gain access to the desired data. This functionality is included in the PMS MTP, a Common Q FPDS. The PMS portion of the AOI function is implemented using the hardware and software dedication and qualification methodologies accepted by the NRC as part of the Common Q topical report SER

process. A fiber-optic link provides communication between the safety subsystem and the non-safety subsystem. Communication isolation is achieved through the use of [ ] transmission of data from the optical transmitter on the safety subsystem to the optical receiver on the non-safety subsystem.

For sequence of events (SOE) signals, such as partial trip signals, reactor trip signals, and ESFAS, each division provides the signals to the SOE system or interface via a [ ] fiber-optic link. The flow of information is strictly from the safety subsystem to the non-safety SOE system or interface. The [ ] nature of the link is assured by the use of a single [ ] fiber. The safety end of the fiber is connected to an optical transmitter. The non-safety end of the fiber is connected to a fiber-optic receiver. This arrangement also provides electrical isolation between the safety and non-safety portions of the system.

Case D

Case D communications allows the non-safety system to communicate with the safety system using discrete digital signals. These signals are used to implement non-safety manual control of system-level safety functions (actuations, manual blocks, and resets, manual reactor trip) and a non-safety interlock of certain PMS test functions.

Case D communications allows non-safety manual controls of system-level safety functions that originate from dedicated switches in the RSR. Section 5.2.1 of WCAP-16674 states that in the RSR, the non-safety manual controls of system-level safety functions (actuations, manual blocks and resets, manual reactor trip) originate from dedicated switches. The individual discrete digital signals are classified as non-safety-related and are, therefore, isolated in the PMS cabinets before being used. At the RSR, a fiber-optic transmitter encodes the switch contact state to send over the fiber-optic cable. In the PMS, the fiber-optic receiver decodes the data and recreates the switch contact state on its discrete output signal to the AC160 rack in the safety system. Electrical isolation is provided via the fiber-optic connection. There is no metallic path to conduct an electrical fault into the PMS. Functional isolation is provided by logic within the PMS to prevent the non-safety data flow from inhibiting the safety function. The functionality associated with these controls is disabled until operation is transferred from the MCR to the RSR. This transfer is accomplished by the divisionalized Class 1E transfer switches, which are connected directly to the LCL controllers in each division. Additionally, when the controls are enabled, their functionality is limited to that defined in the PMS functional design, because the information transferred is only in the form of discrete digital signals (i.e., there is no computer software-based communication). Specifically, the PMS design only permits the RSR manual system-level ESF actuations and the manual reactor trip inputs to initiate safety functions, not inhibit them. The manual system-level resets only remove the system-level actuation signals; they do not cause any components to change state. An additional signal is required to cause a component to change state. To reduce the chance of the spurious actuation of a function, switch contacts and communication paths are arranged in complementary pairs. Two simultaneous failures in opposite directions would be required to cause a spurious actuation.

In addition for some PMS test functions that are subject to interlocks, Case D communications also allows for transfer of discrete individual hardwired digital signals for interlocks from non-safety equipment to the PMS. Section 5.1.2 of WCAP-16674 states that, for certain PMS test functions that are subject to interlocks from non-safety equipment, individual hardwired digital

signals from non-safety systems are isolated in the PMS cabinets before being used. Qualified isolation devices are used. These devices provide electrical isolation between the systems, as required by IEEE Std. 603-1991.

Case E

Case E communications allows the non-safety system to communicate with the safety system using discrete digital signals. These signals are used to implement non-safety manual component-level controls of safety components.

As described in Section 5.2.2 of WCAP-16674, Case E communications allows manual component soft controls originating in the PLS to actuate safety components. The use of a remote I/O node, consisting of one or more Class 1E CIMs, will congregate the signals from the non-safety manual soft controls to provide one signal digital output to a non-processor-based priority logic also contained in the CIM. The remote I/O node from the non-safety system is physically located within each division of the safety system. The remote I/O node is electrically isolated from the non-safety system by the fiber-optic remote I/O bus. The node is powered by the safety system, and the portions of the node not performing a safety function are qualified as Associated Class 1E equipment, in accordance with IEEE Std. 384-1981. Specifically, the safety-system qualification program will demonstrate that, when it is subject to environmental, electromagnetic, and seismic stressors, it does not degrade the Class 1E circuits below an acceptable level. The environmental, electromagnetic, and seismic stressors used for these tests are the same as those used to qualify the Class 1E equipment in the same cabinet.

Within the CIM, demands from the non-safety system are evaluated against Class 1E automatic actuation signals and Class 1E manual actuation signals from the PMS subsystem. If conflicting demands are present, the safe state of the component takes priority. The CIM uses non-processor-based priority logic hardware to implement this priority function. The CIM module also provides status updates of the safety component to the PLS. The remote I/O bus that connects the remote I/O node to the PLS uses fiber-optic cables to provide electrical isolation. As depicted in Figure 6-3 of WCAP-16674, the remote I/O bus uses bidirectional communications between the PLS and the remote I/O node. However, the communications interface of the CIM translates this data into simple discrete signals for input into the Class 1E priority logic to ensure communications independence.

PMS Interfaces to Standalone Systems

In addition to the five cases of communications between the PMS and non-safety systems, Section 4.2.1 of WCAP-16674 states that the PMS interfaces to the standalone Radiation Monitoring System (RMS). RMS has two parts, one for safety functions and the other for non-safety functions. There is no interface between the two parts. The safety portion of the RMS interfaces to the PMS using simple analog and/or discrete digital signals; this interface does not use network or datalink connections. Communication isolation does not apply to discrete hardwired signals. Electrical isolation between the RMS and the PMS is not required since the safety portion of the RMS is Class 1E. There is no interface between the non-safety portion of the RMS and the PMS.

The core exit thermocouples (CETs) used by the QDPS function of the PMS are physically housed within IIS. There is no electrical interface between the CETs and the incore

instrumentation electronics of the IIS. The CETs interface to the PMS using simple analog signals; these interfaces do not use network or datalink connections. Communication isolation does not apply to discrete hardwired signals. Electrical isolation between the CETs and the PMS is not required since the CETs are Class 1E.

7.9.3.2 Technical Evaluation of Safety to Non-safety Data Communication

IEEE Std. 603-1991, Clause 5.6.3, requires independence between safety and non-safety systems, such that credible failures in and consequential actions by non-safety systems shall not prevent the safety system from accomplishing its intended safety function. In addition, GDC 24 requires the protection system to be separated from control systems to the extent that failure of any single control system component or channel, or failure or removal from service of any single protection system component or channel, which is common to the control and protection systems, leaves intact a system satisfying all reliability, redundancy, and independence requirements for the protection system. SRP Section 7.9 provides acceptance criteria for independence between safety and non-safety systems to meet the requirements of IEEE Std. 603-1991, Clause 5.6.3, and GDC 24. SRP Section 7.9 states that physical, electrical, logical, or software malfunction in one portion cannot adversely affect the safety functions of the connected system. In addition, SRP BTP 7-11 provides acceptable methods for ensuring electrical isolation between safety and non-safety systems. The staff evaluated each of the five cases of communication between the components within the PMS and non-safety systems, and the PMS interface to non-safety standalone systems, against the requirements of IEEE Std. 603-1991, Clause 5.6.3, and GDC 24. DI&C ISG #4-HICRc clarifies existing guidance on acceptable methods to meet the communications independence requirements of IEEE Std. 603-1991, Clause 5.6. Section 1 of this ISG specifies that communications between safety and non-safety systems should adhere to the points presented in that section. The staff evaluated the safety-to-non-safety communications scheme for each of the five cases against the criteria presented in DI&C ISG #4-HICRc. The staff's evaluation is documented below.

