7.0 INSTRUMENTATION AND CONTROLS

Chapter 7, "Instrumentation and Controls," of this safety evaluation report (SER) describes the results of the review by the staff of the U.S. Nuclear Regulatory Commission (NRC or Commission), hereinafter referred to as the staff, of Chapter 7 of the Korea Electric Power Corporation (KEPCO) and Korea Hydro & Nuclear Power Co., Ltd (KHNP), hereinafter referred to as the applicant, Design Control Document (DCD), for the design certification (DC) of the Advanced Power Reactor 1400 (APR1400).

This describes the instrumentation and controls (I&C) for the APR1400 design. The description of I&C systems includes system classifications, functional requirements and assignment, and system architecture. The information provided emphasizes those instruments and associated equipment that constitute the safety-related systems as defined in Title 10 of the *Code of Federal Regulations* (10 CFR), Section 50.55a(h), the General Design Criteria (GDC) of 10 CFR Part 50, "Domestic Licensing of Production and Utilization Facilities," Appendix A, "General Design Criteria for Nuclear Power Plants," and other I&C-related regulations in 10 CFR Part 50.

7.1 Instrumentation and Controls – Introduction

7.1.1 Introduction

The I&C systems provide control of plant processes to protect against unsafe and improper reactor operations during steady-state and transient power operations. The I&C systems also provide initiating signals to mitigate the consequences of accident conditions.

7.1.2 Summary of Application

Final Safety Analysis Report (FSAR) Tier 1: DCD Tier 1 information associated with this section is found in DCD Tier 1 Section 2.5, "Instrumentation and Control Systems."

DCD Tier 2: The applicant provided a system description in DCD Tier 2 Section 7.1, "Introduction," which is summarized in the following discussion.

The I&C system consists of both safety-related and non-safety I&C systems. The safety-related I&C systems consist of the plant protection system (PPS), the core protection calculator system (CPCS), engineered safety features – component control system (ESF-CCS), ESF-CCS soft control module (ESCM), qualified indication and alarm system-P (QIAS-P), excore neutron flux monitoring system (ENFMS), auxiliary process cabinet – safety (APC-S), and the safety-related portion of the radiation monitoring system (RMS). These systems perform the necessary functions to maintain the plant in the prescribed safety limits and provide indications to the operators for post-accident monitoring functions.

The non-safety distributed control system (DCS) provides for component-level control, automatic process control, and high-level group control. The DCS utilizes a redundant and fault-tolerant architecture and consists of the power control system (PCS), nuclear steam supply system (NSSS) process control system (NPCS), and process-component control system (P-CCS).

An independent and diverse actuation system (DAS) is provided to cope with software common-cause failures (CCFs) of the safety-related I&C systems. The DAS consists of the

diverse protection system (DPS), the diverse manual actuation (DMA) switches, and the diverse indication system (DIS).

The safety and non-safety I&C systems are implemented using two major platforms. Most safety-related I&C systems are implemented using the safety-related programmable logic controller (PLC) platform, which the applicant has identified as Asea Brown Boveri's (ABB) AC160 platform as described in the Westinghouse Topical Report WCAP-16907, "Common Qualified Platform Topical Report." An industrial DCS platform is used for the data processing and non-safety control systems. Several I&C systems such as the ENFMS, the safety portion of the RMS, the Turbine/Generator (T/G) control and protection system, and the APC-S are implemented on independent platforms. The DPS and DIS are implemented using field programmable gate array (FPGA) logic controllers (FLC) and the DMA are hardwired switches.

Inspections, Tests, Analyses, and Acceptance Criteria (ITAAC): The ITAAC associated with DCD Tier 2 Section 7.1 are given in DCD Tier 1 Section 2.5.

Technical Specifications (TS): The TSs associated with DCD Tier 2 Section 7.1, are given in DCD Tier 2 Chapter 16, "Technical Specifications." Specifically, Technical Specifications, Section 3.3, "Instrumentation," and Section B 3.3, "Instrumentation," address I&C systems.

7.1.3 Regulatory Basis

The relevant requirements of the U.S. Nuclear Regulatory Commission (NRC or Commission) regulations for this area of review, and the associated acceptance criteria, are given in NUREG-0800, "Standard Review Plan (SRP) for the Review of Safety Analysis Reports for Nuclear Power Plants: Light Water Reactor Edition" (hereafter referred to as the SRP), Section 7.1, "Instrumentation and Controls – Introduction," and Appendix 7.1-A, "Acceptance Criteria and Guidelines for Instrumentation and Control Systems Important to Safety," Revision 5, and are summarized below. Although Revision 6 of SRP Chapter 7 was issued in August 2016, per the requirements of 10 CFR 52.47(a)(9), the applicant is only required to evaluate its standard design against the SRP revision in effect 6 months before the docket date of the application. Review interfaces with other SRP sections can also be found in SRP Section 7.1.

1. GDC 1, "Quality Standards and Records," as it relates to assuring structures, systems, and components (SSCs) important to safety are designed, fabricated, erected, and tested to quality standards commensurate with the importance of the safety functions to be performed.

2. GDC 2, "Design Bases for Protection Against Natural Phenomena," as it relates to assuring SSCs important to safety shall be designed to withstand the effects of natural phenomena without loss of capability to perform their safety functions.

3. GDC 4, "Environmental and Dynamic Effects Design Bases," as it relates to assuring SSCs important to safety shall be designed to accommodate the effects of and to be compatible with the environmental conditions associated with normal operation, maintenance, testing, and postulated accidents, including loss-of-coolant accidents (LOCAs).

4. GDC 13, "Instrumentation and Control," as it relates to assuring instrumentation is provided to monitor variables and systems over the anticipated ranges for normal operation, for anticipated operational occurrences (AOOs), and for accident conditions

as appropriate to assure adequate safety, including those variables and systems that can affect the fission process, the integrity of the reactor core, the reactor coolant pressure boundary, and the containment and its associated systems.

5. GDC 20, “Protection System Functions,” as it relates to the protection system to be designed (1) to initiate automatically the operation of appropriate systems including the reactivity control systems, to assure that specified acceptable fuel design limits are not exceeded as a result of AOOs and (2) to sense accident conditions and to initiate the operation of systems and components important to safety.

6. GDC 21, “Protection System Reliability and Testability,” as it relates to assuring the protection system is designed for high functional reliability and inservice testability commensurate with the safety functions to be performed as well as redundancy and independence sufficient to assure 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.

7. GDC 22, “Protection System Independence,” as it relates to the design of the protection system to assure that the effects of natural phenomena, and of normal operating, maintenance, testing, and postulated accident conditions on redundant channels do not result in loss of the protection function.

8. GDC 23, “Protection System Failure Modes,” as it relates to assuring the protection system is designed to fail into a safe state or into a state demonstrated to be acceptable on some other defined basis if conditions such as disconnection of the system, loss of energy, or postulated adverse environments are experienced.

9. GDC 24, “Separation of Protection and Control Systems,” as it relates to assuring the protection system is 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 of the protection system as well as assuring that interconnection of the protection and control systems is limited to assure that safety is not significantly impaired.

10. GDC 29, “Protection Against Anticipated Operational Occurrences,” as it relates to protection and reactivity control systems to be designed to assure an extremely high probability of accomplishing these safety functions in the event of AOOs.

11. 10 CFR 50.55a(h)(3), “Safety Systems,” as it relates to compliance with Institute of Electrical and Electronics Engineers (IEEE) Standard (Std) 603-1991, “IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations,” and the January 30, 1995, correction sheet.

12. 10 CFR 52.47(b)(1), “Contents of applications; technical information,” requires that a design certification contain the proposed ITAAC that are necessary and sufficient to provide reasonable assurance that, if the inspections, tests, and analyses are performed and the acceptance criteria met, a plant that incorporates the design certification is built and will operate in accordance with the design certification, the provisions of the Atomic Energy Act of 1954, and NRC regulations.

Acceptance criteria adequate to meet the above requirements include the SRP Table 7-1, "Regulatory Requirements, Acceptance Criteria, and Guidelines for Instrumentation and Control Systems Important to Safety," Section 3 (Staff Requirements Memoranda (SRMs)), Section 4 (Regulatory Guides (RGs)), and Section 5 (Branch Technical Positions (BTPs)), that list the SRP acceptance criteria applicable to I&C systems important to safety.

7.1.4 Technical Evaluation

The objectives of the staff's review are to confirm that the I&C system design includes the functions necessary to operate the nuclear power plant safely under normal conditions and to maintain it in a safe condition under accident conditions; that these functions, the implementing systems, and the equipment have been properly classified; and that the commitments have been made to use appropriate quality standards for the I&C systems.

Several of the design considerations are addressed in this section with references, as appropriate, for information contained in Sections 7.2 through 7.9 of this SER. The staff's review of the I&C systems conducted in this section is based on the docketed FSAR, Revision 0, and FSAR, Revision 1. The following technical evaluation discusses the staff's review of the conformance of the proposed design to applicable NRC regulations.

10 CFR 52.47(a)(2) requires, in part, for the applicant to provide a description and analysis of the SSCs of the facility, with emphasis upon performance requirements, the bases, with technical justification therefor, upon which these requirements have been established, and the evaluations required to show that safety functions will be accomplished. It is expected that the standard plant will reflect through its design, construction, and operation an extremely low probability for accidents that could result in the release of significant quantities of radioactive fission products. The description shall be sufficient to permit understanding of the system designs and their relationship to the safety evaluations. 10 CFR 52.47a(3)(i) requires applicants to provide information on the principal design criteria for the facility. Appendix A to 10 CFR Part 50, GDC, establish the minimum requirements for the principal design criteria for water-cooled nuclear power plants similar in design and location to plants for which construction permits have previously been issued by the Commission and provides guidance to applicants in establishing principal design criteria for other types of nuclear power units.

The submittal letter by the applicant for the application for design certification of the APR1400 Standard Design, dated December 23, 2014, provides a list of technical reports that contain analyses and other information that supplement the materials included in the FSAR, with certain technical reports shown as incorporated by reference (IBR). This includes the following reports:

- APR1400-Z-J-NR-14001, "Safety I&C System" Technical Report (Safety I&C System TeR).
- APR1400-Z-J-NR-14003, "Software Program Manual" Technical Report (SPM TeR).
- APR1400-Z-J-NR-14004, "Uncertainty Methodology and Application of Instrumentation" (Uncertainty Methodology TeR).
- APR1400-Z-J-NR-14005, "Setpoint Methodology for Plant Protection System" (Setpoint Methodology TeR).

Based on the staff's review of this list, the staff requested the applicant to incorporate by reference additional technical and topical reports currently not listed as IBR, as documented in

Request for Additional Information (RAI) 274-8277, Question 07.01-36. Specifically, DCD Tier 2 Chapter 7 references several technical and topical reports that the staff uses as bases in the safety evaluation. This includes the following reports:

- APR1400-Z-J-NR-14002, "Diversity and Defense-in-Depth" Technical Report (D3 TeR).
- APR1400-Z-A-NR-14019, "CCF Coping Analysis" Technical Report (CCF Coping Analysis TeR).
- APR1400-E-J-NR-14001, "Component Interface Module" Technical Report (CIM TeR).
- APR1400-F-C-NR-14003, "Functional Design Requirements for a Core Protection Calculator System for APR1400" Technical Report (CPCS TeR).
- APR1400-Z-J-NR-14012, "Control System CCF Analysis" Technical Report (CSCCF TeR).
- APR1400-Z-J-NR-14013, "Response Time Analysis of Safety I&C System" Technical Report (Response Time Analysis TeR).
- APR1400-A-J-NR-14003-, "APR1400 Disposition of Common Q Topical Report NRC Generic Open Items and Plant Specific Action Items" Technical Report (Common Q Platform Disposition TeR).
- APR1400-A-J-NR-14004-, "Common Q Platform Supplemental Information in Support of APR1400 Design Certification" Technical Report (Common Q Supplemental TeR).
- WCAP-10697-P-A, Revision 3, "Common Q Platform Topical Report," (Common Q Platform Topical Report).

The staff requested that these technical and topical reports be included in the list of IBR reports. In the August 11, 2016 response to RAI 274-8277, Question 07.01-36 (Agencywide Documents Access and Management System (ADAMS) Accession No. ML16224A440), the applicant committed to IBR the requested list of technical and topical reports. Based on these proposed changes, the staff finds the issue identified in RAI 274-8277, Question 07.01-36, is closed and resolved. The verification that the proposed markups are incorporated into the next revision of the FSAR was a confirmatory item. The staff verified that the proposed markups have been incorporated into Revision 1 of DCD Tier 2, Sections 1.6 and 7.1. As such, this confirmatory item has been satisfied.

DCD Tier 2, Sections 7.1.2.2 thru 7.1.2.35 identify regulations that the I&C systems are designed in accordance to. This description does not clearly state that these I&C systems meet the requirements of these NRC regulations. For example, DCD Tier 2 Section 7.1.2.5 states that "The I&C systems that are applicable to 10 CFR 50.34(f)(2)(xi) (Reference 12), as shown in Table 7.1-1, are designed in accordance with 10 CFR 50.34(f)(2)(xi)." In RAI 43-7887, Question 07.01-12, the staff requested the applicant to modify DCD Tier 2 Sections 7.1.2.2 thru 7.1.2.35 to clearly state whether the I&C systems meet the requirements of applicable NRC regulations. In the August 12, 2015, response to this RAI (ML15224B645), the applicant stated that DCD Tier 2, Sections 7.1.2.2 through 7.1.2.35 are modified to state that the applicable I&C systems listed in Table 7.1-1 meet the requirements of applicable NRC regulations. The

applicant included proposed markups of the applicable DCD Tier 2, Sections 7.1.2.2 through 7.1.2.35. Based on the proposed change to the FSAR to state that the applicable I&C systems listed in Table 7.1-1 meet the requirements of applicable NRC regulations, the staff finds the issue of RAI 43-7887, Question 07.01-12, is closed and resolved. The verification that the proposed markups are incorporated into the next revision of FSAR was a confirmatory item. The staff verified that the proposed markups have been incorporated into Revision 1 of DCD Tier 2 Section 7.1. As such, this confirmatory item has been satisfied.

In addition, DCD Tier 2 Section 7.1.2, identifies regulations that the I&C systems are designed in accordance to. For several of the regulations (i.e., 10 CFR 50.34(f)(2)(xx), "Power for Pressurizer Level Indication and Controls for Pressurizer Relief and Block Valves," 10 CFR 50.55a(h)(3), which requires compliance to IEEE Std 603-1991, GDC 10, 13, 15, 16, 24, 25, 28, 29, 33-35, 38, 41, and 44), the applicant did not include references to applicable FSAR sections and technical reports that contain information on how these regulations are met. In RAI 43-7887, Question 07.01-13, the staff requested the applicant to modify the applicable DCD Tier 2, sections to include the appropriate references in order to meet the requirements of 10 CFR 52.47(a)(2) and 10 CFR 52.47(a)(3)(i). In the August 12, 2015 response to this RAI (ML15224B645), the applicant stated that DCD Tier 2, Sections 7.1.2 and11.5.2.1, and the D3 TeR is modified to describe references to applicable FSAR sections and TeRs that contain information on how regulations are met. The proposed markups for RAI 43-7887, Question No. 07.01-12, included the proposed changes to DCD Tier 2, Sections 7.1.2.2 through 7.1.2.35 to provide references on how the requirements cited in those sections are met. Based on the proposed modifications to DCD Tier 2, Sections 7.1.2, 7.1.2.2 through 7.1.2.35, and 11.5.2.1, and the D3 TeR, the staff finds that the applicant has provided appropriate references to FSAR sections and TeRs that contain information on how the requirements of 10 CFR 50.34(f)(2)(xx), 10 CFR 50.55a(h)(3), GDC 10, 13, 15, 16, 24, 25, 28, 29, 33-35, 38, 41, and 44 are met. As such, the staff finds the issues identified in RAI 43-7887, Question 07.01-13, is closed and resolved. The verification that the proposed markups are incorporated into the next FSAR revision was a confirmatory item. The staff verified that the proposed markups have been incorporated into Revision 1 of DCD Tier 2 Section 7.1. As such, this confirmatory item has been satisfied.