Case A and Case B

Based on the staff's evaluation of technical reports WCAP-16675 and WCAP-16674, the staff finds that the design of hardwired interfaces used to send analog and digital signals from the PMS to the PLS meets the electrical isolation and communications independence requirements of IEEE Std. 603-1991, Clause 5.6.3, and GDC 24. Specifically, the staff finds that since the signal transmission between the PMS and PLS is limited to analog and discrete digital signals, communications independence do not apply. Section 5 of WCAP-16674 qualified isolation devices are used in Case A and Case B communications to provide electrical isolation between the PMS and the PLS. As stated in Section 7.1.2.10 of the AP1000 DCD, isolation devices are used 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 (such as open circuits, short circuits, or applied credible voltages) in one circuit from propagating to another circuit. The staff finds this design criteria is consistent with the guidance of SRP BTP 7-11. Since the design criteria has not changed from the certified Revision 15 of the AP1000 DCD to the current revision, the staff finds the use of qualified isolation devices acceptable to ensure adequate electrical isolation between the PMS and non-safety systems. Therefore, the staff finds that the applicant has satisfied the requirements of IEEE Std. 603-1991, Clause 5.6.3, and GDC 24. In addition, in Tier 1, Chapter 2, Table 2.5.2-8 of the AP1000 DCD, the staff identified ITAAC for isolation devices from the PMS to the PLS

and from the PMS to the DDS to ensure electrical isolation. Since these ITAAC were approved in Revision 15 of the AP1000 DCD, and no modifications have been made in subsequent revisions, the staff finds that these ITAAC adequately verify electrical isolation between the PMS and the PLS and DDS to meet the electrical isolation requirements in IEEE Std. 603-1991, Clause 5.6.3, GDC 24.

Case C

The staff evaluated the description of the safety-to-non-safety system communications in Case C against the electrical isolation requirements, and the communications and functional independence requirements, of IEEE Std. 603-1991 and GDC 24. Based on the information presented in Section 5.1.2 of WCAP-16674, the staff finds the use of one-way fiber-optical communication between the MTP and the AOI Gateway, and between the PMS and the SOE system and interface in Case C, provides adequate electrical isolation and communications independence between the PMS and the non-safety, Ovation® network to meet the requirements of IEEE Std. 603-1991, Clause 5.6.3, and GDC 24. Specifically, the staff finds that the use of fiber-optic cable for electrical isolation is in accordance with BTP 7-11. The staff finds that communications independence is achieved in the design, since the design does not include an optical receiver on the MTP for data to traverse from the non-safety network to the PMS. Since the communication is physically [ ] from the safety system to the non-safety system, a failure within the non-safety system cannot propagate to the safety system. The staff finds that the safety-to-non-safety system communications in Case C meet the communication and functional independence requirements of IEEE Std. 603-1991, Clause 5.6.3, and GDC 24.

Case D

The staff evaluated the description of interconnections between the RSR and the PMS in support of non-safety manual controls of system-level safety functions in Case D communications based on the electrical isolation and functional independence requirements of IEEE Std. 603-1991, Clause 5.6, and GDC 24. Based on the information provided in Section 5.2.1 of WCAP-16674, the staff finds that the design provides adequate electrical isolation, and communications and functional independence for manual system-level ESF actuation and manual reactor trip inputs from the RSR to the PMS to meet the requirements of IEEE Std. 603-1991, Clause 5.6.3, and GDC 24. Specifically, the staff makes the following findings:

- The use of fiber-optic cables provides adequate electrical isolation, as specified in SRP BTP 7-11.

- Since the data flow from the RSR to the PMS is in the form of discrete digital signals (e.g., no communications protocol or handshaking), the guidance in DI&C ISG #4-HICR does not apply. The use of discrete digital signals for initiating system-level ESF actuation and reactor trip from the RSR using point-to-point fiber cabling provides adequate communications independence between the PMS and the RSR.

- The software within the PMS, which allows the discrete signals to only initiate safety functions, specifically, initiation of system-level ESF actuation and reactor trip, provides adequate functional isolation.

The staff evaluated the description of data communications between non-safety equipment and the PMS in support of certain PMS test functions that require interlocks in Case D communications based on the electrical isolation and communications and functional independence requirements of IEEE Std. 603-1991, Clause 5.6, and GDC 24. The staff finds that the information presented in Section 5.2.1 of WCAP-16674 provides an adequate description of how electrical isolation, communications and functional independence are achieved for the inputs from non-safety equipment to the PMS to meet the requirements in IEEE Std. 603-1991, Clause 5.6.3, and GDC 24. Specifically, the staff makes the following findings:

- Electrical isolation is provided between the PMS and non-safety equipment through the use of an isolation device. As stated above in the evaluation of Case A and Case B communications, the isolation device serve to prevent credible faults (such as open circuits, short circuits, or applied credible voltages) in one circuit from propagating to another circuit, which is consistent with the guidance of SRP BTP 7-11.

- Since the data flow from the non-safety equipment to the PMS is in the form of discrete digital signals (e.g., no communications protocol or handshaking), the guidance of DI&C ISG #4-HICR does not apply. The use of discrete digital signals for activating interlocks for certain PMS tests provides adequate communications independence between the PMS and the non-safety equipment.

- The software in the PMS allows the discrete signals to only affect the ability to perform tests. The interlocks do not affect automatic or manual safety functions.

In Tier 1, Chapter 2, Section 2.5.2, Table 2.5.2-8 of the AP1000 DCD, the staff identified ITAAC for isolation devices between the PMS and the PLS and between the PMS and the DDS to ensure electrical isolation. However, the staff did not identify any ITAAC for verifying electrical isolation between the PMS and the non-safety equipment that will be used to activate interlocks for these PMS tests. The staff requested the applicant to provide additional information to demonstrate how the qualified isolation devices provide electrical isolation between the non-safety equipment and the PMS. Specifically, the staff requested the applicant to provide an additional ITAAC to verify electrical isolation between the PMS and the non-safety equipment to activate these interlocks. In response letter, "AP1000 Response to Proposed Open Item (Chapter 7),"ML100470598, dated February 8th, 2010, the applicant proposed to include an additional ITAAC in Tier 1, Chapter 2, Section 2.5.2, Table 2.5.2-8 of the AP1000 DCD. The proposed ITAAC states:

> "The PMS receives signals from non-safety equipment that provide interlocks for PMS test functions through isolation devices."

The proposed acceptance criteria states:

> "A report exists and concludes that the isolation devices prevent credible faults from propagating into the PMS.

The staff finds this proposed ITAAC acceptable in verifying that adequate electrical isolation exists to prevent credible faults from non-safety equipment from impacting the PMS, and thus satisfies the requirements of IEEE Std. 603-1991, Clause 5.6.3, and GDC 24. The staff will

verify the incorporation of this ITAAC in the next version of the AP1000 DCD. This is tracked as **CI-SRP7.9-ICE-02**.