7.1.4.1 Proposed Alternatives to IEEE Std 603-1991

By letter dated December 23, 2014 (ML14357A449), the applicant submitted its request for NRC approval to use an alternative design to the independence requirements of IEEE Std 603-1991, Clause 5.6.1, "Between Redundant Portions of a Safety System," to satisfy the requirement of 10 CFR 50.55a(h)(3). The applicant's alternative request proposes to utilize shared sensors as an alternative to independent safety division sensors required by IEEE Std. 603-1991, Clause 5.6.1. The applicant's letter states that the basis and technical justification for this alternative is provided in Appendix D of the Safety I&C System TeR. The applicant requested approval of this alternative request as part of the staff's SER for the FSAR and supporting licensing documentation. The staff's evaluation of this alternative request is in Section 7.2.4.2 of this SER.

7.1.4.2 Overview of Instrumentation and Controls Systems

This sub-section outlines the I&C system as submitted by the applicant in the design certification application. The description of the I&C Systems is found in DCD Tier 2, Chapter 7, Revision 0, and the Safety I&C System TeR.

System-Level Instrumentation and Controls Architecture

DCD Tier 2, Revision 0, Figure 7.1-1, "APR1400 I&C System Overview architecture," illustrates the main I&C systems design used for control and monitoring in the plant. These I&C systems perform the majority of signal input processing, automation, operator interface, annunciation of abnormal process conditions, and actuator output functions in the plant. These I&C systems also implement functional requirements specified by various plant mechanical and electrical systems.

The I&C systems are implemented using two major platforms: (1) a safety-related PLC platform for the safety-related systems and (2) a non-safety DCS platform for the data processing system and non-safety control systems. Independent systems such as the T/G control and protection system, the NSSS monitoring system, and the balance of plant (BOP) monitoring system perform the required functions of a portion of the I&C systems.

Most safety-related I&C systems within the APR1400 design are implemented using the Common Q platform, which has been dedicated and qualified for nuclear power plants. The NRC evaluated the Common Q platform and found it acceptable for safety-related I&C applications in nuclear power plants as documented in the staff's safety evaluation (ML13022A011). The following safety-related systems are implemented using the Common Q platform: PPS, CPCS, ESF-CCF, the ESCM, and the QIAS-P. Section 7.1 of DCD Tier 2 states that the ENFMS, the APC-S, the safety portion of RMS, and the CIM are implemented on platforms which are independent from the safety-related PLC platform. For these independent safety-related I&C systems, the staff requested the applicant to provide descriptions of these independent platforms in RAI 43-7887, Question 07.01-18. Specifically, the staff requested the applicant describe how the ENFMS, the APC-S, and the safety portion of the RMS meet the requirements of IEEE Std 603-1991, including Clauses 5.1, 5.3, 5.5, and 5.6. In addition, this RAI requested the applicant to clarify whether there are any other standalone safety-related I&C systems. In the August 12, 2015, response to this RAI (ML15224B643), the applicant stated that besides the safety-related portion of the RMS, there are no other standalone safety-related I&C systems. Further, the applicant stated that the RMS consists of two channels: (1) the safety-related divisionalized cabinet (SRDC), and (2) the non-safety RMS computer cabinet, as shown in DCD Tier 2 Figure 7.3-23. The safety portion of the RMS consists of the radiation element, the local unit, and the SRDC. The divisional SRDC transmits the engineered safety feature actuation system (ESFAS) initiation signals to the dedicated ESFAS measurement channels, as described in Section 7.3.1.1. The safety portion of the RMS is part of the engineered safety features (ESF) system as described in the Section 7.1.1.3. Therefore, the safety portion of the RMS is a part of ESF system and designed to comply with ESF System applicable criteria in the DCD Tier 2 Table 7.1-1, "Regulatory Requirements Applicability matrix." The applicant stated that the ESF system, including the safety portion of the RMS complies with the requirements of IEEE Std 603-1991, Clauses 5.1, 5.3, 5.5, and 5.6 as described in Section 7.3.3.2, "Conformance with IEEE Std 603," is addressed in Appendix A, "Conformance to IEEE Std 603-1991," of Safety I&C System TeR. Based on the staff's review of DCD Tier 2, Sections 7.3.1.1 and 7.1.1.3, and Appendix A of the Safety I&C System TeR, the staff finds that additional information was needed to clarify the design description of the RMS as described below:

a. DCD Tier 2 Section 7.3.1.1 states that the BOP ESFAS receives process variable signals from the safety portion of the RMS, the manual ESF system-level actuation switches, and the manual channel bypass switches. The BOP ESFAS consists of 1-out-of-2 logics taken twice except for the fuel handling area emergency ventilation

actuation signal (FHEVAS), which has one 1-out-of-2 (1oo2) logic. DCD Tier 2 Figure 7.3-23 shows the RMS measurement channel functional diagram, but design descriptions or reference to this figure were not provided in DCD Tier 2 Section 7.3. Based on this figure, it was not clear how many divisions are in the RMS SRDC. In addition, it was not clear whether the RMS computer cabinet is safety-related or non-safety. If the RMS processor in the computer cabinet is non-safety, then staff seeks to understand how the RMS processor is isolated from the SRDC processor to meet the independence requirements of IEEE Std 603-1991, Clause 5.6.3. If the RMS processor is safety-related, the staff seeks to understand how it is meeting independence requirements of IEEE Std 603-1991, Clause 5.6.3 when transmitting information to the information processing system (IPS) and qualified indication and alarm system-non-safety (QIAS-N).

b. Appendix A of the Safety I&C System TeR, Section A.5.3 states that the platform to be used for the safety-related I&C system is qualified as described in Common Q Platform Topical Report, Revision 3. However, DCD Tier 1 Section 7.1.1.3 states that the safety portion of the RMS is implemented on an independent platform that is different from the Common Q platform. Further, the SPM TeR does not appear to address standalone safety-related systems such as the RMS. As such, it is unclear how the requirements of IEEE Std 603-1991, Clause 5.3 are met for the safety portion of the RMS.

c. In the FSAR, state that the RMS is the only standalone safety-related I&C system.

The staff issued RAI 274-8277, Question 07.01-34, to request the applicant provide this information. In the August 30, 2016, response to this RAI (ML16243A544), the applicant proposed to modify the design description in DCD Tier 2, Section 7.3.1.1 and Figure 7.3-23 to reflect the revised system functional configuration. The design is revised such that the RMS processor receives electrically isolated radioactivity measurement signal directly from the local unit, rather than from the safety related divisionalized SRDC processor. The RMS computer cabinet is non-safety; Figure 7.3-23 is to be revised accordingly for clarity. Those measurement signals originating from the safety related detector channels that are transmitted to the non-safety RMS processor will be electrically isolated using an IEEE Std 384-1992 Class 1E qualified isolator, at each local unit. Although the RMS supplier and platform have not been determined, the applicant proposed to modify DCD Tier 2, Sections 7.3.3.2 and 7.3.3.3 to state that the SRDC will be supplied by a 10 CFR Part 50, Appendix B, qualified supplier. The hardware of the SRDC will be qualified to Class 1E, and the software of the SRDC will meet the requirements of RG 1.152, “Criteria for Digital Computers in Safety Systems of Nuclear Power Plants,” Revision 3, which endorses IEEE Std 7-4.3.2-2003, “Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations.” The applicant stated that there will not be any other standalone safety-related systems besides the ones described in DCD Tier 2 Section 7.1. Based on the proposed design changes and revisions to the FSAR to include electrical isolation within the local unit and to commit to using a 10 CFR Part 50 Appendix B supplier for the SDRC, the staff finds the safety related portion of the RMS meets the requirements of IEEE Std 603-1991. As such, the staff finds the issues identified in RAI 274-8277, Question 07.01-34 is closed and resolved. The verification that the proposed markups are incorporated into the next revision of FSAR was a confirmatory item. The staff verified that the proposed markups have been incorporated into Revision 1 of DCD Tier 2 Section 7.1. As such, this confirmatory item has been satisfied.

The DCS conducts the functions of the operator interface, component-level control, automatic process control, high-level group control, and data processing for normal operation. The DCS is

designed with a redundant and fault-tolerant architecture. The P-CCS, which includes the NPCS, the PCS and the IPS are implemented using the DCS platform. The evaluation of the DCS is provided in Section 7.7 of this SER.

The QIAS-N is implemented using the Common Q platform in order to provide a diverse means of displaying important plant parameters from the IPS. Some I&C functions are implemented using independent systems to fulfill system design requirements. Non-standard systems include the DPS, DIS, NSSS integrity monitoring system (NIMS), RMS, and the seismic monitoring system (SMS). The evaluation of these systems is provided in Sections 7.5, 7.7, and 7.8 of this SER.

7.1.4.2.1 Safety-Related I&C Systems

The following section describes the safety-related I&C systems. The evaluation of how these systems meet applicable NRC regulations are provided in Sections 7.1.4.3-7.1.4.26, 7.2-7.6, and 7.9 of this SER.

PPS

The PPS is an integrated safety-related system that performs the reactor trip and ESF actuation functions. The PPS consists of four redundant divisions that perform the bistable, coincidence, initiation logic, and maintenance and test functions. The PPS initiates reactor trip and system-level ESF actuation functions to prevent plant conditions from exceeding the safety limit. To detect such conditions, the system utilizes measurements of the reactor core, reactor coolant system (RCS), main steam supply system, and containment building parameters. The PPS contains two subsystems, the Reactor Protection System (RPS) which performs reactor trip functions and the ESFAS which performs the ESF functions.

Section 4.2.2.1 of the Safety I&C System TeR states that the PPS consists of four redundant divisions (A, B, C, and D as depicted on Figure 4-4 of this technical report). Each PPS division contains a bistable processor rack and a local coincidence logic (LCL) rack. Each PPS redundant division receives the process and discrete signals directly from field sensors or via the APC-S, ENFMS, and CPCS. The bistable processor generates a reactor trip signal for each channel once the process variable exceeds a predetermined setpoint and sends its bistable trip status to each redundant LCL processor in the same division via non-fiber optic serial data link (SDL) and to LCLs in redundant divisions via fiber optic SDL. The redundant LCL racks within each division receive the bistable trip signals and perform a 2-out-4 (2oo4) coincidence logic for each reactor trip and ESFAS function.

Section 4.2.1 of the Safety I&C System TeR states that the PPS provides means for achieving manual initiation of each protective action. In addition, this section states that the PPS provides outputs for operator monitoring on the status of the PPS. The PPS provides alarms to the QIAS-N via the interface and test panel (ITP). The PPS also provides status alarms to the IPS via the maintenance and test panel (MTP).

The PPS includes four operator modules, one per division, located on the main control room (MCR) safety console. The operator modules provide the operator with information on the trip, pre-trip, and bypass status, initiation circuit status breaker position, and phase current status. The manual switches for operating bypass and setpoint reset control are provided on the MCR safety console and remote shutdown room (RSR) consoles.

The PPS also includes four ITPs and four MTPs that are divisionalized. The ITP monitors the PPS division status. It transfers the PPS status information to the QIAS-N for display and it supports testing functions. The MTP is the local human system interface (HSI) for maintenance and testing of the PPS. The MTP is used for setpoint modification and resetting of the reactor trip switchgear system (RTSS) and ESFAS initiation signals. The MTP provides the capabilities to perform surveillance and corrective maintenance, initiate tests, and display detailed system diagnostic messages. The trip channel bypass, all-bypass, operating bypass, and setpoint reset switches are provided on the MTP switch panel. These switches are directly hardwired to digital input modules of the bistable processor or LCL. The MTP also provides gateway function for unidirectional communication from the safety-related I&C system via the safety data network (SDN) to the DCS (data communications network-information (DCN-I) network).

CPCS

The CPCS has four redundant channels that compute the departure from nucleate boiling ratio (DNBR) and local power density (LPD) values using process values, reactor coolant pump (RCP) speed, Control Element Assembly (CEA) position and ex-core neutron flux. The CPCS compares the DNBR and LPD values against setpoints to determine if fuel design limits are exceeded. When these values exceed the setpoint, a trip signal is generated and transmitted to the PPS using hardwired cables.

DCD Tier 2 Section 7.1.2.3 states “The I&C systems that are applicable to 10 CFR 50.55a(h)(2) (Reference 10), as shown in Table 7.1-1, are designed in accordance with 10 CFR 50.55a(h)(2) except that the CPCS has two channels of a reed switch position transmitter (RSPT) for each control element assembly.” 10 CFR 50.55a(h)(2) does not apply to current applications. As such, in RAI 43-7887, Question 07.01-22, the staff requested the applicant to remove the reference to this requirement from the FSAR and modify the discussion on CPCS to the discussion on compliance to 10 CFR 50.55a(h)(3), which is the compliance requirement for current applicants. In the July 22, 2015, response to this RAI (ML15203A389), the applicant proposed to delete the reference to 10 CFR 50.55a(h)(2) in DCD Tier 2 Section 7.1.2.3. In addition, DCD Tier 2 Section 7.1.2.4 is revised to include discussion regarding the CPCS which was previously contained in Section 7.1.2.3. DCD Tier 2 Table 7.1-1 is revised to indicate 10 CFR 50.55a(h)(2) does not apply to the APR1400 design certification application. The applicant included proposed markups of the applicable DCD Tier 2 Sections 7.1.2.3, 7.1.2.4, and Table 7.1-1 in the response. Based on the commitment to remove the reference to 10 CFR 55.55a(h)(2) and the inclusion of the discussion of the CPCS in the DCD Tier 2 Section 7.1.2.4, the staff finds the issues identified in RAI 43-7887, Question 07.01-22, are closed and resolved. The verification that the proposed markups are incorporated into the next revision of FSAR was a confirmatory item. The staff verified that the proposed markups have been incorporated into Revision 1 of DCD Tier 2 Section 7.1. As such, this confirmatory item has been satisfied.

Reactor Trip System

The Reactor Trip System (RTS) performs reactor trip functions and consists of sensors, APC-S cabinets, ENFMS cabinets, CPCS cabinets, the RPS portion of the PPS cabinets, and RTSS cabinets. The RTS initiates a reactor trip based on the signals from the sensors that monitor various NSSS parameters and the containment pressure.

When a safety limit is approached, the RPS portion of the PPS initiates a signal that opens the reactor trip breakers. This action removes power from the control element drive mechanism (CEDM) coils, permitting the rods to fall by gravity into the core. The rapid negative reactivity insertion causes the reactor to shut down.

ESF System

The ESF system includes the actuation systems of ESF and the components that perform protective actions after receiving a signal from the ESFAS or the operator. The ESF system includes the containment isolation system, main steam isolation system, safety injection system (SIS), auxiliary feedwater system (AFWS), and containment spray system (CSS). The ESF system also includes sensors, APC-S cabinets, the ESFAS portion of the PPS, the safety portion of the RMS, and the ESF-CCS.

ESF-CCS

The ESF-CCS consists of four independent divisions that perform an additional 2oo4 voting logic, component control logic, and priority logic function. The group controller of each ESF-CCS division receives ESFAS initiation signals from each of the four PPS divisions and performs an additional 2oo4 coincidence logic to generate the ESF actuation signal. The group controller also receives two division ESFAS initiation signals derived from the RMS and performs 1oo2 logic to generate an ESF actuation signal. The output of the group controller is sent to the Loop Controller of the ESF-CCS. The Loop Controller performs the priority function for the operator's manual control signal and ESF actuation signal. The operator manual's control signal is received by the Loop Controller via the ESCM on the operator console. The Loop Controller executes the component control logic and outputs the component control signal to the CIM.

CIM

Section 4.1.1.7 of the Safety I&C System TeR states that the CIM is a hardware based safety module for ESF component control. The CIM receives component control signals from the ESF-CCS, DPS, DMA switches, and front panel control switch. The CIM prioritizes between input signals according to prioritization and transmits an output signal to the plant component according to the priority mode.

QIAS-P

The QIAS-P consists of two independent divisions that process plant parameters for display on the QIAS-P safety flat panel displays (FPDs) located on the MCR safety console. The QIAS-P receives input from the safety-related I&C system via the safety data network, APC-S via hardwired interfaces, and process instrumentation directly. The QIAS-P FPDs receive data from the QIAS-P via SDN. The QIAS-P also transmits sensor signals and the calculated variables to the IPS and QIAS-N through the MTP and ITP, respectively.

SRM-SECY-93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor Designs," Item II.T states that the alarm system for advanced light water reactors should meet the applicable EPRI requirements for redundancy, independence, and separation. In addition, alarms that are provided for manually controlled actions for which no automatic control is provided and that are required for the safety-related systems to accomplish the safety functions, shall meet the applicable requirements for Class 1E equipment and circuits. DCD Tier 2 Section 7.1.2.37 states "The alarm systems are required to meet the redundancy, independence, and safety alarm system requirements in accordance with SECY-93-087, Item II.T (Reference 5)." This statement does not reference the SRM to this SECY which is the Commission's position on alarm systems. In RAI 43-7887, Question 07.01-17, the staff requested the applicant to clarify in the FSAR how the alarm systems design conforms to the SRM to SECY-93-087, Item II.T. In the August 12, 2015

response to this RAI (ML15224B643), the applicant stated that the DCD Tier 2 Section 7.1.2.37, 7.1.5, and 7.5.5, and DCD Tier 2 Table 7.1-1, as well as Safety I&C System TeR, Section 3.3.2 is revised to reference the SRM to SECY-93-087, Item II.T. Section 3.3.2 of the Safety I&C System TeR describes how the requirements of the SRM to SECY-93-087, Item II.T are met. The applicant provided markups to these FSAR sections, and to the Safety I&C System TeR. Based on the commitment to modify the applicable FSAR sections, and the Safety I&C System TeR to reference the SRM to SECY-93-087, Item II.T, the staff finds that that the issue identified in RAI 43-7887, Question 07.01-17, is closed and resolved. The evaluation of how the APR1400 alarm system meets the requirements of the SRM to SECY-93-087, Item II.T is provided in Section 7.5 of this SER. The verification that the proposed markups are incorporated into the next revision of the FSAR and the Safety I&C System TeR was a confirmatory item. The staff verified that the proposed markups have been incorporated into Revision 1 of DCD Tier 2, Sections 7.1.2.37, 7.1.5, and 7.5.5, and DCD Tier 2 Table 7.1-1 and the Safety I&C System TeR, Revision 1. As such, this confirmatory item has been satisfied.

APC-S

The APC-S consists of four redundant safety channels that receive safety sensor signals and distributes them to the PPS, CPCS, ESF-CCS, QIAS-P, and DIS via hardwired interfaces. The APC-S includes signal conditioning/splitting equipment and the associated power supplies for sensor input. Qualified isolation devices are used to transmit safety signals from the APC-S to non-safety systems.

ENFMS

The ENFMS provides a means to measure reactor power level by monitoring the neutron flux leakage from the reactor vessel for reactor control, protection and information display. The ENFMS consists of four redundant safety channels. The ENFMS provides input to the PPS via hardwired discrete signals.

RTSS

The RTSS consists of four redundant safety divisions that receive reactor trip signals from the PPS, manual reactor trip switches, and the DPS through hardwired cables. The PPS interfaces with the undervoltage trip device of RTSS breakers. The DPS interfaces with the shunt trip device of the RTSS breakers. The RTSS disconnects the power to the digital rod control system (DRCS) for dropping CEAs into the reactor core after receiving a reactor trip signal from the PPS or a manual reactor trip signal from the MCR or RSR.

Safety Portion of the RMS

The safety portion of the RMS provides inputs to the ESF-CCS for the performance of BOP ESFAS initiation functions. These signals are transmitted as discrete contact signals to the digital input module in the group controllers within Divisions A and B of the ESF-CCS.

7.1.4.2.2 Non-Safety Related I&C Systems

The following section describes the non-safety I&C systems in the APR1400 design. The evaluation of how these systems meets applicable NRC regulations are provided in Sections 7.1.4.3-7.1.4.26, and 7.7-7.8 this SER.

PCS

The PCS is an integrated control system that provides reactor power level control. The PCS includes the reactor regulating system (RRS), reactor power cutback system (RPCS), and DRCS. The RRS/RPCS logic and DRCS cabinets include the redundant DCS controllers with associated v. The PCS is distributed to separate controller groups.

P-CCS

The P-CCS is designed to control non-safety components such as pumps, valves, heaters, and fans. The P-CCS performs data acquisition from field instruments and discrete/continuous controls, and provides process variables and status information to the IPS and QIAS-N for plant monitoring.

Standardized component control logic and input/output interfaces are provided for the various types of components to be controlled. Manual operator controls for the P-CCS are performed through the soft control display on the information flat panel display (IFPD) driven by the IPS. The P-CCS is distributed to separate controller groups.

NPCS

The NPCS consists of the pressurizer pressure control system (PPCS), pressurizer level control system (PLCS), feedwater control system (FWCS), steam bypass control system (SBCS), boron dilution alarm system, and single control loops of the chemical and volume control system (CVCS). The NPCS is implemented as a part of the P-CCS. The NPCS is distributed to separate controller groups.

NIMS

The NIMS detects selected conditions which indicate a deterioration or which could lead to a deterioration of the RCS pressure boundary. The system consists of internal vibration monitoring system, acoustic leak monitoring system, loose parts monitoring system, and RCP vibration monitoring system.

Fixed In-core Detector Amplifier System

The fixed in-core detector amplifier system (FIDAS) monitors the fixed in-core neutron detector current signals, performs the necessary signal conversion to engineering unit values and transmits them to the IPS. The IPS uses these signals for the core operating limit supervisory system (COLSS) to estimate the gross power distribution and thermal margin in the core, and fuel burn-up in each fuel assembly.

QIAS-N

The QIAS-N is a single division indication and alarm system that supports alternative plant operation if the IPS is unavailable. It provides the information required for emergency operating procedure (EOP) execution, safe shutdown, and important human actions under unavailable conditions of the operator consoles. The QIAS-N also provides a display of all Types B and C variables as defined in RG 1.97, “Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants,” Revision 4, which endorses IEEE Std 497-2002, “IEEE Standard Criteria for Accident Monitoring Instrumentation for Nuclear Power Generating Stations.” The QIAS-N displays selected variables of RG 1.97, Revision 4, Types D and E variables to support safe

shutdown of the plant and EOPs. Section 4.1.2.5 of the Safety I&C System TeR states that the QIAS-N receives divisionalized information from the four safety divisions via ITPs for safety variables and from the QIAS-N MTP for non-safety variables. The QIAS-N HSI is provided by the FPDs on the MCR safety console.

IPS

The IPS is the data processing system and HSI system that provide operational means for control and monitoring of the plant. It consists of networking equipment, along with an alarm server, application program server, database server, data link server and the IFPD installed on the operator consoles. The information is derived from other I&C systems and self-contained algorithms called application programs.

The IFPD provides the operator with the HSI resources including process mimic displays, alarms, and historical data access. It provides the soft control templates for manual component controls. The soft control of the IFPD is used for control associated with the P-CCS controllers directly attached to the non-safety DCS network. The IFPD is also used to control safety related equipment by sending safety component selection information via the ESCM.

Diverse Actuation System

The DAS includes the DPS, DIS, and DMA. The DPS is designed to mitigate the effects of an anticipated transient without scram (ATWS) event characterized by an AOO followed by a failure of the reactor trip portion of the protection system. In addition, the DPS is designed to mitigate the effects of a postulated software CCF of the digital safety-related I&C system coincident with the DBEs analyzed in DCD Tier 2 Chapter 15, “Transient and Accident Analysis.” The DIS is a single channel display that provides operators diverse indications in case of a software CCF of the safety-related I&C system. The DIS displays inadequate core cooling monitoring information, subset of accident monitoring instrumentation (AMI) parameters information, and a subset of emergency operation-related variables. The DMA switches consist of conventional hardwired switches on the MCR safety console for manual actuation of ESF components. The DMA switches control safety components via the CIM.

Turbine I&C System

The turbine generator control system (TGCS) is a microprocessor-based monitoring and control system that controls turbine speed, load, and flow for startup and normal operations. The TGCS operates the turbine main stop valves, control valves (CVs), intermediate stop valves, and intercept valves. The TGCS combines the capabilities of redundant digital processing and high-pressure hydraulics to regulate steam flow through the turbine. The TGCS provides the following turbine control functions:

- Automatic control of turbine speed and acceleration through the entire speed range.
- Automatic control of load and loading rate from no load to full load, with continuous load adjustment and discrete loading rates.
- Semi-automatic control of speed and load when it becomes necessary to take portions of the automatic control out of service while continuing to supply power to the system.
- Limiting of load in response to preset limits on operating parameters.

- Detection of dangerous or undesirable operating conditions, annunciation of detected conditions, and initiation of proper control response to such conditions.

- Monitoring of the status of the control system, including the power supplies and redundant control circuits.

- Testing of valves and controls.

The turbine overspeed protection function is provided by two major subsystems, a mechanical overspeed trip system and an electrical overspeed trip system. Turbine generator supervisory instrumentation is provided for operational analysis and malfunction diagnosis.

GDC 1 requires, in part, that

> structures, systems, and components important to safety shall be designed, fabricated, erected, and tested to quality standards commensurate with the importance of the safety functions to be performed. Where generally recognized codes and standards are used, they shall be identified and evaluated to determine their applicability, adequacy, and sufficiency, and shall be supplemented or modified as necessary to assure a quality product in keeping with the required safety function.

GDC 24 states,

> the protection system shall 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 of the protection system. Interconnection of the protection and control systems shall be limited so as to assure that safety is not significantly impaired.

In addition, Clause 5.6.3 of IEEE Std 603-1991 requires independence between safety-related and non-safety systems. DCD Tier 2 Section 7.1, states, "…independent systems such as the T/G control and protection system, the NSSS monitoring system, and the BOP monitoring system perform the required functions of a portion of the I&C systems." The staff reviewed Chapter 10 of the DCD Tier 2, and could not find information on the design of the T/G control and protection system, including how this system interfaces with safety-related I&C systems to meet the independence requirements of GDC 24 and IEEE Std 603-1991, Clause 5.6.3. In RAI 43-7887, Question 07.01-19, the staff requested the applicant to describe how the design of the T/G I&C system and the interfaces of this system to safety-related I&C systems (e.g., PPS) in order to demonstrate compliance to GDC 1, 24, and IEEE Std 603-1991, Clause 5.6.3. In addition, the applicant should clarify whether there are any other non-safety, standalone I&C systems that have interfaces to the safety-related I&C systems and demonstrate that these interfaces meet the requirements of GDC 24 and IEEE Std 603-1991, Clause 5.6.

In the August 12, 2015 response to RAI 43-7887, Question 07.01-19 (ML15224B643), the applicant stated that the turbine control system (TCS) interfaces with the PPS in the safety-related I&C systems for the turbine trip function on reactor trip. DCD Tier 2 Section 7.2.1.4, Item l and Figure 7.2-14 provide information about the turbine trip function and

functional logic. The PPS transmits the turbine trip signal via hardwired connection to the TCS when the reactor trip initiation signal is generated as indicated on the right side of Figure 7.2-14. The non-safety stand-alone I&C systems include the TCS, SMS, NIMS, and FIDAS. This response includes a table (Table 9-1) that summarizes the interfaces between the non-safety standalone I&C systems with safety-related I&C systems. In addition, this response states that that the PPS and ENFMS do not receive any signals from non-safety systems but only send signals to non-safety systems. Electrical isolation is provided in the PPS and ENFMS through isolation devices. Based on this response, the staff requested the applicant provide additional information in RAI 274-8277, Question 7.1-35, to determine whether the requirements of IEEE Std 603-1991, Clause 5.6.3 have been met for the interfaces between safety and standalone non-safety as described below:

1. Include in the FSAR the description from this RAI response regarding the interface between safety-related I&C systems and non-safety standalone system. This includes the statement that the PPS and ENFMS do not receive any signals from non-safety systems but only send signals to non-safety systems. Electrical isolation is provided in the PPS and ENFMS through isolation devices. The applicant should also include in the FSAR a clarification on whether these isolation devices are Class 1E qualified. In addition, include the information from Table 07.01-19-1 of this RAI response into the FSAR.

2. DCD Tier 2, Figure 7.2-14 only shows the PPS system interface logic diagram for Division D. It is unclear to the staff whether the interfaces depicted in this figure also applies to the other three PPS divisions. The applicant should clarify in the FSAR whether this figure applies to other PPS divisions. If there are differences between these interfaces for different divisions, provide a description of the differences in the FSAR.

3. DCD Tier 2 Section 10.2.2.3.3 states that each trip input is applied to a triple redundant protection module. 2oo3 majority voting is conducted within the protection system where possible to prevent spurious turbine trips and enhance protection system operation on an actual turbine trip. The turbine includes instrumentation for a trip on excess vibration and a remote trip input signal from the plant control system on a reactor trip. Since there are four divisions of PPS, and the turbine protection system only has triple redundancy, the staff was unclear about how each PPS division interface with the turbine protection system produce a turbine trip. This information should be provided in the FSAR.

In the December 29, 2015, response to RAI 274-8277, Question 7.1-35 (ML15363A340), the applicant committed to revise Section A.5.6 of the Safety I&C System TeR to clarify that the isolation devices in the PPS and ENFMS are Class 1E qualified. In addition, the applicant committed to include the information provided in Table 07.01-19-1 of the response to RAI 43-7887, Question 07.01-19 in Sections 7.2.1.4, 7.2.2.3, and 7.7.1.5 of DCD Tier 2 and Section 4.2.1.1 of the Safety I&C System TeR. The applicant clarified that Note 2 and 4 within DCD Tier 2 Figure 7.2-14 applies to all PPS divisions except for the CEA withdrawal prohibit (CWP) implementation.

The applicant also clarified that the "2-out-of-3 [(2oo3)] majority voting logic stated in DCD Tier 2 Section 10.2.2.3.3 is dedicated logic within the TCS to generate the turbine trip signal during the system abnormal condition (e.g., generator stator wind coolant low flow, generator stator inlet water low pressure). This 2oo3 voting logic does not use the signal from the 2oo4 voting logic implemented in the PPS.

For turbine trip, each PPS division interfaces with the TCS as follows:

- Two (2) sets of contact signals are provided per division in the RTSS. A total of eight (8) output signals are generated. The contact signal, as a momentary signal type, is provided through hardwired connections. Isolation is achieved by using Class 1E isolation relays within the RTSS.

- The two sets of contact signals from each division in the RTSS are inputted to two P-CCS cabinets through hardwired connections. The P-CCS cabinets have 2oo4 voting logic to prevent spurious turbine trip due to single P-CCS cabinet failure. The results of the 2oo4 voting logic in the P-CCS cabinets are provided to the TCS to initiate turbine trip.

The applicant committed to revise DCD Tier 2 Section 7.2.1.4 and Figure 7.2-14 of to include the above information.

The staff finds the commitment to revise the FSAR and the Safety I&C System TeR to include information on the use of Class 1E qualified systems between safety-related I&C systems and non-safety systems, and the description of the interface between the PPS and the TCS acceptable. However, the applicant did not include markups that incorporates all the information within Table 07.01-19-1 of RAI 43-7887, Question 07.01-19 (i.e., SMS, VMS and FIDAS do not have interfaces to safety-related I&C systems) as committed to in the response to RAI 274-8277, Question 07.01-35. As such, the staff requested the applicant to supplement the response to include the requested markups and RAI 43-7887, Question 07.01-19 is closed and unresolved. The staff is tracking this issue with RAI 274-8277, Question 07.01-35. Pending the resolution of this issue, RAI 274-8277, Question 07.01-35 was tracked as an open item. In the September 26, 2016 supplemental response to this RAI (ML16270A360), the applicant included the requested information in proposed markups to the DCD Tier 2 Sections 7.2.1.4, 7.2.2.3, 7.7.1.5, 7.9.1.4 and Figure 7.2-14 and Sections 4.2.1.1 and A.5.6 of the Safety I&C System TeR. Because the applicant included the requested information on how non-safety standalone systems interfaces with safety-related I&C systems into the FSAR and the Safety I&C System TeR, the staff finds the response acceptable. The staff verified that the proposed markups have been incorporated into Revision 1 of DCD Tier 2, Sections 7.2.1.4, 7.2.2.3, 7.7.1.5, 7.9.1.4 and Figure 7.2-14 and Sections 4.2.1.1 and A.5.6 of the Safety I&C System TeR, Revision 1. As such, the open item associated with RAI 274-8277, Question 07.01-35, is closed and resolved.