Case E

The staff evaluated the description of data communications between the CIM and the PLS in Case E, based on the electrical isolation and communications and functional independence requirements of IEEE Std. 603-1991, Clause 5.6, and GDC 24. The staff finds that the information presented in Section 5.2.2 of WCAP-16674 provides an adequate description of how Westinghouse achieves electrical isolation and communications and functional independence for non-safety manual component-level control of safety components for Case E, to meet the requirements of IEEE Std. 603-1991, Clause 5.6.3, and GDC 24. Specifically, the staff makes the following findings:

- The use of fiber-optic cables between the remote I/O bus that connects the remote I/O node to the PLS provides adequate electrical isolation, as specified in SRP BTP 7-11.

- Although the remote I/O bus uses bidirectional communications between the PLS and the remote I/O node, the communications interface of the CIM translates these data into simple discrete signals for input into the Class 1E priority logic. Since the data flow into the Class 1E priority logic is in the form of discrete digital signals (e.g., no communications protocol or handshaking), the guidance in DI&C ISG #4-HICR does not apply. The use of discrete digital signals for initiating non-safety manual component-level control of safety components provides adequate communications independence between the CIM and the PLS.

- The priority logic within the CIM provides functional isolation by ensuring that the PMS has priority to actuate the safety component, such that the non-safety signal cannot prevent the PMS from actuating the component. If the non-safety system initiates an actuation command without the PMS initiating an actuation command, then the safe state of the component takes priority.

IEEE Std. 603-1991 defines associated circuits as non-Class 1E circuits that are not physically separated or are not electrically isolated from Class 1 E circuits by acceptable separation distance, safety class structures, barriers, or isolation devices. IEEE Std. 384-1992, Clause 5.5, contains the classification and qualification of associated circuits. IEEE Std. 384-1992, Clause 5.5.3, states that associated circuits, including their isolation devices or the connected loads without the isolation devices, shall be subject to the qualification requirements placed on Class 1E circuits to ensure that the Class 1E circuits are not degraded below an acceptable level. Associated circuits need not be qualified for performance of function, since the function is non-Class 1E. The staff finds that Section 5.2.2 of WCAP-16674 adequately demonstrates how the RNC is qualified as an associated circuit to meet the requirements of IEEE Std. 603-1991, Clause 5.6, and IEEE Std. 384-1992. Specifically, the staff finds that the commitment, as part of the overall safety-system qualification program, to demonstrate that, when the RNC is subject to environmental, electromagnetic, and seismic stressors, it does not degrade the Class 1E circuits below an acceptable level, meets the associated circuit qualification requirements in IEEE Std. 384-1992, Clause 5.5.3.

PMS Interfaces to Standalone Systems

Section 4.2.1 of WCAP-16675 provides a description of the PMS interfaces to standalone safety systems. This section states that the PMS interfaces to the standalone Radiation Monitoring System (RMS). However, there is no interface between the safety portion of the RMS and the non-safety portion.

In addition, the core exit thermocouples (CETs) used by the QDPS function of the PMS are physically housed within IIS. There is no electrical interface between the CETs and the incore instrumentation electronics of the IIS. The CETs interface to the PMS using simple analog signals; these interfaces do not use network or datalink connections.

Based on the information provided in Section 4.2.1 of WCAP-16675 regarding PMS interfaces with standalone systems, such as the RMS, the staff finds the design adequately demonstrates compliance with the communications and functional independence requirements of IEEE Std. 603-1991, Clause 5.6.3, and GDC 24. Specifically, for the RMS, since there is no interface between the safety portion of the RMS and the non-safety portion, communications independence does not apply. In addition, functional independence is achieved through the isolation of safety functions to only the safety portion of the RMS, and does not require interaction with the non-safety portion to perform the intended safety functions. For the CETS used by the QDPS function of the PMS, the staff finds that since the CETS interface to the PMS using simple analog signals and these signals are Class 1E, communication independence does not apply. Since the CETs are Class 1E, the staff finds that electrical isolation between the CETs and the PMS is not required.

7.9.4 Non-safety Communications

7.9.4.1 Description of the Nonsafety Communication Network

Non-safety communications consist primarily of the non-safety communication network and the non-safety data link interface. The non-safety communication network is implemented using the Ovation® network. This network uses unaltered Ethernet protocols, high-speed Ethernet switches, and full duplex cabling (fiber or copper shield twisted pair).

Section 3 of WCAP-16674 provides a detailed description of the AP1000 non-safety communications system. The non-safety communications network provides real-time data distribution and general purpose communications. Real-time data distribution is defined as the scheduled periodic broadcast of real-time data pertaining to the plant processes. The term “general purpose communications” is defined as the aperiodic exchange of data for other purposes, such as system operation, diagnostics, and maintenance.

The Ovation® network supports network standard communications protocols, such as Transmission Control Protocol/Internet Protocol and User Datagram Protocol/Internet Protocol for general purpose communications. Within the Ovation® system, general purpose communications based on standard protocols are used for aperiodic data, including file-type data transferred from the historian and plant databases to be presented at the HSI, plant informational data messages, alarm messages, and SOE messages to the plant historian for long-term historical storage. This communication occurs on the same physical media as the real-time periodic data, but it is implemented in such a way as to preserve the design philosophy of guaranteeing the real-time periodic data transmission without loss, degradation, or delay, even during plant upsets.

With respect to periodic data, the network is designed to support up to 200,000 point values per second, using a nominal percentage of the overall network bandwidth. The network load associated with periodic data origination is constant; it does not change during plant upset conditions. The Ovation® vendor has tested the network at the limit of 200,000 point values per second. A design goal is to limit the number of point values per second, to the extent possible. This will provide additional spare capacity and will result in a lower base load on the network. As the design is finalized, a firm number of point values per second will be determined. This will be used to calculate the base network load and, therefore, the network bandwidth available for aperiodic data communications. With respect to aperiodic data, the network load is variable but managed. The aperiodic data levels can be managed through careful system configuration. Alarm message data will be minimized, to the extent possible, by limiting the number of points subject to alarm checking and by carefully selecting alarm limits to minimize nuisance alarms. Network impacts associated with station staff in the main control area are somewhat limited by the number of operators and operator stations and by the number of engineers and engineering stations. In general, the network load from aperiodic data traffic is expected to be very small in relation to the overall bandwidth of the system. Analytical justification of network capacities will be reviewed for correctness. Based on the current evaluation of expected network traffic, the single network design will meet or exceed all system capacity and network loading requirements.

Storm control is configured on the Ovation® network to ensure that highway availability requirements are satisfied, given the possibility that a software or hardware malfunction, or a malicious network attack, would introduce a packet storm on the control system highway. Storm control is implemented with configuration settings provided by the switch operating system. In general, each port subject to storm control is configured with traffic ingress block and restoration settings. These values are typically a percentage of the total available bandwidth that can be used by the broadcast or multicast traffic. When traffic entering a port exceeds the predefined block value, packet forwarding on the port is blocked. Packet forwarding resumes when the traffic falls below the predefined “restore forwarding” setting. Storm control is put in place to protect the network from data storms produced as a result of atypical conditions, including hardware malfunctions, and errors introduced by humans. The thresholds are set on a per-port basis, so that native Ovation® traffic (e.g., periodic process point data, aperiodic alarm message traffic) will not activate the storm control function. In addition to the system storm control configuration installed on the network switches, the Ovation® controller has been hardened against excessive network traffic through the use of a software modification that prioritizes critical control functionality over network communications.