7.1.4.2.3 Data Communication Systems

The data communication systems utilized within the I&C systems provide communications between segment of a division, between divisions, and between systems. DCD Tier 2 Section 7.1.1.9 states:

> The [data communication systems] consist of hardware, protocols, and interfacing cabling. The systems are designed to provide the accurate, reliable, and timely transfer of data between control, protection, and information systems or within information systems. Input modules in cabinets acquire plant data, and the acquired data are transmitted to control and protection systems. The IPS and QIAS-N acquire information from data communication networks, process the data, and provide information to the display devices and other peripherals.

The staff evaluation of how the data communications system meets applicable NRC requirements are provided in Section 7.9 of this SER.

7.1.4.2.3.1 Data Communications for Safety I&C Systems

Data communications within the safety-related I&C system use the SDN and SDL. The SDN and SDL are equivalent to the Advant Field 100 network and high speed data link, respectively, in WCAP-16097, Common Q Platform Topical Report. The SDN is a bus that is used for intradivisional communication. Within the PPS, the SDN is used to connect the bistable processor, LCL Processor, operator module, MTP and ITP. DCD Tier 2 Section 7.9.1.1 states that the SDN is used for safety data communication in the following ways:

- Bistable processors and LCL processors send status data to MTP, operator module, and ITP through the SDN. Bistable processors and LCL processors receive testing data from the MTP through the SDN.

- The CPCS sends data for monitoring all processors, including inputs and calculated output to the MTP, operator module, and ITP through the SDN.

- The ESF-CCS group controller sends status data to the MTP and ITP through the SDN. The ESF-CCS Loop Controller sends ESF component status data to the MTP through the SDN.

- The QIAS-P processor sends the value and system status data to the IPS and QIAS-N through the MTP and ITP, respectively, which provide data communication isolation function and electrical isolation function. The QIAS-P processor communicates with the QIAS-P display, MTP, and ITP through the SDN.

- The ESCM sends component control signals to the control channel gateway (CCG) through the SDN. The ESCM receives the equipment feedback signal from the CCG through the SDN.

- The ITP receives status data from safety-related systems through the SDN.

- The MTP receives status data from safety-related systems and sends testing data and setpoint data through the SDN.

- The operator module receives status data from safety-related systems and sends testing data and setpoint data through the SDN. The setpoint data are sent to the CPCS.

- The control panel multiplexer (CPM) communicates with the bistable processor in the PPS, ITP, ESF-CCS group controller, and Loop Controller for receiving status information through the SDN.

- The CCG sends component control signals to the ESF-CCS Loop Controller through the SDN. The CCG receives the feedback data from the Loop Controller through the SDN.

The SDL communication is used to transmit the safety data within the safety channel or across safety channels for the performance of reactor trip and ESF actuation functions. Section 4.5 of the Common Q Platform Topical Report states that the SDL is a serial RS 422 link using high

level data link control protocol. The transmit data is optically isolated and transmitted to the other divisions. The SDL are broadcast only.

DCD Tier 2 Section 7.9.1.1 states that the SDL provides data communication as follows:

a. PPS

- SDL for LCL voting logic: There are two sets of interdivisional communication SDLs per redundant PPS division. Each bistable processor sends data to the LCL processors through the SDL.
- SDL for ESF-CCS group controller voting logic (actuation logic): Each LCL processor sends ESFAS initiation signals to the group controllers for selective 2oo4 voting logic through the SDL.

b. CPCS

- The CPCS consists of a core protection calculator (CPC) rack with two processor modules (CPC processor and auxiliary CPC processor) and a CEA calculator (CEAC) rack 1 and 2 (each with a CEAC and a CEA position processor (CPP)). The CPP sends CEA position signals to the CPP and CEAC processor through CPPs in the same channel and other channels using the SDLs.
- The CPP sends target CEA position signals to the CPC in the same channel through the SDLs.
- The CEAC sends penalty factors and target CEA position signals to the CPC in the same channel via the SDLs.

c. ESF-CCS

- The ESF-CCS uses SDLs to deliver control signals and data network for delivering status and monitoring signals.
- The ESF-CCS uses SDLs to send control signals to the LCs.

7.1.4.2.3.2 Data Communications Between Safety I&C and Non-Safety I&C Systems

DCD Tier 2 Section 7.9.1.4 describes the data communication interfaces between safety-related I&C systems and non-safety I&C systems. Each data communications interface from the safety-related I&C systems to non-safety I&C systems is described below.

Uni-directional Data Communication Interface from Safety to Non-safety Systems:

1. MTP: The MTP sends data to the IPS through the DCS gateway server uni-directionally using a fiber-optic cable.

2. The ITP sends the status and alarm information to the QIAS-N uni-directionally through the SDL.

3. The DCS gateway server receives data from safety-related systems with fiber-optic isolation.

Uni-directional Data Communication Interface from Non-safety to Safety Systems:

Ethernet communication is used to communicate from the IFPD to the ESCM. The signal from the IFPD provides component identification information to the ESCM. This signal is used for bringing up the control template on the ESCM display for the control of safety related components.

7.1.4.2.3.3 Data Communications Among Non-Safety I&C Systems

DCD Tier 2 Section 7.9.1.3 describes the DCN-I used for data communication among non-safety I&C systems. This section states that the DCN-I network provides non-safety data communication network to integrate the data from safety-related and non-safety systems. As shown on DCD Tier 2 Figure 7.9-1, the systems that are connected to the DCN-I network include:

- IPS server
- IFPD
- Engineering workstation
- Computer-based procedure system server
- DCS gateway to be interfaced with the MTP in each safety division
- Multi-channel gateway to be interfaced with the QIAS-N MTP
- P-CCS group controllers and LCs (including the NSSS-P-CCS controller)
- BOP monitoring systems
- TGCS
- PCS
- FIDAS
- NIMS

The DCN-I network is a redundant network but not physically separated and electrically isolated. The IPS server processors interface with the DCN-I network via a redundant data communication path. The IPS server processors communicate with the IPS display systems through the DCN-I network. The DCN-I network is independent of the QIAS-N network. The DCN-I network uses different data communication hardware and protocols from the QIAS-N network.

7.1.4.3 Quality Standards and Records

10 CFR Part 50, Appendix A, GDC 1, require SSCs to be designed, fabricated, erected, constructed, tested, and inspected to quality standards commensurate with the importance of the safety function to be performed. In order for the staff to evaluate whether the design met the requirements of 10 CFR Part 50, Appendix A, GDC 1, the staff used guidance as found in SRP Section 7.1, SRP Appendix 7.1-A, and SRP Table 7-1, "Regulatory Requirement, Acceptance Criteria, and Guidelines For Instrumentation and Control Systems Important to Safety." The guidance in SRP Appendix 7.1-A states that the staff is to confirm that the appropriate RGs and endorsed standards are identified as applicable for each I&C system important to safety.

DCD Tier 2 Section 7.1.2.2, references 10 CFR 50.55a(a)(1). However, the requirements of 10 CFR 50.55a(a)(1) have been moved to 10 CFR 50.54(jj) and 10 CFR 50.55(i). 10 CFR 50.54(jj) and 10 CFR 50.55 (i) does not apply to DC applicants. In addition, DCD Tier 2 Section 7.1.2.2 states that the "The I&C [instrumentation and controls] systems that are applicable to 10 CFR 50.55a(a)(1) (Reference 8), as shown in Table 7.1-1, are designed in accordance with 10 CFR 50.55a(a)(1) by complying with IEEE Std 603 (Reference 9), Clause 5.3." In RAI 43-7887, Question 07.01-10 and RAI 43-7887, Question 07.01-11, the staff requested the applicant to modify the FSAR to reflect the change in regulations such that the application only references GDC 1.

In the November 4, 2015 response to RAI 43-7887, Question 07.01-10, and RAI 43-7887, Question 07.01-11 (ML15308A591), the applicant committed to delete references 10 CFR 50.55a(a)(1) in the FSAR. The applicant included markups in the response with the proposed revisions. Based on this commitment, the staff finds the response to RAI 43-7887, Question 07.01-10 and RAI 43-7887, Question 07.01-11 acceptable, and thus finds the issues identified in these two RAIs are closed and resolved. The verification that the proposed markups are incorporated into the next revision of the FSAR was a confirmatory item. The staff verified that the proposed markups have been incorporated into Revision 1 of DCD Tier 2 Chapter 7 and the Safety I&C System TeR, Revision 1. As such, these confirmatory items have been satisfied.

The applicant commits to conform to the RGs and standards referenced in the SRP Sections 7.1 through 7.9. The staff notes that DCD Tier 2 Section 1.9.1, "Conformance with Regulatory Guides," states that DCD Tier 2 Table 1.9-1, "APR1400 Conformance with Regulatory Guides," provides a conformance assessment of the RGs as they apply to the APR1400 design certification. The staff's review of DCD Tier 2 Table 1.9-1 confirmed the applicant committed to conform to the RGs referenced in the SRP Sections 7.1-7.9. Additionally, the staff found that DCD Tier 2, Sections 7.1.2.38 – 7.1.2.57, and Table 7.1-1, "Regulatory Requirements Applicability Matrix," indicate the applicable I&C systems and corresponding RGs and standards for which the applicant commits conformance.

Exceptions to guidance are discussed in the relevant section of this SER. For example, the applicant took exception to some software configuration regulatory positions in RG 1.169, "Configuration Management Plans for Digital Software Used in Safety Systems of Nuclear Power Plants," Revision 1, which endorses IEEE Std 828-2005, "Standard for Software Configuration Management Plans." The staff reviewed this exception in the Software Program Manual in Section 7.1.4.7 of this SER.

The applicant commits to conform to the SRP BTPs in DCD Tier 2 Section 1.9.2, "APR1400 Conformance with the Standard Review Plan." Additionally, the staff found the DCD Tier 2

Table 7.1-1 indicates the applicable I&C systems and the corresponding SRP BTPs for which the applicant commits conformance. DCD Tier 2 Table 1.9.2 states conformance to SRP BTP 7-3, "Guidance on Protection System Trip Point Changes for Operation with Reactor Coolant Pumps Out of Service," but FSAR Table 7.1-1 and Section 7.1.2.60 states SRP BTP 7-3 is not applicable because "the reactor is not permitted to operate with reactor coolant pump out of service. The PPS trips the reactor by low reactor coolant flow. Therefore, [SRP] BTP 7-3 is not applicable." The staff issued RAI 301-8280, Question 07.01-43, requesting the applicant to reconcile the conformance statement and not applicable assertions. In the December 28, 2015, response to RAI 301-8280, Question 07.01-43 (ML15362A593), the applicant committed to revising DCD Tier 2 Table 1.9-2 to show that SRP BTP 7-3 is not applicable to the APR1400 design. The APR1400 design does not permit operation with a reactor coolant pump out of service; if flow is lost in any loop, the PPS would trip the reactor due to low reactor coolant flow. Thus, based on the provision of a reactor trip upon low reactor coolant flow conditions, the staff finds the response to RAI 301-8280, Question 07.01-43, acceptable. The verification that the proposed markups are incorporated into the next revision of the FSAR was a confirmatory item. The staff verified that the proposed markups have been incorporated into Revision 1 of DCD Tier 2, Chapter 1, Table 1.9-2. As such, these confirmatory items have been satisfied.

Exceptions to SRP BTPs are evaluated in the relevant section of this SER. For example, the applicant took exception to SRP BTP 7-12, "Guidance on Establishing and Maintaining Instrument Setpoints" with regards to the surveillance and calibration interval. The staff reviewed this exception in Section 7.1.4.25 of this SER, which provides the Setpoint Methodology technical evaluation.

Section 8 of the Safety I&C System TeR states, "The [safety-related] I&C system is implemented on a common PLC platform using Common Q. The platform has been dedicated and qualified for nuclear power plants and accepted by NRC after reviewing Common Qualified Platform Topical Report Revision 3. The platform is configured using various hardware building blocks and loaded with application software to develop safety-related I&C systems such as PPS, ESF-CCS, CPCS, and QIAS-P." The staff issued RAI 301-8280, Question 07.01-44, to request the applicant to identify the ITAAC which verifies that the Common Q platform is installed in accordance with the approved Common Q Platform Topical Report, and as necessary, provide corresponding updates to the FSAR The staff also requested that the applicant provide details regarding any modifications to the Common Q platform design, processes, hardware, and software, since the Common Q Platform Topical Report was approved by the staff. In the April 22, 2016 response to RAI 301-8280, Question 07.01-44 (ML16113A458), the applicant committed to include an additional ITAAC to verify that the Common Q platform is installed in accordance with the approved Common Q Platform Topical Report for these systems: PPS, CPCS, QIAS-P, and ESF-CCS. The response also addressed the details regarding any modifications to the Common Q platform since the Common Q Platform Topical Report was approved by the staff by referencing the Common Q Supplemental TeR. The modifications are evaluated in other parts of this safety evaluation. Overall, the staff finds the response acceptable since the additional ITAAC will help verify that the Common Q platform are installed properly. The verification that the proposed markups to RAI 301-8280, Question 07.01-44 are incorporated into the next revision of the FSAR was a confirmatory item. The staff verified that the proposed markups have been incorporated into Revision 1 of DCD Tier 1, Sections 2.5.1.1, 2.5.3.1, 2.5.4.1, and Tables 2.5.1-5, 2.5.3-3, 2.5.4-4 and Revision 1 of DCD Tier 2 Section 7.1. As such, these confirmatory items have been satisfied.

Based on the commitment in the FSAR to conform to the guidance in the RGs and the endorsed standards and SRP Chapter 7, the staff concluded that the APR1400 I&C system design meets the requirements of GDC 1.

7.1.4.4 Design Bases

10 CFR 50.55a(h)(3) requires compliance to IEEE Std 603-1991. Clause 4 of IEEE Std 603-1991 is the design bases requirement for safety-related I&C systems.

The Safety I&C System TeR, Appendix A, "Conformance to IEEE Std 603-1991," provides safety analysis for compliance with Clause 4 of IEEE Std 603-1991. Below is the staff's review of APR1400 safety analysis of design bases.

Clause 4.1 of IEEE Std 603-1991 requires the identification of the design basis event (DBE) applicable to each mode of operation, and Clause 4.2 requires documentation of the safety functions and corresponding protective actions of the execute features for each DBE. The safety-related systems are designed to protect the health and safety of the public by limiting the release of radioactive material following AOOs and postulated accidents (PAs). The Safety I&C System TeR, Appendix A, Section A.4.1, states, "The RPS is designed to ensure adequate protection of the fuel, fuel cladding, and RCS boundary during AOOs…the RPS is designed to assist the ESF Systems in mitigating the consequences of accidents. The ESFAS mitigates the result of an event to within the allowable value during the DBE described in [DCD Tier 2] Chapter 15." The Safety I&C System TeR, Appendix A, Section A.4.2, states, "The RPS consists of fifteen trips in each of the four RPS divisions that will initiate the required automatic protective action utilizing a coincidence of two or more trip signals." The PPS automatically initiates appropriate protective action when a condition monitored by the system reaches a preset level. The safety analyses demonstrate that even under conservative critical conditions for design basis accidents (DBAs), the safety-related system provides confidence that the plant is put into and maintained in a safe state following an AOO/PA. Table 7.1-1 lists the reactor protection system monitored variables and ranges. Table 7.1-2 lists the reactor protection system trip functions, inputs and purposes. Section 4.2.1.1 of the Safety I&C System TeR states, "the PPS also automatically initiates a turbine trip signal to the TCS. The turbine trip signal is generated from the PPS when the PPS generates a reactor trip signal."