7.9.4.2 Technical Evaluation of the Non-safety Communication Network

The staff evaluated the adequacy of the non-safety Ovation® network to perform the required control functions specified in the AP1000 DCD and the supporting TRs, as well as WCAP-16675 and WCAP-16674, including how the applicant met the requirements of 10 CFR 52.47(a)(9). Regulations in 10 CFR 52.47(a)(9) require applications for light-water-cooled NPPs to evaluate the standard plant design against the SRP revision in effect 6 months before the docket date of the application. The evaluation required by this section shall include an identification and description of all differences in design features, analytical techniques, and procedural measures proposed for the design and those corresponding features, techniques, and measures given in the SRP acceptance criteria. SRP Section 7.9 provides performance criteria for data communication systems; specifically, for system capacity, data rates, and bandwidth requirements. The staff finds that the description provided for system capacity, data rates, and

bandwidth requirements, and the analysis on expected network traffic, presented in Section 3 of WCAP-16674, adequately address the performance criteria for data communications systems specified in SRP Section 7.9. Specifically, the staff finds that the evaluation of expected network traffic demonstrates that the network design is bounded by the Ovation® system capacity and network loading requirements.

Specifically, the staff evaluated the non-safety Ovation® network design features to determine how Westinghouse has addressed operating experience with data storm, as described in NRC Information Notice 2007-15, "Effects of Ethernet-Based, Non-Safety Related Controls on the Safe and Continued Operation of Nuclear Power Stations," dated April 17, 2007 (ADAMS Accession Numbers ML071510428). The staff finds that the storm control features within the Ovation® network design adequately demonstrate how data storms are precluded in the Ovation® network. Specifically, the staff finds that the use of storm control configuration settings provided by the switch operating system, and the software feature that prioritizes critical control functionality over network communications, ensure that the Ovation® controller can continue to control critical plant operations during a network storm or a complete loss-of-network event.

7.9.4.3 Description of the Non-safety Data Link Interfaces

Section 3.2 of WCAP-16674 describes the non-safety data link interfaces in the AP1000 I&C design. Each system is summarized below.

Standalone Systems

The Ovation® system supports standard and custom data links, both at the controller and workstation level. Controller-level interfaces include standard interfaces to Allen-Bradley programmable logic controllers and GE Mark V/VI, Toshiba, and MHI turbine control systems, as well as a standard MODBUS interface and OSI PI historian interface. At the controller level, the data link interface can be accomplished via a standard I/O module (the R-line Link Controller), or via fast Ethernet communications interfaces at the controller processor level.

Remote I/O

The Ovation® system supports the use of remote I/O**,** so that I/O modules can be clustered close to field devices, minimizing field cabling costs and also accommodating harsher environments. Remote I/O is in contrast to local I/O**,** which is housed in the same cabinet as the controller or next to it in an extended cabinet. For local I/O**,** all I/O modules reside in up to four cabinets, which are placed side by side. All field wiring leads to these cabinets.

Non-safety Smart I/O Field Buses

The Ovation® system supports HART I/O, FOUNDATION™ Fieldbus, Prefabs DP, and DeviceNet™ smart I/O interfaces. The Ovation® fieldbus solution is modular, and a single controller can simultaneously interface to fieldbus devices, HART I/O modules, conventional I/O modules, and third-party I/O.

HART I/O

The Ovation® controller supports native HART I/O modules. HART is technology that provides a digital information signal superimposed on a 4-20 milliampere traditional sensor loop. The digitized signal provides up to four HART multivariables, which provide additional information from HART-enabled devices, eliminating additional cabling required to provide the same information using traditional sensors and control output devices.

The Ovation® HART input module has eight inputs, with each input having an individual HART modem (supporting up to four HART multivariables), and individual channel-to-channel isolation. The Ovation® HART output module has four channels, also with individual HART modems per channel, and individual channel-to-channel isolation.

Foundation Fieldbus

FOUNDATION™ Fieldbus H1 is typically used for analog devices, such as sensors and modulating control valves. A large assortment of “smart” devices is available with the interface. The Ovation® FOUNDATION™ Fieldbus solution is modular and scalable. The interface between the FOUNDATION™ Fieldbus instrumentation and the Ovation® controller is via dedicated, redundant Fieldbus Ethernet switches, and Ovation® FOUNDATION™ Fieldbus Gateways. There are up to 16 FOUNDATION™ Fieldbus gateways per controller, with up to four H1 segments per gateway and up to 16 devices per segment.

Profibus DP

Profibus DP is typically used for digital on/off devices. In addition to being supported by the appropriate devices, it is suitable for long distances while remaining less sensitive to power, grounding, polarity, and resistance concerns.

The Ovation® Profibus Interface uses a standard Ethernet switch, attached to the Ovation® controller via the controller's standard MODBUS/TCP third-party I/O capability.

DeviceNet

DeviceNet™ is an interface for discrete actuators and sensors. The Ovation® DeviceNet™ interface has the same fundamental design as the Profibus DP interface, using a standard Ethernet switch, attached to the Ovation® controller via the controller standard MODBUS/TCP third-party I/O capability.

Asset Management

Another important component of the intelligent field interface solution is the Asset Management Solutions (AMS) suite of software. AMS software and the associated SNAP-ON applications are a suite of software solutions for streamlining all maintenance activities related to instrumentation and valves in a process plant. This package can be integrated into the Ovation® workstation and Ovation® controller to give the user direct access to all intelligent devices connected to the Ovation® I/O. With AMS integrated into Ovation®, digitized HART or FOUNDATION™, Fieldbus parameters such as valve position can be mapped to Ovation® process points that can be used anywhere they are required in the Ovation® distributed control system. AMS provides direct visibility from the Ovation® workstation to each “smart” device in the plant that is connected to Ovation®.

7.9.4.4 Technical Evaluation of the Non-safety Data Link Interfaces

The staff evaluated the non-safety data link interfaces within the AP1000 I&C design. IEEE Std. 603 1991, Clause 5.6.3, requires independence between safety and non-safety systems so that credible failures in, and consequential actions by, non-safety systems shall not prevent the safety system from accomplishing its intended safety function. In addition, GDC 24 requires the protection system to be separated from control systems to the extent that failure of any single control system component or channel, or failure or removal from service of any single protection system component or channel that is common to the control and protection systems, leaves intact a system satisfying all reliability, redundancy, and independence requirements of the protection system. These non-safety data link interfaces do not communicate with any of the safety systems beyond the five cases of safety-to-non-safety system data communications specified in WCAP-16674. As such, the staff finds that the electrical isolation, communications and functional independence requirements of IEEE Std. 603-1991, Clause 5.6.3, and GDC 24 do not apply.

7.9.5 Secure Development and Operational Environment

10 CFR Part 50, Appendix A, General Design Criterion (GDC) 21 requires, in part, that protection systems (or safety systems) must be designed for high functional reliability commensurate with the safety functions to be performed. Criterion III of Appendix B to 10 CFR Part 50, requires, in part, that quality standards must be specified and design control measures must be provided for verifying or checking the adequacy of design.

10 CFR 50.55a(h) requires that safety systems for nuclear power plants must meet the requirements stated in IEEE Std. 603-1991, “Criteria for Safety Systems for Nuclear Power Generating Stations.” Clause 5.6.3 of IEEE Std. 603-1991 requires safety systems to be designed such that credible failures in and consequential actions by other systems will not prevent safety systems from performing their intended safety functions. In addition, Clause 5.9 of IEEE Std. 603-1991 requires the design to 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.

RG 1.152, Rev. 2 provides a method that the NRC finds acceptable for complying with the Commission’s regulations (i.e., 10 CFR Part 50, Appendix A, GDC 21, Criterion III of Appendix B to 10 CFR Part 50, and IEEE Std. 603-1991, Clauses 5.6.3 and 5.9) for promoting high functional reliability, design quality, and security for use of digital computers in safety systems of nuclear power plants. Security in this context refers to the establishment of a secure development and operational environment (SDOE) for digital safety systems by: (i) measures and controls taken to establish a secure environment for development of the digital safety system against undocumented, unneeded and unwanted modifications and (ii) protective actions taken against a predictable set of undesirable acts (e.g., inadvertent operator actions or the undesirable behavior of connected systems) that could challenge the integrity, reliability, or functionality of a digital safety system during operations. RG 1.152, Rev. 2 utilizes the waterfall life cycle phases to provide a framework for establishing digital safety system security guidance, as well as criteria for acceptability, in the development of high quality safety systems.

As proposed in the response to OI-SRP7.1-ICE-01, Section 7.1.2.14.1 of the AP1000 DCD will be revised to reference, APP-GW-J0R-012, “Protection and Safety Monitoring System Computer Security Plan,” hereinafter referred to as “PMS Computer Security Plan,” to

demonstrate how computer security is incorporated into the design and development of AP1000 safety systems. This plan provides a description of the planning phase for the AP1000 PMS. This plan summarizes the quality standards and design control measures implemented to provide computer security and ensure that the PMS and CIM are designed for high functional reliability commensurate with the safety functions to be performed throughout the development phases of digital safety system lifecycle. These commitments include the design and development of security features and development controls for the PMS and CIM. Although the PMS Computer Security Plan does not officially commit to conformance to RG 1.152, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants," Revision 2, this technical report addresses the system security aspects of the Common Q platform, PMS application, and CIM from the Concepts Phase through the Test Phase to protect against non-malicious events that is consistent with the criteria provided by RG 1.152, Revision 2.

The safety evaluation for AP1000 I&C secure development and operational environment, ML102210335, provides a separate assessment of the PMS Computer Security Plan and contains OUO information. This separate safety evaluation forms the basis for the following conclusions.

- The identified vulnerabilities in the PMS design for the conceptual phase of the development life cycle, and the security capabilities that mitigate these vulnerabilities adequately address Regulatory Position C.2.1 within RG 1.152, Revision 2.

- The performance of additional V&V activities for the Common Q platform satisfies the criteria for identifying and mitigating vulnerabilities as specified in Regulatory Position C.2.1 of RG 1.152, Revision 2.

- Although the vulnerabilities of the PMS and CIM development process are general, these vulnerabilities were only based on the conceptual phase assessment, and these vulnerabilities encompass more detailed vulnerabilities that may be identified in later portions of the development process. Thus, the identified vulnerabilities are acceptable in specifying particular portions of the development process that are susceptible to unintended or inadvertent modification to the PMS or CIM while under development or to the development tools. As such, the applicant has adequately addressed the criteria within Regulatory Position C.2.1 of RG 1.152, Revision 2 for the PMS application and the CIM. In addition, the quality assurance program for both the development of the PMS and the CIM, and the V&V process are adequate to mitigate the identified vulnerabilities by identifying and preventing inadvertent changes to the PMS and CIM design during development.

- By precluding capabilities for remote access to the PMS during operations in the design and by ensuring one way data flow from the PMS to non-safety systems (except for use of discrete digital or analog signal), the applicant has satisfied Regulatory Position C.2.1 within RG 1.152, Revision 2. In addition, the commitment to ensure that the isolated development infrastructure (IDI) is created to preclude remote access is sufficient to satisfy Regulatory Position C.2.1 within RG 1.152, Revision 2.

- Based on the PMS access control functional requirements, the safety to non-safety interfaces requirements, and the commitment to ensure that proper human factors are considered during the development of the PMS design, these requirements adequately

provide sufficient measures to protect the PMS from inadvertent operator actions or unpredictable behavior of connected systems during operations to address the criterion within Regulatory Position C.2.2.1 of RG 1.152, Revision 2 to define the security functional performance requirements.

- The Common Q Platform has adequately addressed the criteria within Regulatory Position C.2.2.1 of RG 1.152, Revision 2. Specifically, the Common Q platform software verification and validation (V&V), as described in Section 5.5.3 of the Common Q Software Program Manual (ML050350234), was reviewed and accepted by the NRC in the safety evaluation report for the Common Q platform Software Program Manual. This includes the approval of the V&V process for use of pre-developed software within the Common Q platform. The V&V activities that were performed on the Common Q platform are adequate to ensure the integrity, reliability, and functionality of this platform for use in the AP1000 PMS application.

- By incorporating the security requirements into the overall system requirements, the PMS V&V process in accordance with the Common Q Software Program Manual is adequate to ensure the correctness, completeness, accuracy, testability, and consistency of the system security requirements. Thus, the applicant has met the criteria within Regulatory Position C.2.2.1 of RG 1.152, Revision 2.

- Based on the described security measures provided in the IDI, the commitment to assess and mitigate vulnerabilities in the IDI, and the quality assurance and V&V process described in the PMS Computer Security Plan, the applicant has adequately ensured that undocumented code or functions are precluded in the design to meet Regulatory Positions C.2.2.2 of RG 1.152, Revision 2.

- By incorporating the security features as part of the overall system design, the design process described in Section 2.3 of the PMS Computer Security Plan is adequate to ensure that the system security requirements is accurately translated into specific design configuration items to meet Regulatory Position C.2.3.1 of RG 1.152, Revision 2. In addition, the additional security assessment completed during the design phase is adequate to ensure that any vulnerability that has not been identified during earlier phases of the development life cycle is captured and that the security features chosen in the conceptual phase are adequate.

- Based on the quality assurance and V&V process described in the PMS Computer Security Plan, the staff finds that the applicant has adequately ensured that undocumented code or functions are precluded in the PMS and CIM design to meet Regulatory Positions C.2.3.2 of RG 1.152, Revision 2. This is based on control of the design document revision process, storage of design process in an accessed controlled manner, and requirements traceability to ensure that all design features are traceable to requirements specifications.

- By incorporating the security features as part of the overall system implementation, the implementation process described in Section 2.4 of the PMS Computer Security Plan is adequate to ensure that the system design is accurately transformed into code, database structures, and related machine executable representations to meet Regulatory Position C.2.3.1 of RG 1.152, Revision 2. In addition, the additional security

assessment completed during the implementation phase is adequate to ensure that the security controls chosen are adequate.

- Based on the commitment to secure the IDI, to perform testing and scanning to identify undocumented code and functions, and to follow the quality assurance and V&V process described in Section 2.1.2.2 of this SER, the applicant has adequately ensured that undocumented code or functions are precluded in the PMS and CIM implementation to meet Regulatory Positions C.2.4.2 of RG 1.152, Revision 2.

- Based on the commitment to perform integration, system, and acceptance tests where practical and necessary on the PMS security features, including testing of the system configuration, and the performance of additional vulnerability assessments to ensure that no new vulnerabilities are identified in the PMS, the applicant has adequately addressed Regulatory Position 2.5 of RG 1.152, Revision 2.

- Based on the commitment to secure the testing environment and to test the hardware architecture, external communication devices, and configurations for unauthorized pathways that affect system integrity, the applicant has adequately addressed Regulatory Position C.2.5.2 of RG 1.152, Revision 2.