Table 7.1-1. Reactor Protection System Monitored Plant Variable Ranges
Source: DCD Tier 2 Table 7.2-2

Monitored Variable	**Minimum**	**Nominal (full power)**	**Maximum**
Neutron flux power, percent (%) of full power	Near 2 × 10-8	100	200
Cold leg temperature, degrees (°) C (°F)	230 (446)	291 (555)	330 (626)
Hot leg temperature, °C (°F)	250 (482)	324 (615)	350 (662)
Pressurizer pressure (narrow range), kilogram (kg)/centimeter (cm)^2 Atmosphere (A) (pounds per square inch absolute (psia))	105 (1,494)	158.2 (2,250)	175 (2,489)
Pressurizer pressure (wide range), kg/cm^{2}A (psia)	0 (0)	158.2 (2,250)	210.9 (3,000)
CEA positions	Full in	NA	Full out
Reactor coolant pump speed, rotations per minute (rpm)	0	1190	1320
Steam generator water level (wide range), %	0	77	100
Steam generator water level (narrow range), %	0	50	100
Steam generator pressure, kg/cm^{2}a (psia)	0 (0)	70.3 (1000)	105.0 (1494)
Containment pressure, cm/H_2O (psig)	-300 (-4)	0 (0)	1200 (17)
Steam generator primary pressure differential, cm/H_2O (psig)	0 (0)	2110 (30)	5000 (71)

Table 7.1-2. Reactor Protection System Trip Functions Source: Safety I&C System TeR, Appendix A		
Reactor Trip Function	**Input**	**Purpose**
Variable Overpower Trip	Neutron flux power from ENFMS	To provide a reactor trip to assist the ESF systems in the event of an ejected CEA accident
High Logarithmic Power Level Trip	Neutron flux power from ENFMS	To ensure the integrity of the fuel cladding and RCS boundary in the event of unplanned criticality from a shutdown condition, resulting from either dilution of the soluble boron concentration or uncontrolled withdrawal of CEAs.
High LPD Trip	• Neutron flux power and hot pin axial power distribution from the ENFMS • Radial peaking factors from CEA position measurement system (reed switch assemblies) • Delta T power from coolant temperatures, pressure, and flow measurements • Penalty factors from CEACs for CEA deviation within a subgroup • Penalty factors generated within the CPC for subgroup deviation and groups out-of-sequence	To prevent the linear rate ((Watt (W)/cm or kilowatt (kW)/ft) of fuel pin in the core from exceeding fuel design limits in the event of AOOs

Table 7.1-2. Reactor Protection System Trip Functions Source: Safety I&C System TeR, Appendix A		
Reactor Trip Function	**Input**	**Purpose**
Low DNBR Trip	• Neutron flux power and hot pin axial power distribution from the ENFMS • Radial peaking factors from CEA position measurement system (reed switch assemblies) • Delta T power from coolant temperatures, pressure, and flow measurements • Penalty factors from CEACs for CEA deviation within a subgroup • Penalty factors generated within the CPC for subgroup deviation and groups out-of-sequence • RCS pressure from pressurizer measurement • Reactor coolant mass flow from reactor coolant pump speeds and temperatures • Core inlet temperature from reactor coolant cold leg temperature measurements	To prevent the DNB ratio of the coolant channel in the core from exceeding the fuel design limit in the event of AOOs. In addition, this trip will provide a reactor trip to assist the ESF systems in limiting the consequences of the steam line break outside containment, steam generator (SG) tube rupture, and reactor coolant pump shaft accidents
High Pressurizer Pressure Trip	Reactor coolant pressure from narrow range pressurizer pressure measurements	To assure the integrity of the RCS boundary for any defined AOO that could lead to over pressurization of the RCS
Low Pressurizer Pressure Trip	Reactor coolant pressure from wide range pressurizer pressure measurements	To provide a reactor trip to assist the ESF systems in the event of reduction in system pressure and a (LOCA)
Low SG1,2 Water Level Trips	Level of water in each SG downcomer region from wide range differential pressure measurements	To provide a reactor trip to assist the ESF systems ensuring that there is sufficient time for actuating the auxiliary feedwater pumps to remove decay heat from the reactor in the event of a reduction of SG water inventory

Table 7.1-2. Reactor Protection System Trip Functions Source: Safety I&C System TeR, Appendix A		
Reactor Trip Function	**Input**	**Purpose**
Low SG1,2 Pressure Trips	Steam pressure in each SG	To provide a reactor trip to assist the ESF systems in the event of a steam line break accident
High Containment Pressure Trip	Pressure inside containment	To assist the ESF systems by tripping the reactor coincident with the initiation of safety injection caused by excessive pressure in containment
High SG1,2 Water Level Trips	Level of water in each SG downcomer region from narrow range differential pressure measurements	To assist the ESF systems by tripping the reactor coincident with initiation of main steam isolation caused by a high SG water level
Low Reactor Coolant Flow of SG1,2	Differential pressure measured across the SG primary side	To provide a reactor trip in the event of a reactor coolant pump sheared shaft
Manual Reactor Trip	Two independent pairs of trip switches are provided at MCR and one set of trip switches in the RSR consoles	Manual reactor trip is provided to permit the operator to trip the reactor

Section A.4.2 of the Safety I&C System TeR states, “the ESFAS utilizes bistable logic and coincidence logic in the PPS and coincidence logic and component control logic in the ESF-CCS to generate actuation signals. Actuation signals are provided as input signals to the ESF system. Upon receipt of ESFAS initiation signals from the PPS, the ESF-CCS generates actuation signals.” Table 7.3-2 of DCD Tier 2 lists the DBEs requiring ESF system action. For example, steam generator tube rupture (SGTR) DBE would require these ESF System Actions: Containment Isolation, Main Steam Isolation, Safety Injection, Auxiliary Feedwater, and Control Room Emergency Ventilation. Table 7.3-6 of the DCD Tier 2 lists the ESFAS monitored variables and ranges, and duplicated in Table 7.1-3 below. Table 7.1-4 lists ESF functions and the initiating events.

Table 7.1-3. Engineered Safety Feature Monitored Variable Ranges Source: DCD Tier 2 Table 7.3-6			
Monitored Variable	**Minimum**	**Nominal (full power)**	**Maximum**
Pressurizer pressure (narrow range), kg/cm^{2}A (psia)	0 (0)	158.2 (2250)	210.9 (3000)
Containment pressure, cm/H_2O (psig)	-400 (-5.7)	0 (0)	5600 (79.5)
Steam generator pressure, kg/cm^{2}A (psia)	0 (0)	70.3 (1000)	105.0 (1494)
Steam generator water level (wide range), %	0	77	100
Steam generator water level (narrow range), %	0	50	100
Containment upper operation area radiation level, mSv/hr	10	-	10^8
Containment operation area radiation level, millisevert (mSv)/hour (hr)	10^{-3}	-	10^2
Spent fuel pool area radiation level, mSv/hr	10-3	-	102
Control room air intake radiation level, Becquerel (Bq)/cubic centimeter (cc)	3.7 x 10^{-2}	-	3.7 x 10^3

Table 7.1-4 Engineered Safety Features Functions Source: Safety I&C System TeR, Appendix A	
ESF Function	**Initiated by**
Containment Isolation Actuation Signal (CIAS)	• High containment pressure trip • Low pressurizer pressure trip
Containment Spray Actuation Signal (CSAS)	• High-high containment pressure trip
Main Steam Isolation Signal (MSIS)	• High containment pressure trip • Low SG1/2 pressure trips • High SG1/2 water level trips
Safety Injection Actuation Signal (SIAS)	• High containment pressure trip • Low pressurizer pressure trip
Auxiliary Feedwater Actuation Signal (AFAS)-1	• Low SG1 water level trips
AFAS-2	• Low SG2 water level trips

The staff reviewed documentation in DCD Tier 2 Chapter 15 analyses, and Sections 7.2 (RPS) and 7.3 (ESF) of the FSAR design details for corresponding protective actions. Based on the staff's evaluation in these SER sections, the staff finds the APR1400 design meets the requirements of IEEE Std 603-1991, Clauses 4.1 and 4.2.

Clause 4.3 of IEEE Std 603-1991 requires documentation of the permissive conditions for each operating bypass capability that is to be provided. The RPS and ESFAS are designed such that protective functions are initiated and accomplished during various reactor operating modes. Table 7.2-1 and Table 7.3-1 of the DCD Tier 2, lists the operating bypass permissive and condition for removal for RPS and ESFAS, respectively. The four RPS operating bypass permissives are DNBR and LPD, Pressurizer pressure, High log power level, and CPC CWP. There is one ESFAS operating bypass permissive, Pressurizer pressure. Where operating requirements necessitate automatic or manual block of a protective function, the block is automatically removed whenever the appropriate permissive conditions are not met. The staff finds that the RPS and ESFAS satisfies Clause 4.3 of IEEE Std 603-1991 requirement to document the permissive conditions for each operating bypass capability. Hardware and software used to achieve automatic removal of the block of a protective function are required to be designed in accordance with the same criteria as the protective function. The operating bypass capability design is evaluated in Section 7.1.4.23 of this SER.

Clause 4.4 of IEEE Std 603-1991 requires documentation of protective system variables and range and rates of change. Section A.4 of the Safety I&C System TeR states:

> The RPS monitors the following generating station conditions in order to provide adequate protection during AOOs: core power (neutron flux), [RCS] pressure, DNBR in the limiting coolant channel in the core, peak local power density in the

limiting fuel pin in the core, SG water level, and reactor coolant flow. The RPS monitors the following generating station conditions in order to assist the ESF in mitigating the consequences of accident: core power, RCS pressure, SG pressure, containment pressure, and reactor coolant flow.

DCD Tier 2, Sections 7.2 and 7.3, describe the variables required to be monitored for protective action and ranges and rates of change. Based on the review of documentation in the Safety I&C System TeR, and FSAR Sections 7.2 and 7.3, which are evaluated in Sections 7.2 and 7.3 of this SER, the staff finds that the PPS design meets Clause 4.4 of IEEE Std 603-1991 requirement to identify protective system variables to provide adequate protection during AOOs and to assist the ESF in mitigating the consequences of accidents.

Clause 4.5 of IEEE Std 603-1991 requires identification of protective actions whose operation may be controlled by manual means. In the APR1400 design, means are provided in the MCR for manual initiation of protective functions at the system level. The manual controls are a backup to the automatic protection provided by the PPS. Manual actuation relies on minimum equipment and once initiated, proceeds to completion unless the operator deliberately intervenes. Failure in the automatic initiation portion of a system-level function does not prevent the manual initiation of the function. The PPS HSI design includes a minimum inventory of dedicated or fixed-position displays and controls. The fixed-position displays and alarms are available in the MCR to support manual initiation of protective functions. Based on the description above, and the evaluation in Sections 7.2 and 7.3 of this SER, the staff finds that the PPS design meets the IEEE Std 603-1991, Clause 4.5 requirement.

Clause 4.6 of IEEE Std 603-1991 requires identification of the minimum number and location of sensors for spatially-dependent process variables. Multiple sensors with spatial distribution are specified because the measurement of certain process variables, notably neutron flux and core exit temperature, can depend on the spatial location of the sensors. Section A.4 of the Safety I&C System TeR states, “The number and location of the sensors provided to monitor those variables in item 4 are given in Tables 7.2-3 and 7.3-4 of the [DCD Tier 2]. The location of precision resistance temperature detectors (RTDs) for measuring RCS log leg temperature is assigned to measure appropriate coolant transmission effects by temperature difference and temperature distribution of hot leg.” Table 7.2-3 of DCD Tier 2 states there are eight precision RTDs in the hot leg piping which is used by the CPC for generating high LPD and low DNBR trips. Table 7.5-1 of DCD Tier 2 states Reactor Coolant Hot Leg Temperature (Wide Range) is a 4 channel, AMI Types A, B, and D Variables, and that there are 2 Hot Leg signals per division (QIAS-P). It was not clear to the staff what is meant by 2 Hot Leg signals per divisions (QIAS-P) and it was not clear to the staff the geometry of the installed hot leg sensors. The staff issued RAI 301-8280, Question 07.01-46 to request the applicant to clarify the description in Table 7.5-1 and to describe the geometry of the installed hot leg sensors. In the December 28, 2015, response to RAI 301-8280, Question 07.01-46 (ML15362A593), the applicant stated, in part, “in DCD Tier 2 Table 7.5-1, for “Reactor Coolant Hot Leg Temperature (Wide Range),” the “Channel Number” column specifies that there are 4 RTD sensors (T-132A, B and T-133A,B) and channels assigned to the RCS hot legs, in total, for AMI. The “Ambiguity (Division)” column of Table 7.5-1 specifies that there are “2 Hot Leg signals per division (QIAS-P).” There are two (2) hot legs which each have two (2) sensor signals (T-132A, T-133A for division A and T-132B, T-133B for division B).” After the May 2016 meeting, staff requested clarifications since DCD Tier 2 Table 7.3-4, “ESFAS Sensors,” do not have any information regarding the number and location of the RCS hot leg temperature sensors, as stated in Section A.4 of the Safety I&C System TeR. Also, DCD Tier 2 Table 7.2-3, “Reactor Protection System Sensors,” states there are 8 RTD sensors for hot leg temperature. The staff is inferring that there are 4 sensors for

each steam generator based on the attached non-FSAR instrument loop diagram of the response. The schematics, "Instrument Loop Diagram for RCS Loop 1 Temperatures," and "Instrument Loop Diagram for RCS Loop 2 Temperatures," do not show the location of the sensors per the RAI response. Lastly, the response stated that "the 'Channel Number' column specifies that there are 4 RTD sensors." The use of "Channel Number" to specify number of sensors is not obvious to the staff. Additional clarification is needed in the FSAR.
RAI 301-8280, Question 07.01-46 was tracked as an open item. In the supplemental response to RAI 301-8280, Question 07.01-46 (ML16292A474), the applicant clarified the design of the RCS hot leg and cold leg temperature sensors by revising DCD Tier 2, Tables 7.2-3 and 7.5-1 to identify "Channel Number" as the number of sensors. The staff finds the proposed changes to DCD Tier 2 in RAI 301-8280, Question 07.01-46 are acceptable. The incorporation of the proposed markup into the next revision of DCD Tier 2 was a confirmatory item. The staff verified that the proposed markups have been incorporated into Revision 1 of DCD Tier 2, Tables 7.2-3 and 7.5-1. As such, these confirmatory items have been satisfied.

The evaluation of spatial dependence ITAAC are documented in Section 14.3.5 of this SER.

Clause 4.7 of IEEE Std 603-1991 requires, in part, that the range of transient and steady-state conditions be identified for the energy supply and the environment during normal, abnormal, and accident conditions under which the system must perform. The I&C equipment is environmentally qualified to meet the accident conditions through which it operates to mitigate the consequences of the accident. The equipment is seismically qualified to meet safe shutdown earthquake levels. The safety-related system is powered by Class 1E direct current power and an uninterruptible power supply system. Section A.4 of the Safety I&C System TeR states "…the safety-related I&C system is capable of performing its intended function under the most degraded conditions of the energy supply, as addressed in Section 8.3 of the [DCD Tier 2]." Based on the information provided in Section A.4 of the Safety I&C System TeR and the evaluation provided in Section 7.1.4.8 of this SER, the staff finds the PPS design meets the IEEE Std 603-1991, Clause 4.7 requirements.

Clause 4.8 of IEEE Std 603-1991 requires, in part, the identification of conditions having the potential to cause functional degradation of safety-related system performance and the proposed protective action. The PPS is located in plant areas that provide protection from accident related hazards such as missiles, pipe breaks, and flooding. The redundant trains of the PPS are isolated from each other and isolated from non-safety systems. Isolation is used to achieve functional independence and communication independence. The staff's evaluation of functional and communication independence is documented in Section 7.9 of this SER. The redundant train arrangement provides independent operations in case of fires or electrical faults. Section A.4 of the Safety I&C System TeR states:

> [The] RPS and ESFAS logic design takes account of functional degradation that could occur in the following conditions: system actuation due to the power loss of measurement channel, appropriate system-level protective action due to single accident in the system, the system is verified according to [IEEE Std 344-2004 (as endorsed by RG 1.100, "Seismic Qualification of Electric and Mechanical Equipment for Nuclear Power Plants," Revision 3)] to demonstrate that the RPS and ESFAS can perform the intended function for seismic conditions, the RPS is verified according to [IEEE Std 323-2003, "Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations," (as endorsed by RG 1.209, "Guidelines for Environmental Qualification of Safety-Related Computer Based Instrumentation and Control Systems in Nuclear Power Plants" Revision 0)] to

> demonstrate that the RPS can perform the intended function for environment conditions, and system components are qualified according to established plan for [electromagnetic compatibility (EMC)] that requires equipment to function properly when subjected to electrical surges, electromagnetic interference, radio frequency interference, and electrostatic discharge.