Based on the staff's conclusions of the PMS Computer Security Plan, as discussed above, the staff finds that the applicant has sufficiently addressed the criteria in Regulatory Positions C.2.1 through C.2.5 of RG 1.152, Rev. 2 to meet the requirements of 10 CFR Part 50, Appendix A, GDC 21; Criterion III of Appendix B to 10 CFR Part 50; and IEEE Std. 603-1991, Clauses 5.6.3 and 5.9; as it relates to security and reliability of the PMS application and CIM. The incorporation of the proposed reference to the PMS Computer Security Plan in Revision 18 of the AP1000 DCD is tracked as **CI-SRP7.9-ICE-03**.

7.9.6 Evaluation, Findings, and Conclusions

The staff reviewed the revisions to Section 7.1 and the associated TRs of the AP1000 DCD against the regulatory requirements of a data communications system as stipulated in the guidance of SRP Section 7.9. Below is a summary of the staff's findings.

Regulations in 10 CFR 50.55a(h) require compliance with IEEE Std. 603-1991 and the correction sheet, dated January 30, 1995. The minimum requirements that are applicable to all data communications systems are in IEEE Std. 603-1991, Clause 5.6.3. Other criteria include those in Clauses 5.4, 5.6.1, 5.7, and 5.9. The staff evaluated the data communications systems in the amendments to the AP1000 I&C systems design for conformance to the requirements of IEEE Std. 603-1991 and has the following findings:

- IEEE Std. 603-1991, Clause 5.4: This requirement has been fully satisfied, as documented in Section 7.9.3 of this FSER supplement. In Table 2.5.2-8 of the AP1000 DCD, the staff identified ITAAC for the seismic, environmental, and Class 1E qualification of PMS equipment, including equipment used for data communications in the PMS.

- IEEE Std. 603-1991, Clause 5.6.1: This requirement has been fully satisfied, as documented in Section 7.9.2.3 of this FSER supplement. The staff finds that the 20

criteria presented in Section 1 of DI&C ISG #4-HICRc have been satisfied in the design for interdivisional communication between divisions of the PMS.

- IEEE Std. 603-1991, Clause 5.6.3: This requirement has been fully satisfied, as documented in Section 7.9.3 of this FSER supplement. The staff finds that the information presented in the AP1000 DCD and the supporting technical reports have sufficiently demonstrated how independence is achieved for each of the five cases of safety and non-safety communications.

- IEEE Std. 603-1991, Clause 5.7: This requirement has been satisfied, as documented in Section 7.9.2.5 of this FSER supplement.

- IEEE Std. 603-1991, Clause 5.9: This requirement has been fully satisfied, as documented in Section 7.9.2 of this FSER supplement. The AP1000 DCD and the supporting TRs have addressed how access controls are incorporated into the design of the PMS.

Regulations in 10 CFR 52.47(a)(9) require applications for light-water-cooled NPPs to evaluate the standard plant design against the SRP revision in effect 6 months before the docket date of the application. The evaluation required by this section shall include an identification and description of all differences in design features, analytical techniques, and procedural measures proposed for the design and those corresponding features, techniques, and measures given in the SRP acceptance criteria. SRP Section 7.9 provides the design considerations for data communications systems, including criteria for performance and reliability considerations. The staff evaluated the data communications systems in the AP1000 DCD against the guidance provided in the SRP Section 7.9, which states that digital computer timing should be consistent with the limiting response times and characteristics of the computer hardware, software, and data communications systems. The staff found the applicant's commitment to modify the acceptance criteria in Item 11 b) of ITAAC Table 2.5.2-8 in the AP1000 DCD to state "Performance of system tests and the documentation of system test results, including a response time test will be performed under maximum CPU loading to demonstrate the PMS can fulfill its response time criteria" is acceptable to address the criteria within SRP Section 7.9 and therefore meets the requirements of 10 CFR 52.47(a)(9).

GDC 21 requires the protection system to be designed for high functional reliability and inservice testability, commensurate with the safety functions to be performed. Redundancy and independence designed into the protection system shall be sufficient to ensure that (1) no single failure results in loss of the protection function, and (2) removal from service of any component or channel does not result in loss of the required minimum redundancy, unless the acceptable reliability of operation of the protection system can be otherwise demonstrated. The protection system shall be designed to permit periodic tests of its functioning when the reactor is in operation, including a capability to test channels independently to determine failures and losses of redundancy. Based on the staff's conclusions of the PMS Computer Security Plan, as discussed in Section 7.9.5 of this SER, the staff finds that the applicant sufficiently addressed the criteria in Regulatory Positions C.2.1 through C.2.5 of RG 1.152, Revision 2 to meet the requirements of 10 CFR Part 50, Appendix A, GDC 21, Criterion III of Appendix B to 10 CFR Part 50, and IEEE Std. 603-1991, Clauses 5.6.3 and 5.9, as it relates to security and reliability of the PMS application and CIM. As such, the staff concludes that the AP1000 design meets the requirements of 10 CFR Part 50, Appendix A, GDC 21; Criterion III of Appendix B to 10 CFR

Part 50; and IEEE Std. 603-1991, Clauses 5.6.3 and 5.9; as it relates to security and reliability of the PMS application and CIM.

GDC 24 requires the protection system to be separated from control systems to the extent that failure of any single control system component or channel, or failure or removal from service of any single protection system component or channel that is common to the control and protection systems, leaves intact a system satisfying all reliability, redundancy, and independence requirements of the protection system. Based on the review of the interfaces between the PMS and the PLS, the staff concludes that this requirement has been fully satisfied, as documented in Section 7.9.3 of this FSER supplement. The staff finds that the information presented in the AP1000 DCD and the supporting technical reports have sufficiently demonstrated how independence is achieved for each of the five cases of safety and non-safety communications.

Appendix 7.A: Evaluation of APP-GW-GLR-137, Revision 0, "Bases of Digital Overpower and Overtemperature Delta-T (OPΔT/OTΔT) Reactor Trips,"

7.A.1 Introduction

This safety evaluation addresses changes made from Revision 15 to 17 of the AP1000 Design Control Document (DCD) (Ref 1) regarding a change in methodology for the Thermal Overtemperature Delta-Temperature (OTΔT) and Thermal Overpower Delta-Temperature (OPΔT) reactor trip design bases. Revision 15 of the DCD references WCAP-8745-P-A, "Design Bases for the Thermal Overpower ΔT and Thermal Overtemperature ΔT Trip Functions." This is the previously approved topical report for the analog calculation of the reactor trip functions (Ref 2). Revision 17 also references WCAP-8745-P-A; however, Revision 17 includes a change from an analog-based OTΔT and OPΔT design to a digital-based design with a different calculational methodology for the trip function. The basis of the setpoint calculations is unchanged from that presented in WCAP-8745-P-A, but the inputs to both margin-to-trip functions have changed. The digital-based core power indication described in technical report APP-GW-GLR-137, Revision 0, "Bases of Digital Overpower and Overtemperature Delta-T (OPΔT/OTΔT) Reactor Trips," proposes the use of density at the reactor core inlet and the enthalpy difference between the exit and inlet of the core, referred to as the "ΔT power signal," to provide a more accurate measurement of core power. The new technical report also claims the setpoint functions have been simplified.