Based on conformance to RG 1.100, Revision 3, as stated in Section A.4 of the Safety I&C System TeR and the staff's evaluation in Sections 7.1.4.8 and 7.3.4.3.1 of this SER related to electromagnetic interference (EMI) / radio frequency interference (RFI), the staff finds the PPS design meets the IEEE Std 603-1991, Clause 4.8 requirements.

Clause 4.9 of IEEE Std 603-1991 requires the applicant to identify the methods used to determine that the reliability of the safety-related system design is appropriate. In addition, it requires that the applicant identify the qualitative or quantitative goals used to verify the reliability imposed on the system design. The Safety I&C System TeR, Section 7, "Equipment Reliability," describe a qualitative evaluation to identify failure modes of the protection system and effects. This failure modes and effects analysis (FMEA) demonstrates that the protection system can sustain a single failure and can still perform its intended safety function. The acceptability of the FMEA, and hazards of the PPS as described in FSAR Sections 7.2 and 7.3 is in Sections 7.2 and 7.3 of this SER, respectively. Based upon the FMEA provided in Safety I&C System TeR, Section 7 and the staff's evaluation in Section 7.2.4.3 of this SER, the staff finds the PPS design meets the IEEE Std 603-1991, Clause 4.9 requirements.

Clause 4.10 of IEEE Std 603-1991 requires identification of the critical points in time or plant conditions for which the protective actions shall be initiated. Section A.4 of the Safety I&C System TeR states:

> The point, for which the reactor shutdowns shall be initiated (trip setpoint) is described in DCD Tier 2, Tables 7.2-4 and 7.3-5A, and initial event and frequency causing initiation of protective action are described in Table 15.0-3 of the [FSAR]….The point in time for the proper completion of RPS safety function is when CEA is injected completely into the core…Core reactivity maintains the subcritical state with sufficient margin corresponding to TS and does not exceed thermal design limit of core and [RCS] by removing core decay heat at controlled cooling rate…the accident analysis in DCD Tier 2, Chapter 15 does not consider manual control in the first 30 minutes after accident and the point in time for automatic control of protection system is set based on accident analysis results.

The detailed evaluation of response time analysis is addressed in Section 7.1.4.9 of this SER. Based on the information provided in Section A.4 of the Safety I&C System TeR and the ESF-CCS response time evaluation in Section 7.3.4.3.1 of this SER, the staff finds the PPS design meets the IEEE Std 603-1991, Clause 4.10 requirements to identify critical points in time or plant conditions for which protective actions are initiated.

Clause 4.11 of IEEE Std 603-1991 requires identification of the equipment protective provisions that prevent the safety-related systems from accomplishing their safety functions. The applicant should discuss the protective features designed to place the safety-related system in a safe state. Section 4.6.1.8 of the Safety I&C System TeR states:

> The [safety-related] I&C system application uses the data communication system to fail into a safe state or into a state established as acceptable in the event of

loss of power supply. These communication systems are also used by the application so that any single failure does not prevent proper protective action at the system-level. The FMEA shows that no single failure results in the failure of more than one of the four redundant divisions of safety-related I&C system or prevents proper protective action at the system-level.

Reactor trip circuit safe state is to trip. ESFAS safe state is fail-as-is. Section A.4 of the Safety I&C System TeR states, “there is no equipment protective provisions that prevent the safety-related systems from accomplishing their safety functions” but did not discuss the equipment protective functions. Typically, nuclear power plant actuators have equipment protective functions, such as overcurrent protection, thermal overload protection, and emergency diesel generator (EDG) protective features; some of which could cause the equipment to trip even in the presence of a safety actuation signal. In RAI 301-8280, Question 07.01-47, the staff requested the applicant to discuss the protective functions for safety-related equipment and describe whether these protective functions could trip/disable the safety-related equipment in the presence of a safety actuation signal or why it could not trip/disable safety-related equipment in the presence of a safety actuation signal. In the February 26, 2016 response to RAI 301-8280, Question 07.01-47 (ML16057A086), the applicant stated, in part, “the [PPS] and [ESF-CCS] consist of redundant channels with independence features. The safety functions are initiated and accomplished by the PPS and ESF-CCS at the system level. Therefore, there is no single failure of an equipment protective device which prevents initiating and accomplishing the safety functions at the system level. Each component control logic in the ESF-CCS loop controller detects the conditions of equipment and determines if the equipment can be operated,” and the applicant provided examples for the load center circuit. At the May 2016 meeting, the staff asked if these equipment protective devices can be controlled by the ESCM (safety) by means of the IFPD (non-safety). In other words, the applicant should clarify whether the component data from IFPD to ESCM can be used to control these equipment protective devices. The staff was concerned that a non-safety IFPD can initiate protective functions. In the September 9, 2016, supplemental response to RAI 301-8280, Question 07.01-47 (ML16253A283), the applicant stated, “the ESCM provides component control signals such as start or stop signal for components. The equipment protective logic is implemented in the component control system or electrical panel. Therefore, the component data from IFPD to ESCM are not used to control equipment protective devices.” The staff finds the response acceptable since the non-safety system (e.g., IFPD) cannot initiate protective functions. The staff finds the proposed changes to the FSAR in RAI 301-8280, Question 07.01-47 are acceptable because non-safety systems cannot initiate equipment protective features that could disable the safety function. The incorporation of the proposed markup into the next revision of FSAR was a confirmatory item. The staff verified that the proposed markups have been incorporated into Revision 1 of the Safety I&C System TeR, Section A.4, Item 11. As such, these confirmatory items have been satisfied.

The staff finds that the PPS design meets the IEEE Std 603-1991, Clause 4.11 requirements because the safety-related systems are designed to fail in a safe state, and that there is no equipment protective provisions that would prevent the safety-related systems from accomplishing their safety functions.

Clause 4.12 of IEEE Std 603-1991 requires identification of any other special design basis that may be imposed on the system design. The APR1400 design provides a DAS, which is a non-safety system that is diverse and separate from the safety PPS and ESF-CCS. The DAS provides functions necessary to reduce the risk associated with postulated CCFs of critical

protection systems. DCD Tier 2, Chapter 7, has documented the design bases for each subsystem, including the bases for diversity, interlocks, and regulatory criteria. The staff evaluation of the DAS and interlocks is documented in Sections 7.6 and 7.8 of this SER respectively. Because the applicant has identified the special design basis features within the APR1400 design, the staff finds the applicant has met the requirements of IEEE Std 603-1991, Clause 4.12.

7.1.4.5 Single Failure Criterion

10 CFR Part 50, Appendix A, GDC 21, requires that the protection system 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 assure 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. In addition, IEEE Std 603-1991, Clause 5.1, states that the safety-related system must perform all safety functions required for a DBE in the presence of (a) any single detectable failure within the safety-related systems concurrent with all identifiable but non-detectable failures, (b) all failures caused by the single failure, and (c) all failures and spurious system actions that cause or are caused by the DBE requiring the safety functions. The single failure could occur prior to, or at any time during, the DBE for which the safety-related system is required to function. In other words, IEEE Std 603-1991, Clause 5.1, requires that any single failure within the safety-related system shall not prevent proper protective action at the system level when required.

The staff reviewed DCD Tier 2 Section 7.1.2.23, which states:

> The I&C systems that are applicable to GDC 21, as shown in Table 7.1-1, are designed in accordance with GDC 21. The protection system is designed to comply with the requirements of IEEE [Std 603-1991]. No credible single failure would result in a loss of the protection function.

As is written, it appears that the applicant is trying to relate the requirements of GDC 21 to IEEE Std 603-1991. However, the applicant does not describe how the two requirements relate to each other (i.e., specify the specific clauses of IEEE Std 603-1991 that map to the requirements of GDC 21) with respect to the APR1400 design. In addition, GDC 21 provides requirements that are not found in IEEE Std 603 (e.g., capability to perform safety function with a single failure and with a component/channel out-of-service). In RAI 43-7887, Question 07.01-14, the staff requested the applicant to modify the FSAR to provide information that describes how GDC 21 relates to IEEE Std 603-1991 and how each requirement is met. In the August 12, 2015 response to this RAI (ML15224B645), the applicant stated that DCD Tier 2 Section 7.1.2.23 is revised to state,

> The applicable I&C systems listed in Table 7.1-1 are designed to meet the requirement of GDC 21. Clause 5.1 of IEEE Std 603 corresponds to the requirement that no single failure results in loss of the protection function as stated in GDC 21. The protection system is designed to conform to Clause 5.1 of IEEE Std 603. Conformance to IEEE Std 603-1991, Clause 5.1 is described in Section A.5.1 of the Safety I&C System TeR. The protection system is designed to meet the requirement that removal from service of any component or channel shall not result in loss of the required minimum redundancy.

The applicant included proposed markups to DCD Tier 2 Section 7.1.2.23 to reflect the proposed modification. Based on the proposed modification to DCD Tier 2 Section 7.1.2.23, the staff finds the applicant has demonstrated how the requirements of GDC 21 and IEEE Std 603-1991, Clause 5.1 are related, and added appropriate references regarding how the requirements of IEEE Std 603-1991, Clause 5.1 are satisfied. Further, the applicant has provided references to where the maintenance and testability requirements of GDC 21 are met. As such, the staff finds the issues identified in RAI 43-7887, Question 07.01-14 are closed and resolved. The verification that the proposed markups are incorporated into the next revision of the FSAR was a confirmatory item. The staff verified that the proposed markups have been incorporated into Revision 1 of DCD Tier 2 Section 7.1.2.22. As such, this confirmatory item has been satisfied.

DCD Tier 2 Table 7.2-7 provides the system level FMEA for the PPS to determine whether the requirements of IEEE Std 603-1991, Clause 5.1 and GDC 21 have been met. For several of the entries in this table, the applicant states that the effect on the PPS will be that the respective safety-related I&C system processor (e.g., CEAC) is declared inoperable. The staff could not find a description of what happens to the output of this processor (e.g., forced to a predefined value of "0" or "1") when it is declared inoperable per technical specification. As such, the staff requested in RAI 274-8277, Question 07.01-39 for the applicant to modify the FSAR to describe what happens to the output of safety-related I&C system processors when the processor is declared inoperable. In the December 29, 2015 response to RAI 274-8277, Question 7.1-39 (ML15363A340), the applicant commits to revise DCD Tier 2 Table 7.2-7 to state, "The output of the [safety] I&C system processors stay in a non-trip state when the processor is declared inoperable." Based on this commitment to define the output state of safety-related I&C system processors, the staff finds the issues identified in RAI 274-8277, Question 07.01-39 is closed and resolved. The verification that the proposed markups are incorporated into the next revision of the FSAR was a confirmatory item. The staff verified that the proposed markups have been incorporated into Revision 1 of DCD Tier 2 Table 7.2-7. As such, this confirmatory item has been satisfied.

DCD Tier 2 Table 7.2-7, No. 2-12, states "Affected CPC uses the last valid penalty factor from the failed CEAC or the current Penalty factor from the operable CEAC, whichever is larger." However, the CPCS TeR, Section 4.2.4 uses the term "last good" DNBR and LPD penalty factors. It was not clear to the staff whether these terms refer to the same penalty factor. It is also not clear to the staff what is meant by "last good" or "last valid" penalty factor. In addition, the CPCS TeR refers to DNBR and LPD penalty factors from the CEAC which is not used in the FSAR or other referenced document. For example, the Safety I&C System TeR states that the CEAC processor module calculates the magnitude of CEA deviation penalty factors and does not refer to the DNBR and LPD penalty factors. Further DCD Tier 2 Table 7.2-7, No. 2-12, states, "If the other CEAC is failed/declared inoperable/or in test, a large pre-assigned penalty factor is assumed in that CPC." However, the CPCS TeR states, "Both CEACs are considered inoperable. Use the pre-determined DNBR and LPD penalty factors." It was not clear to the staff whether the terms "pre-assigned" and "pre-determined" have the same meaning. Definitions were also not provided for these terms. As such, the staff requested in RAI 274-8277, Question 07.01-38 for the applicant to review the design descriptions of the CPCS in the FSAR and its referenced documents to ensure consistency of the terminology used and to provide definitions for the terms used. In the December 29, 2015 response to RAI 274-8277, Question 07.01-38 (ML15363A340), the applicant provided definitions for the terms "last valid" and "pre-assigned" penalty factor. However, the staff was unable to verify this information based on documents reviewed at a CPCS audit as documented in the audit report

(ML16061A027). As such, the staff closed RAI 274-8277, Question 07.01-38, as closed and unresolved and the staff issued follow up question, RAI 328-8422, Question 04.04-8, to address this issue. The staff's review of the response to RAI 328-8422, Question 04.04-8, is documented in Section 4.4 of this SER. The staff concluded in Section 4.4 of this SER that the response to RAI 328-8422, Question 04.04-8, is acceptable.

Section 7.2.4.3 of this SER provides the review single failure criterion requirements for reactor trip functions. Section 7.3.4.3.2 of this SER provides the review single failure criterion requirements for ESFAS functions.

Based upon the information presented in the FSAR and referenced technical reports and the review of the single failure criterion for reactor trip and ESFAS functions documented in Sections 7.2.4.3 and 7.3.4.3.2 of this SER, the staff finds the safety-related I&C system design meets single failure requirements of IEEE Std 603-1991, Clause 5.1 and GDC 21.

7.1.4.6 Completion of Protective Action

The staff reviewed the APR1400 safety-related I&C design to determine if IEEE Std 603-1991, Clause 5.2 has been adequately addressed. IEEE Std 603-1991, Clause 5.2 requires the safety-related system design to provide features to ensure that system-level actions go to completion. Per the guidance in SRP Appendix 7.1-C, "Guidance for Evaluation of Conformance to IEEE Std 603," the staff review of this item included a review of the functional and logic diagrams to ensure that "seal-in" features are provided to enable system-level protective actions to go to completion. IEEE Std 603-1991, Clause 5.2, requires that the safety RPS shall be designed so that once a reactor trip is initiated, automatically or manually, that the intended reactor scram function continue until completion. IEEE Std 603-1991, Clause 7.3, "Completion of Protective Action," states, in part, that when the sense and command features reset, the execute features shall not automatically return to normal and that the execute features shall require separate, deliberate operator action to be returned to normal. Per the guidance in SRP Appendix 7.1-C, "Guidance for Evaluation of Conformance to IEEE Std 603," the staff's evaluation for conformance for the RPS completion of protective action included a review of the functional and logic diagrams to ensure that "seal-in" features are provided to enable system-level protective actions to go to completion.

7.1.4.6.1 Automatic Reactor Trip Completion of Protective Action

To perform an automatic reactor trip, DCD Tier 2 Section 7.2.1, "System Description," states that the two RPS bistable processor per division, generate reactor trip initiation signals if the sensed field monitored process values exceed the respective setpoints. The automatically initiated reactor trip signals are sent from the bistable processors to all four RPS divisions' LCL processors for reactor trip coincidence voting actuation. The LCL processors, upon receiving two or more PPS divisions' bistable processor reactor trip initiation signals, will generate two reactor trip actuation signals. This reactor trip actuation path is shown in Figure 7.2-1, "PPS Basic Block Diagram," of DCD Tier 2. As shown in DCD Tier 2, Figure 7.2-11, "PPS Testing Overlap," and the Safety I&C System TeR, Figure 4-7, "Watchdog Timer for PPS," the reactor trip actuation signal path from the output of the LCLs go through the LCL's digital output module initiation relay to the RPS initiation circuit. However, the staff was not able to identify "Note 2" on the logic diagram of Figure 4-7, "Watchdog Timer for PPS," of the Safety I&C System TeR. The staff issued RAI 272-8313, Question 07.02-13, and RAI 356-7881, Question 07-14, to have the applicant provide more details regarding the watchdog timer (WDT), including the figures in the Safety I&C System TeR. In the December 11, 2015, response to RAI 272-8313,

Question 07.02-13 (ML15345A360), the applicant provided FSAR markups that provides clarity by inserting “Note 2” in Figure 4-7. The response also provided markups to the Safety I&C System TeR to clarify that a manual reset is necessary for the trip circuit breakers to return the latched trip state to the normal state. The staff found that the response is acceptable since it corrected the legend in Figure 4-7 and added additional design description clarity. The incorporation of the proposed markup into the next revision of the Safety I&C System TeR was a confirmatory item. The staff verified that the proposed markups have been incorporated into the Safety I&C System TeR, Revision 1. As such, this confirmatory item has been satisfied. In the September 27, 2016 response to RAI 356-7881, Question 07-14 (ML16271A348), the applicant proposed to modify Figure 4-7 to include corrections to the legend. The response also provided more details on how the output of the WDT is connected to the interposing relay of the undervoltage trip device in the reactor trip initiation circuit. The staff found that the response acceptable since it corrected the legend in Figure 4-7. The evaluation of the other parts of this RAI response is Section 7.1.4.9 of this SER. The incorporation of the proposed markup into the next revision of the Safety I&C System TeR was a confirmatory item. The staff verified that the proposed markups have been incorporated into Revision 1 of the Safety I&C System TeR. As such, this confirmatory item has been satisfied. The RPS initiation circuit contacts are normally closed which keeps the reactor trip switchgear (RTSG) undervoltage interposing relays energized. As shown in DCD Tier 2 Figure 7.2-10, “PPS Channel A Trip Path Diagram,” and Figure 7.2-15, “Reactor Trip Initiation Diagram,” per RPS safety division, there are four LCL reactor trip actuation signals going into two RPS, selective 2oo4, initiation circuits, which provide power to the interposing relays which keep the reactor trip circuit breakers (TCBs) closed. De-energizing the interposing relay will cause the TCB to open. Opening the TCB interrupts power being sent from the motor generator sets to the control rods’ CEDMs. When power is removed from the CEDM coils, the armature springs automatically disengage the latches from the CEDM driveshafts, allowing the control rods (i.e., CEAs) to drop (insert) into the core by gravity. The circuit path for power from the motor generator sets to the CEDMs is shown in DCD Tier 2 Figure 7.7-2, and “Digital Rod Control System - Reactor Protection System Interface Block Diagram.” A minimum of two divisions of RPS reactor trip signals are required for a reactor trip. Once the TCBs have opened and the control rods have fully inserted into the core by gravity, the reactor trip safety function is complete. The RPS reactor trip function is not designed to automatically return the control rods to the normal position once the TCBs are opened.

The Safety I&C System TeR, Revision 0, Section A.7.3, “Completion of Protective Action,” states that operator action is required to reset both the plant conditions which caused the reactor trip and the reactor TCBs before returning to the normal operation condition. This ensures that once the TCB are opened, the control rods will insert into the core and will not return to the normal state without deliberate operator action. The staff finds that this design function (i.e., TCBs will not automatically return to the normal position without deliberate operator action) meets the requirements of IEEE Std 603-1991, Clauses 5.2 and 7.3, “Completion of Protective Action.”

7.1.4.6.2 Manual Reactor Trip Completion of Protective Action

For a manually actuated reactor trip, manual reactor trip switches are provided on the MCR safety console. This is shown on DCD Tier 2 Figure 7.3-2, “Block Diagram of the ESF-CCS.” The manually initiated reactor trip actuation signal path starts at the manual reactor trip switch and is connected directly to the undervoltage trip device of the reactor TCB. The manual trip initiation circuitry completely bypasses the RPS automatic trip logic actuation circuitry. This manual actuation logic is shown in DCD Tier 2 Figure 7.2-16, “Manual Reactor Trip Initiation

Diagram." The manual reactor trip switch circuit is directly wired to the reactor trip switchgear. This manual initiation reactor trip direct connection is shown in DCD Tier 2 Figure 7.2-10, "PPS Channel A Trip Path Diagram." Manually actuating any pair of manual reactor trip switches results in opening the reactor TCBs and interrupting motor generator power to the control rods CEDMs causing the control rods to drop into the core by gravity. Once a pair of manual reactor trip switches are actuated and the TCB are opened, the reactor trip initiation signal is latched and must be reset before returning the reactor TCBs to the normal position to apply power to begin withdrawing the control rods. Therefore, once the TCBs have opened and the control rods have fully inserted into the core, the reactor trip safety function is complete, and by design, the control rods cannot be returned to a withdrawn state until deliberate operator action is taken to reset the plant trip conditions that caused the reactor trip.

The staff has reviewed the logic diagrams using the guidance of SRP Appendix 7.1-C, "Guidance for Evaluation of Conformance to IEEE Std 603," to make a finding of conformance for the RPS reactor trip safety function. Based on staff's above evaluation of the RPS reactor trip protective action operation, the staff finds that the RPS reactor trip design meets the requirements of IEEE Std 603-1991, Clause 5.2 and Clause 7.3, "Completion of Protective Action."

Section 7.3.4.3.5 of this SER provides the review of completion of protection action requirements for ESFAS functions.

7.1.4.7 Quality

The staff reviewed the APR1400 design to determine if the quality standards requirements of GDC 1 were adequately addressed. This discussion is located in Section 7.1.4.3 of this SER. Additionally, the staff reviewed the application to determine if IEEE Std 603-1991, Clause 5.3 has been adequately addressed. IEEE Std 603-1991, Clause 5.3, requires components and modules be of a quality that is consistent with minimum maintenance requirements and low failure rates, and safety-related system equipment be designed, manufactured, inspected, installed, tested, operated, and maintained in accordance with a prescribed quality assurance program. GDC 1 requires, in part, a quality assurance program be established and implemented in order to provide adequate assurance that these SSCs will satisfactorily perform their safety functions. The staff used the guidance in SRP Appendix 7.1-C. The review guidance provided in SRP Appendix 7.1-C, Section 5.3, "Quality," indicates that the application should confirm that the quality assurance provision of 10 CFR Part 50, Appendix B is applicable to the safety-related system. SRP Appendix 7.1-C, Section 5.3 states that the evaluation of the adequacy of the overall quality assurance program is addressed in the review of DCD Tier 2 Chapter 17. Therefore the evaluation of the overall quality assurance program can be found in Section 17 of this evaluation. For digital computer-based systems, SRP Section 7.1-C points to guidance provided by IEEE Std 7-4.3.2-2003. The following topics are areas of focus for the review of digital computer systems quality design:

- Software development.
- Software tools.
- Verification and validation (V&V) as well as independent V&V (or IV&V).
- Software configuration management.

- Software project risk management.

The SPM TeR describes the overall software lifecycle development process. The SPM provides specific design details on each of the bulleted items above.

7.1.4.7.1 Software Quality

To determine the acceptability of the applicant's software quality, the staff used the guidance in SRP Appendix 7.1-C and in SRP Appendix 7.1-D, "Guidance for Evaluation of the Application of IEEE Std 7-4.3.2." The guidance in SRP Appendix 7.1-C states that for digital computer-based systems, the staff is to confirm that the application addresses the quality requirements described in IEEE Std 7-4.3.2-2003, Clause 5.3. The guidance in SRP Appendix 7.1-D, Section 5.3, indicates that the application should address the quality criteria described in IEEE Std 7-4.3.2-2003, Clause 5.3, and that software quality is addressed in IEEE/Electronic Industries Alliance (EIA) Std 12207.0-1996, "Standard for Information Technology – Software [Lifecycle] Processes." IEEE Std 7-4.3.2-2003, Clause 5.3 indicates that the review of software quality also includes a review of software development, V&V, as well as independent V&V, software configuration management, and software project risk management. Also, SRP BTP 7-14, "Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems," refers to IEEE Std 7-4.3.2-2003, Clause 5.3. SRP BTP 7-14 describes the specific features of software development that should be reviewed by the staff.

The SPM TeR describes the software quality assurance requirements for the development of the APR1400 digital I&C system that uses advanced design features such as digital data communication, a network-based distributed digital control system, and a compact workstation-based HSI in the control room. The I&C architecture of the APR1400 is implemented by two major independent and diverse platforms:

(1) Safety-related PLC platform for the safety-related systems, and

(2) Non-safety DCS platform for the data processing system and non-safety control systems.

In addition, independent non-safety systems such as the T/G control and protection system, the NSSS monitoring system, and the BOP monitoring system perform the required functions of a portion of the I&C systems.

The safety-related I&C system is designed for implementation on the Westinghouse Common Q platform, which is the safety PLC platform. This platform is configured using various hardware building blocks and loaded with application software to develop safety-related I&C systems. The following I&C subsystems makeup the PLC platform:

- QIAS-N displays PPS:
    - Bistable Processor
    - Local coincidence logic Processor
- CPCS:
    - CPC

    - CEA calculator
    - CEA position processor
- ESF-CCS:
    - Group controller
    - Loop controller
    - ESCM
    - DMA (hardwired)
    - CIM
- Data communication system
    - SDL
    - SDN
    - CCG
    - CPM
- Safety system ITP
- Safety system MTP
- Safety system operator module
- QIAS-P
    - QIAS-P processor
    - QIAS-P displays
- QIAS-N
    - QIAS-N processor

The PLC platform software resides in the processor module and consists of a real-time operating system, task scheduler, diagnostic functions, communication interfaces, and an application program. The application program is created using a software development tool that includes a function block library and developed according to the structured software lifecycle process as described in the SPM TeR. Application software for subsystems designated for the safety PLC platform are categorized in one of the following categories:

- Safety-critical (Protection): Software whose function is necessary to directly perform reactor protection system initiation actions, ESFAS control actions, and safe shutdown control actions.

- Important-to-safety (ITS): Software whose function is necessary to directly perform DPS control actions, software that is relied on to monitor or test safety critical functions, or software that monitors plant critical safety functions.

Both categories of software for safety-related I&C systems are implemented on Class 1E hardware. Note, the SPM TeR uses the term “class.” However, the use of this term is intended to mean “category” because it is not the intention of this technical report to address classification of systems. As such, the staff is using the term “category” in this SER.

In Appendix A of the SPM TeR, the applicant provides justification for use of ITS category software in the safety-related I&C systems, which states, in part:

- [ ].
- [ ].
- [ ].
- [ ].

[ ]:

- [ ]
- [ ]
- [ ]
- [ ]
- [ ]
- [ ]
- [ ]
- [ ]
- [ ]

The SPM TeR also applies to the software for FPGA based non-1E DPS and DIS [ ]. Appendix D of the SPM TeR outlines the FPGA development process.

Software for the non-safety computer-based procedure system, and safety parameter display and evaluation system (SPADES+) [ ] and is developed in accordance with this SPM TeR. [

].

Required tasks and responsibilities for each category of the software are described in Table 4-3 of the SPM TeR, e.g., [

].

The SPM TeR describes the software lifecycle and engineering process for digital I&C systems, which is conducted in seven phases, namely; concept, requirement, design, implementation, test, installation and checkout, and operation & maintenance phases. These seven phases are covered by the 12 software plans described within the SPM TeR. Figure 2-1 of the SPM TeR shows the relationship between the seven lifecycle phases and the 12 software plans.

The project-specific application software lifecycle is controlled by the following 12 software plans:

Software Plans	**SPM TeR Sections**
Software Management Plan (SMP)	3.0
Software Quality Assurance Plan (SQAP)	4.0
Software Verification and Validation Plan (SVVP)	5.0
Software Configuration Management Plan (SCMP)	6.0
Software Development Plan (SDP)	7.0
Software Integration Plan (SIntP)	8.0
Software Installation Plan (SInstP)	9.0
Software Training Plan (STrngP)	10.0
Software Operation and Maintenance Plan (SOMP)	11.0
Software Safety Plan (SSP)	12.0
Software Test Plan (STP)	13.0
Secure Development and Operational Environment (SDOE)	14.0

DCD Tier 1 Table 2.5.1-5, ITAAC 11, is associated with development of the PPS software. DCD Tier 1 Table 2.5.2-4, Item 6 is associated with development of the DPS software. DCD Tier 1 Table 2.5.3-3, Item 5 is associated with development of the QIAS-P software. DCD Tier 1

Table 2.5.4-4, Item 15, is associated with development of the ESF-CCS software. The evaluation of these ITAAC are in Section 14.3.5 of this SER.

SRP BTP 7-14 provides guidance on software reviews for digital computer-based I&C systems. The applicable sections of the FSAR and related technical reports are reviewed for conformance to SRP BTP 7-14, specifically the acceptance criteria described in SRP BTP 7-14, Section B.3.

The SPM TeR defines the software engineering process based on SRP BTP 7-14 to be followed in creating and revising software of the I&C systems. Section 2.1 of the SPM TeR describes the software categories based on the functionality and importance related to safety. Software tasks and responsibilities assigned to each class of software are described in Table 4-3. Appendix A of the SPM TeR outlines assignments of I&C systems' software to specific class, and provides justification for use of ITS class software in the safety-related I&C systems. Staff's review of these SPM TeR sections resulted in the following questions for the applicant per RAI 261-8253, Question 07.01-26:

1. Appendix A, Section A.2, of the SPM TeR includes information to justify the use of ITS class software and states that a software hazard analysis is provided. The applicant was asked to provide this analysis.
2. The SPM TeR, Table A-1, "Assignment of Software for the I&C Systems to Classes," outlines assignments of I&C systems' software to specific class. However, software class for subsystems CPM, CCG, and CIM is not specified. The applicant was asked to provide software classification for CPM, CCG, and CIM subsystems.
3. Table 4-2, Footnote 2, and the section in Table 4-3 applicable to Table 4-2, Footnote 2, have opposing statements. The applicant was asked to resolve this discrepancy.

In the December 17, 2015 response (ML15351A198) to RAI 261-8253, Question 07.01-26, the applicant stated the following.

1. The hazards analysis for ITS software to be used with safety critical software in the safety-related I&C system is included in the hazard analysis for the safety critical software, and accordingly proposed changes to Appendix A, Section A.2 of the SPM TeR;

2. [ ] since CIM does not contain any software, and accordingly proposed changes to the SPM TeR, Table A-1;

3. Consistent with Table 4-2, Footnote 2, [ ], and accordingly proposed changes to the SPM TeR, Table 4-3.

The staff finds the RAI response and proposed changes to the SPM TeR in RAI 261-8253, Question 07.01-26, acceptable, since (1) hazards analysis for ITS software is provided within the safety critical software hazards analysis; (2) [ ], and since CIM does not contain any software, therefore [ ]; and (3) since [ ], therefore correctly identifying this fact in SPR TeR Table 4-3 is acceptable. The incorporation of the proposed markup into the next revision of the SPM TeR was a confirmatory item. The staff verified that the proposed markups have been

incorporated into Revision 1 of the SPM TeR, Appendix A, Section A.2, Table A-1, and Table 4-3. As such, this confirmatory item has been satisfied.

Development of the APR1400 I&C system software is conducted using a formally defined lifecycle process, which consist of seven phases and controlled through 12 software plans. These 12 plans are described in Sections 3 through 14 of the SPM TeR. The staff's evaluation of these software program plans is discussed as follows.

7.1.4.7.1.1 Software Management Plan (SMP)

The purpose of the SMP is to describe the management aspects of the software development project. SRP BTP 7-14, B.3.1.1, states that Section 3, "Project Management Process," of IEEE Std 1074-1995, "Standard for Developing a Software Lifecycle Process," which is endorsed by RG 1.173, Revision 0, "Developing Software Lifecycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," describes an acceptable approach to software project management. Note, the applicant commits to Revision 1 of RG 1.173, which endorses IEEE Std 1074-2006. Section 3 states that project management processes are the processes that initiate, monitor, and control software projects throughout the software lifecycle. The staff looks for evidence that software development will be managed in such a way that high quality software will result. Supporting characteristics include independence between the design organizations and the organizations that check the quality of the software development, defined roles and responsibilities, and proper oversight of vendors to meet 10 CFR Part 50, Appendix B.

Section 3.1 of the SPM TeR describes the requirements for SMP, and states that the SMP requirements comply with SRP BTP 7-14 and IEEE Std 1058-1998, "IEEE Standard for Software Project Management Plans." Section 3.1 of the SPM TeR describes the purpose or key functions of the software to be developed, and states that the implementing procedures shall be prepared in accordance with the requirements specified in this SPM TeR and in accordance with the APR1400 Quality Assurance Manual (QAM). Figure B-1 of the SPM TeR shows the software project organization for the safety-related I&C systems, and roles and responsibilities of the team members of this organization are outlined in Appendix B of the SPM TeR. [

].