7.A.2 Evaluation

7.A.2.1 Background

Request for Additional Information (RAI) RAI-SRP16-CTSB-42 (Ref 3) requested that Westinghouse either submit a previously approved reference supporting the changes to the OTΔT and OPΔT trip functions or submit a reference that supports the changes. The RAI also requested that Westinghouse comply with Generic Letter 88-16 to include the appropriate and approved methodology regarding the revised trip functions in Technical Specification (TS) Section 3.3.1-1 and bases which are addressed in Chapter 16 of this report.

The response to RAI-SRP16-CTSB-42 (Ref 4) led to the generation of open item (OI) OI-SRP16-CTSB-42 (Ref 5) since the response did not fully address the staff's request. The Chapter 16 Safety Evaluation Report (SER), which is based on changes to the DCD between Revision 15 and Revision 17, references the open item.

The initial response to OI-SRP16-CTSB-42 was submitted to address staff concerns (Ref 6). A reference to technical report APP-GW-GLR-137, Revision 0, "Bases of Digital Overpower and Overtemperature Delta-T (OPΔT/OTΔT) Reactor Trips," was given to provide the information requested by NRC staff (Ref 7). Changes to the DCD for Revision 17 were also provided to maintain consistency between the submitted technical report and the following DCD sections:

- Section 7.2.1.1.3
- Section 7.2.4

- TS Table 3.3.1, Notes 1 and 2

Staff submitted RAIs based on the review of technical report APP-GW-GLR-137. After reviewing the responses, the staff found the information given in technical report APP-GW-GLR-137 to be acceptable in support of the digital-based OPΔT and OTΔT reactor trip function methodology.

7.A.2.2 Proposed Change

The OPΔT and OTΔT trips are used to protect the specified acceptable fuel design limits (SAFDLs) so as to maintain the fuel in a geometry amenable to cooling. The design basis of the OTΔT trip is to prevent a departure from nucleate boiling (DNB) on all fuel surfaces, while the design basis of the OPΔT trip is to prevent excessive fuel centerline temperatures for all fuel rods.

In the analog technology of the OPΔT trip setpoint, as described in WCAP-8745-P-A, the setpoint is calculated as a function of the average coolant temperature (T_{AVG}) and a core power reduction term related to adverse axial offset. The OTΔT setpoint has the same inputs as the OPΔT trip setpoint with the addition of pressurizer pressure. The setpoints use T_{AVG}, axial offset, and pressurizer pressure (only for OTΔT) as inputs to a dynamically compensated function to determine the percent of rated thermal power (RTP) at which the reactor should trip. The analog signals are converted to ΔT signals by adjusting gains. The basis for the determination of both ΔT setpoints is derived from thermal design limits as explained in WCAP-8745-P-A.

The change from the analog technology to the digital technology is in both the reactor trip function and the RTP measurement. The analog method uses ΔT as a measure of core power while the digital method uses actual core power. In the digital method, core power is determined by calculating an enthalpy difference between the core inlet and outlet. The inputs from the respective protection system divisions used to calculate the enthalpy terms are T_H for the inlet, T_C for the outlet, and pressurizer pressure, which is used in both terms. Core average temperature is eliminated as the major functional variable in the digital-based function.

In both the analog and digital technology, the OPΔT trip setpoint uses only a preset bias based on a percentage of RTP, which is based on pre-determined thermal limits, as discussed in WCAP-8745-P-A. This term is compared to core thermal power and then dynamically compensated to obtain a margin to trip signal.

In the proposed change to digital technology, the OTΔT trip setpoint directly translates DNB thermal design limits, which give core inlet temperature as a function of RTP for various pressurizer pressures, into inputs for the setpoint calculation. Core inlet temperature and pressurizer pressure information are linearly interpolated from a table that provides the corresponding RTP to serve as the appropriate setpoint. This setpoint is compared to the core thermal power calculation and then dynamically compensated to obtain a margin to trip signal.

7.A.2.3 Regulatory Basis

10 CFR Part 50, Appendix A, General Design Criterion (GDC) 10 states, “The reactor core and associated coolant, control, and protection systems shall be designed with appropriate margin to assure that specified acceptable fuel design limits are not exceeded during any condition of normal operation, including the effects of anticipated operational occurrences.” GDC 10

therefore applies directly to the design of the OTΔT and OPΔT reactor trips since they are part of the reactor protection system.

Furthermore, Generic Letter 88-16, "Guidance for Technical Specification Changes for Cycle-Specific Parameter Limits," was issued to allow licensees to update all applicable cycle-specific limits without formal review by the NRC. These cycle-specific limits are now located in the core operating limits report (COLR) and are referenced throughout TS. The methodologies by which the cycle-specific limits are updated undergo a formal review by the NRC and are referenced in Section 3.3.1 and bases of the TS.

Since Westinghouse has revised the method by which the OPΔT and OTΔT reactor trip functions are calculated in the digital methodology, as discussed in technical report APP-GW-GLR-137, the new methodology must be reviewed and approved by NRC staff. Furthermore, once the review is completed and approved, TS 3.3.1 and bases should be updated to reflect the methodologies that serve as the basis for determining the limits given in the COLR.

7.A.2.4 Technical Evaluation

As previously discussed, all methodologies used to update limits given in the COLR must be reviewed and approved by the staff. The change in calculational methodology of the OPΔT and OTΔT reactor trip setpoints is given in technical report APP-GW-GLR-137. The staff reviewed the document and submitted RAIs to better understand how the trip function calculations have changed and to ensure that SAFDLs will not be exceeded.

A review of the RAI responses in support of OI-SRP16-CTSB-42 closure is provided in the following discussion. Westinghouse's RAI responses are documented in Reference 8.

- Question 1 of Reference 8 asks how the single failure criterion of 10 CFR 50.55a(h) is met when an individual resistance thermowell detector (RTD) in one of four divisions votes for a trip due to an approach to a saturation condition. In the response, it is stated that the single failure criteria is not impacted by an RTD in a saturated condition since the two-out-of-four voting logic by division is unaffected. When a single RTD approaches saturation, it is removed from the average hot leg temperature calculation for that division. Further it was stated that when two RTDs approach saturation, a trip vote occurs in the affected division. Based on the applicant's response, it was determined that 10 CFR 50.55a(h) has not been violated and Question 1 is resolved**.**

- Question 2 discusses the accuracy of the ΔT power signal and asks how the bias applied to the $T_{hot\text{-}local}$ signal leads to approximation of the mixed mean hot leg temperature. The concern is that the correction factor applied to the individual hot leg RTDs, which are used to calculate the average hot leg temperature, might lead to an inaccurate calculation of the ΔT power signal. The response states that the ΔT power signal is frequently calibrated, as required by TS, so consequently there is reasonable assurance that the streaming bias applied to the $T_{hot\text{-}local}$ signals will not affect the calculation of the ΔT power signal used in the margin to trip calculation. Based on the applicant's indication that the ΔT power signal is continuously monitored and validated, Question 2 is resolved and Westinghouse indicated that the technical report will be updated for clarification. This is **Confirmatory Item (CI) CI-SRP7.A-SRSB-01.**

- Question 3 is related to the discussion of the redundant sensor algorithm and asks if the discussion is included in Chapter 7 of the DCD. The applicant stated that APP-GW-GLR-137, which includes the discussion, is referenced in Chapter 7 of the DCD. The inclusion of the technical report as a reference in Section 7.2.4 in Chapter 7 is captured as **CI-SRP7.A-ICE-01**.

- Question 4 is concerned with how the weighted averaging of the $T_{hot\text{-}local}$ signals is performed for T_H determination. Specifically, the concern is that automatic adjustment of weighting factors might violate 10 CFR 50 Appendix B, Criterion III, Design Control. The response states that weighting factors are not changed. If one of the $T_{hot\text{-}local}$ signals is dropped from the determination of T_H, due to an approach to saturation condition, then the same weighted average is performed, only with two weighting factors instead of three. Based on Westinghouse's response, it is clear that the weighting factors are not adjusted and there is no violation of 10 CFR Part 50 Appendix B, Criterion III. Westinghouse committed to update the technical report for clarification and therefore the staff opened **CI-SRP7.A-SRSB-02**.

- There was concern with how a failure of the core inlet temperature signal (T_C) would affect the protection system. Question 5 asks how the system responds to a "BAD" quality T_C signal. The response states that an alarm is actuated in the main control room to notify operators to take appropriate action. The value of the signal (e.g. failed off-scale low, failed off-scale high or otherwise) will determine whether or not a trip is voted for. Based on the applicant's response, it is clear that a failure of a T_C signal will result in appropriate operator action and therefore Question 5 is resolved.

- To determine how the margin to trip function interfaces with the protection system bi-stable controller, Question 6 asks how the margin to trip signal feeds into the logic that generates a division trip vote and if the margin to trip signal is used elsewhere. The response states that the margin to trip signal is directly input to the trip bi-stable controller, which looks for a negative value to allow for a trip vote. The signal also goes to the main control room for alarm and display. It is also stated that the margin to trip signal is hardwired into the plant control system and that the information is available for use by other systems if needed. Based on clarification of how the margin to trip signal interfaces with the protection system, Question 6 is resolved.

- Question 7 refers to the use of time constants in the T_H, T_C, and OPΔT and OTΔT margin to trip signal development. Clarification was requested regarding the extra lag term and also how the values of these constants differ from those in the previously approved analog methodology. The response indicates that the extra lag term is dedicated to signal noise filtering and does not affect the shape of the output signal (i.e. it is comparable to the output signal that uses a first order lag term). The technical report discusses the possible factors that go into calculation of the net lead and lag constants, many of which are optional, and furthermore are determined in the plant-specific safety analysis of record to verify the adequacy of the protection system. The response to Questions 9-11 give typical values assumed in performed analog versus digital comparative analyses. Based on the provided clarification, Question 7 is resolved.

- Question 8 refers to the use of the bias coefficient and the conversion factor used in calculating the ΔT power signal. The question asks how the constants are determined

and how often they must be adjusted. The response states that the bias coefficient will be adjusted so that the ΔT power signal indicates zero at hot zero power. This action is mandatory as part of the channel calibration required by TS surveillance requirement (SR) 3.3.1.9 which requires calibration every 24 months. The conversion factor is a gain adjustment that is adjusted as necessary in compliance with SR 3.3.1.3, which requires comparing the ΔT power signal to the calorimetric power, similar to the neutron flux power range signal surveillance, every 24 hours. Based on the provided clarification, Question 8 is resolved.

- Questions 9 through 11 ask the applicant to discuss the differences between the analog and digital based dynamic response when a trip occurs. Provided in the response are the assumed time constants used in comparing the analog response to the digital response. The differences are shown in a comparative example. Additional concern was expressed with regard to the Chapter 15 design basis accidents which credit the OPΔT and OTΔT reactor trips. It was asked if the Chapter 15 accidents were revised to include the revised digital-based reactor trip functions.

  The comparisons between the two trip responses given in the response to RAI-TR36-012 (Ref 9) show that the trip responses are similar, which provides reasonable assurance that the dynamic compensation terms applied to the digital-based method and the proposed trip functions are appropriate. It was stated that the Chapter 15 design basis accidents were not updated to reflect the digital-based functions since the comparative studies performed confirmed that the digital-based method closely simulates the analog-based method without a loss of safety margin. Revision 18 of the DCD will incorporate the discussion of the trip response comparison with respect to the Chapter 15 analyses, which is **CI-SRP7.A-SRSB-03**. Questions 9 through 11 are therefore resolved.

- Question 12 was asked to resolve a discrepancy between time constants reported in APP-GW-GLR-137 and those shown in Figure 7.2-1 (Sheet 5) of the DCD. An updated figure was provided with the RAI responses for consistency, and Question 12 is therefore resolved. The action of updating Figure 7.2-1 (Sheet 5) in the DCD is **CI-SRP7.A-ICE-02**.

- Question 13 asked the applicant to ensure that the TS and bases are consistent with the information provided in APP-GW-GLR-137. The response states that appropriate changes are being made and will be reflected in Revision 18 of the DCD. Question 13 is resolved and is **CI-SRP7.A-CTSB-01**.

- An additional confirmatory item is required for the update of Reference 4 in Section 5.0, “References,” of APP-GW-GLR-137 since the currently referenced topical report discusses the methodology used to determine certain uncertainties that factor into the calculation of the OP∆T and OT∆T setpoints. APP-GW-GLR-137 states that a revision to the topical report will be issued at a later date. This is **CI-SRP7.A-SRSB-04.**

The staff concludes that, based on the information provided in APP-GW-GLR-137 and the responses to RAIs given in Reference 8, no significant change was made to the functional output and underlying methodology for the digital based OPΔT and OTΔT margin to trip functions and it is therefore concluded that SAFDLs will not be exceeded. Improvements to the

measurement of core power for input to the margin to trip calculation were made by using actual core parameters versus using differential temperature. This change addresses a source of previous inaccuracy in the trip functions. To provide further assurance that the ΔT power signal used in the margin to trip calculation is valid, the signal is also compared to the plant calorimetric heat balance routinely performed in SR 3.3.1.3 as given in Chapter 16 of the DCD.

The setpoint calculated in the digital-based methodology for the OTΔT setpoint is based on allowable core power as a function of pressurizer pressure and core inlet temperature instead of allowable ΔT as a function of T_{AVG}. This is a simpler method and allows for direct translation of the appropriate DNB thermal design limits into the OTΔT trip function. The OPΔT setpoint calculation is unchanged in the digital methodology, except for the units. The OPΔT setpoint is manually fixed at a determined power level and only changes as a function of the adverse axial offset.

7.A.3 Conclusion

After reviewing APP-GW-GLR-137, the staff finds the proposed OPΔT and OTΔT reactor trip function calculational methodology to be acceptable and considers OI-SRP16-CTSB-42 to be resolved pending the completion of all confirmatory items below.

Confirmatory Items:
CI-SRP7.A-ICE-01
CI-SRP7.A-ICE-02
CI-SRP7.A-SRSB-01
CI-SRP7.A-SRSB-02
CI-SRP7.A-SRSB-03
CI-SRP7.A-SRSB-04
CI-SRP7.A-CTSB-01

7.A.4 References

[1] AP1000 Design Control Document
[2] WCAP-8745-P-A, ML073521507
[3] RAI-SRP16-CTSB-42, ML082700083
[4] Response to RAI-SRP16-CTSB-42, ML083290461
[5] Chapter 16 Safety Evaluation Report, ML090700697
[6] OI-SRP16-CTSB-42 R0, ML092360183
[7] APP-GW-GLR-137, ML092360182
[8] OI-SRP16-CTSB-42 R1, ML100270768
[9] Response to RAI-TR36-012, ML072830050