The staff reviewed the criteria for SMP to verify compliance with applicable regulatory requirements. Based on the staff's evaluations detailed in the discussion above, the staff finds that, the criteria for SMP are acceptable and meets the relevant guidance of SRP BTP 7-14 and requirements in GDC 1 and 10 CFR 50.55a(h)(3).

7.1.4.7.1.2 Software Quality Assurance Plan (SQAP)

SRP BTP 7-14, Section B.3.1.3, provides guidance in evaluating an SQAP. The SQAP shall comply with the requirements of 10 CFR Part 50, Appendix B, and the applicant's overall quality assurance program. 10 CFR Part 50, Appendix B, states that the applicant shall be responsible

for the establishment and execution of the QAP. The applicant may delegate the work of establishing and executing the QAP, or any part thereof, but shall retain responsibility for the QAP.

The SQAP identifies which quality assurance procedures are applicable to specific software processes, identifies particular methods chosen to implement quality assurance procedural requirements, and augments and supplements the quality assurance program as needed for software. Clause 5.3.1 of IEEE Std 7-4.3.2-2003, as endorsed by RG 1.152, Revision 3, provides guidance on SQA. IEEE Std 7-4.3.2-2003, Clause 5.3.1 states, in part, that guidance for developing software quality assurance plans can be found in IEEE Std 730-1998.

SPM TeR Section 4.0 describes the requirements for SQAP and states that the SQAP shall be prepared in accordance with SRP BTP 7-14 and meets IEEE Std 730, "IEEE Standard for Software Quality Assurance Plan." The SQAP describes the process by which the applicant manages software and documentation throughout the software development lifecycle. Management of the SQAP is overseen by the managers of design team and V&V team. Organizationally, verification of the implementation of quality assurance requirements is performed by the quality assurance team in accordance with the APR1400 QAM. The quality assurance team is responsible for assuring that the planned software development and V&V activities are appropriately conducted. The quality assurance team conducts independent audits on the design team and V&V team activities to confirm that requirements and implementation of the software lifecycle process are appropriately planned and executed in accordance with the QAM.

The design certification application (specifically, the Safety I&C System TeR, Revision 0, Section 8, "Safety I&C System Platform") identifies Common Q as the digital platform that will be used to implement safety-related I&C systems. NRC has approved WCAP-16096-NP-A, Revision 4, "Software Program Manual for Common Q Systems," dated February 2013. However, the SPM TeR does not provide any relationship to the Common Q Software Program Manual. In RAI 261-8253, Question 07.01-28, the staff asked the applicant to describe the relationship between the SPM TeR and the Common Q SPM (WCAP-16096). In the December 17, 2015, response (ML15351A198) to the RAI, the applicant stated that the SPM and the Common Q SPM are separately developed documents and they do not refer to one another. The Common Q software has been developed in accordance with the Common Q SPM and is considered existing software to be used in the APR1400 safety-related I&C systems, and it is treated in the manner described in Section 4.1.2 of the SPM TeR. As a supplemental question to this RAI, the applicant was requested to revise the SPM TeR with the description of how Common Q platform is treated in developing the APR1400 I&C systems in accordance with the SPM TeR. In the October 7, 2016, supplemental response (ML16281A212) to the RAI, the applicant stated that in accordance with Section 2.1 of the SPM TeR, this topical report does not assign any software classification or categorization to the original or existing software. Therefore, no revisions are needed are needed to the SPM TeR. The staff verified that the contents of Section 2.1 of the SPM TeR and concurs that it adequately addresses treatment of the existing software and finds the supplemental response to RAI 261-8253, Question 07.01-28, acceptable and this RAI, is closed and resolved.

Section 4.1.2 of the SPM TeR describes the criteria for using pre-existing software in the APR1400 I&C systems. However, the criteria do not describe the analysis of software features/functionality, the environment/interface the pre-existing software used, and necessary modifications to allow its use in the APR1400 I&C systems. While the use of pre-existing software can provide benefits, without a thorough analysis of its functionality, interface points,

and how it will fit in the new application environment, software faults can be introduced. In RAI 261-8253, Question 07.01-29, the applicant was requested to identify and describe the analysis that will need to be performed on pre-existing software to demonstrate that it can be safely re-used in the APR1400 design. In the December 17, 2015, response (ML15351A198) to the RAI, the applicant stated that the documentation for the existing software is reviewed to analyze features/functionality and the application environment/interface of the software in accordance with the criteria described in Section 5.3.3.2, "Requirements Phase V&V Tasks," of the SPM TeR, and proposed revising SPM TeR Section 4.1.2, which would state that the pre-existing software shall be analyzed with the criteria for previously developed for sub-vendor software described in Section 5.3.3.2 of the SPM TeR. Because the applicant added description of how existing software will be reviewed, the staff finds the RAI response and proposed changes to the SPM TeR in RAI 261-8253, Question 07.01-29, acceptable. The incorporation of the proposed markup into the next revision of the SPM TeR was a confirmatory item. The staff verified that the proposed markups have been incorporated into Revision 1 of the SPM TeR, Section 4.1.2. As such, this confirmatory item has been satisfied.

Section 4 of the SPM TeR describes the requirements for SQAP. However, it does not appear to describe the relationship between the SQAP and the APR1400 QAM. In RAI 261-8253, Question 07.01-30, the applicant was asked to provide a description of the relationship and interfaces between these to documents. In the September 21, 2016, response (ML16265A637) to the RAI, the applicant stated that the APR1400 QAM applies to all documents for the APR1400, including the SPM TeR, and the SPM TeR applies to all software documents to be developed for the APR1400 I&C systems, including the SQAP for a specific I&C system for APR1400. References made to QAM in the SPM TeR are the references to the APR1400 QAM and to clarify this, the "Acronyms and Abbreviations" list was revised accordingly. The staff finds the RAI response and proposed changes to the SPM TeR in RAI 261-8253, Question 07.01-30, acceptable. The incorporation of the proposed markup into the next revision of the SPM TeR was a confirmatory item. The staff verified that the proposed markups have been incorporated into Revision 1 of the SPM TeR, Acronyms and Abbreviations Section. As such, this confirmatory item has been satisfied.

The staff reviewed the requirements for SQAP to verify its compliance with applicable regulatory requirements. Based on the staff's evaluations detailed in the discussion above, the staff finds that the process outlined in the SPM TeR for developing the SQAP is acceptable and meets the relevant guidance of SRP BTP 7-14 and requirements in 10 CFR Part 50, Appendix B.

7.1.4.7.1.3 Software Verification and Validation Plan (SVVP)

SRP BTP 7-14, Section B.3.1.10 provides guidance for evaluating an SVVP. SRP BTP 7-14, Section B.3.1.10.1 states that management characteristics of the SVVP should exhibit purpose, organization, oversight, responsibilities, and risks. RG 1.168, "Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," Revision 2, endorses IEEE Std 1012-2004, "Standard for Software Verification and Validation," as providing methods acceptable for meeting the applicable cited regulation.

The SPM TeR, Section 5.0 describes the requirements for SVVP and states that the development of the SVVP shall comply with RG 1.168, Revision 2. The SPM TeR Section 5.2.1 states that the V&V team for safety critical and ITS class software is organized independently of the design team, and the V&V team members shall not be directly involved in the software design of the project. Appendix B of the SPM TeR states that the V&V team shall be technically independent, managerially independent, and financially independent as defined in Annex C of

IEEE Std 1012-2004, and the V&V team is responsible for all IV&V activities and tasks described in the Section 5.2.5 of the SPM TeR. The V&V team is responsible for configuration management activities on the V&V output documents. With respect to the APR1400 software lifecycle phases, V&V activities start with the Concept Phase and run through the Operation and Maintenance Phase. The scope of the SVVP is described in the SPM TeR, Section 5.0 and illustrated in the SPM TeR, Table 5-1. In accordance with RG 1.168, Revision 2, Regulatory Position C.1, the SVVP covers all equipment with Software Integrity Level 4. The quality assurance organization will perform periodic assessment of the V&V process in accordance with APR1400 QAM.

The staff reviewed the criteria for SVVP to verify compliance with applicable regulatory requirements. Based on the applicant's description of how the development of the SVVP will conform to RG 1.168, Revision 2, and SRP BTP 7-14, the staff finds that the criteria for SVVP are acceptable and meet the relevant guidance of SRP BTP 7-14 and requirements in GDC 1 and 10 CFR 50.55a(h)(3).

7.1.4.7.1.4 Software Configuration Management Plan (SCMP)

SRP BTP 7-14 Section B.3.1.11 provides guidance for evaluation of an SCMP. Section A.1.2.2 of IEEE Std 1074-2006, as endorsed by RG 1.173, Revision 1 provides an acceptable approach to software configuration management. Section 7.2.1 states that software configuration management identifies the items in a software development project and provides both for control of the identified items and for reporting the status of such items to management to maintain visibility and accountability throughout the software lifecycle. Examples of items to be controlled include, but are not limited to, code, documentation, plans, and specifications. SRP BTP 7-14, Section B.3.1.11.1, asks for the definition of the responsibilities and authority of the software configuration management organization.

The SPM TeR Section 6.0 describes the requirements for SCMP and states that the SCMP shall be prepared in accordance with RG 1.169, Revision 1. The SPM TeR Section 6.2 describes the organizations and their software configuration management responsibilities. The design team leader is responsible for the implementation of adequate measures to manage and control the software configuration in accordance with the SCMP. The librarian maintains all controlled software items as well as all control records. The SPM TeR Section 6.3 describes seven functions of software configuration management activities: configuration identification, configuration control, status accounting, configuration audits and reviews, interface control, subcontractor/vendor control, and release management and delivery. APR1400 application software baseline is established at the implementation phase and changes are documented and approved as described in this SCMP.

The staff reviewed the criteria for SCMP to verify its compliance with applicable regulatory requirements. Based on the applicant's description of how the development of the SCMP will conform to RG 1.169, Revision 1, and SRP BTP 7-14, the staff finds that the criteria for SCMP are acceptable as they meet the relevant guidance of SRP BTP 7-14 and requirements in GDC 1 and 10 CFR 50.55a(h)(3).

7.1.4.7.1.5 Software Development Plan (SDP)

The purpose of an SDP is to describe the plan for technical project development. SRP BTP 7-14 Section B.3.1.2 describes acceptance criteria for the SDP. RG 1.173, Revision 1 endorses IEEE Std 1074-2006 as providing an acceptable approach to software development

lifecycle processes. SRP BTP 7-14 states that the SDP should clearly state tasks of each lifecycle and state the lifecycle inputs and outputs. The SDP should also include a review and V&V at the end of each lifecycle activity.

The SPM TeR Section 7.0 describes the requirements for SDP, and states that the SDP shall comply with RG 1.173, Revision 1 which endorses IEEE Std 1074-2006. To comply with Section 4.2 of IEEE Std 1074-2006, which requires that a software lifecycle model be selected to support the management of the project, the applicant selected a software lifecycle model consistent with RG 1.152, Revision 3 and RG 1.173, Revision 1, as stated in Section 7.2 of the SPM TeR. Section 4.8 of the SPM TeR states the use of the "waterfall" model (or a sequential (non-iterative) design process) of software development and testing techniques shall be employed. However, this is the only statement in the software program manual regarding the waterfall model. Based on recent experiences developing new nuclear power plant software, vendors use a cyclic model that incorporates several baselines of software that go through the various lifecycle phases multiple times versus a once-through development process such as the waterfall model. As such, in RAI 261-8253, Question 07.01-31, the staff requested the applicant to clarify whether the APR1400 use a true waterfall model for software development or will it use a form of cyclic software development. The staff requested the applicant to describe the type of software development lifecycle model that will be employed for the APR1400 safety software development. In the September 21, 2016, response (ML16265A637) to this RAI, the applicant proposed revision to Section 4.8 of the SPM TeR that instead of committing to the use of waterfall model will now state, "The software development organization may use its own lifecycle model provided that within its work scope, the required activities and tasks described in this report are performed and the required outputs specified in this report and provided." The staff finds the RAI response and proposed changes to the SPM TeR in RAI 261-8253, Question 07.01-31, acceptable, since Section B.3.1.2.4 of SRP BTP 7-14 does not prescribe a specific model for developing the software and states that the SDP should clearly state which tasks are a part of each lifecycle and define the lifecycle inputs and outputs and how they are reviewed verified and validated. The incorporation of the proposed markup into the next revision of the SPM TeR was a confirmatory item. The staff verified that the proposed markups have been incorporated into Revision 1 of the SPM TeR, Section 4.8. As such, this confirmatory item has been satisfied.

The SPM TeR, Section 2.2 states that the software lifecycle phases includes the following phases.

- Concept
- Requirements
- Design
- Implementation
- Test
- Installation and Checkout
- Operation and Maintenance (including retirement)

Section 7.2 of the SPM TeR states that the SDP shall describe the software lifecycle processes that will be used on the project, and shall discuss the various processes that make up this lifecycle. For each process, the SDP shall give the input information required in order to carry out the process, a description of the actions that must take place during the process, and the output information produced by the process. Generically, outputs from these software lifecycle processes are to be made available for the staff's evaluation, which the applicant has identified in Table 4-2 of the SPM TeR. Figure 2-1 of the SPM TeR shows the relationship between each phase of the software lifecycle and the software lifecycle plans for the safety critical class software. Whereas, Table 4-2 of the SPM TeR identifies tasks required for each software class.

SRP BTP 7-14, Section B.3.1.2.4 provides guidance for software tools, and references IEEE Std 7-4.3.2-2003, Clause 5.3.2, which states, in part, that software tools used to support software development processes and V&V processes shall be controlled under configuration management. The section further states either a test tool validation program shall be developed to provide confidence that the necessary features of the software tool function as intended or the software tool shall be used in a manner such that defects not detected by the software tool will be detected by V&V activities.

The SPM TeR Section 7.3 states that the SDP shall describe the methods and techniques that will be used to develop the software, and the tools that will used in connection with those methods and techniques. The staff does not dictate which software tools are used; however, the use of software tools should adhere to IEEE Std 7-4.3.2-2003, Clause 5.3.2. Examples include, but are not limited to, adequate training for software developers to use the tools, testing to verify the outputs of the tools, and configuration management of the version of the tools being used. The outputs of software tools should undergo the V&V process as defined in the SVVP of the SPM TeR. In this SER, the staff has not reviewed or approved any of the software tools.

The staff reviewed the criteria for SDP to verify its compliance with applicable regulatory requirements. Based on the applicant's description of how the development of the SDP will conform to RG 1.152, Revision 3, RG 1.173, Revision 1, and SRP BTP 7-14, the staff finds that, the criteria for SDP are acceptable as they conform to the relevant guidance of SRP BTP 7-14 and meets the requirements in GDC 1 and 10 CFR 50.55a(h)(3).

7.1.4.7.1.6 Software Integration Plan (SIntP)

SRP BTP 7-14 Section B.3.1.4, provides guidance in evaluating a SIntP and asks for a description of the software integration process and the software integration organization. Clause A.1.2.8 of IEEE Std 1074-2006, as endorsed by RG 1.173, Revision 1 provides an acceptable approach to an integration plan. Clause A.1.2.8 states that during the plan integration activity, the software requirements and the software design description (SDD) are analyzed to determine the order of combining software components into an overall system. In addition, Clause A.1.2.8 of IEEE Std 1074-2006 states that the integration planned information shall be coordinated with the Evaluation Planned Information described in Section A.1.2.1 of IEEE Std 1074-2006.

Section 8.0 of the SPM TeR describes the requirements for SIntP and states that the SIntP shall be prepared in accordance with SRP BTP 7-14. In the APR1400 design, software integration consists of three major phases; integrating the various software components from single programs, integrating the software with hardware, and testing the resulting integrated product. The SPM states that the SIntP shall include the system build document that describes precisely how the system hardware and software components are combined into the specific operational

system. The V&V organization, as described in the SVVP, will verify that the integrated system satisfies all requirements through executing the integration V&V test procedures. Software integration is performed in accordance with the APR1400 QAM. The staff reviewed the requirements for SIntP, and found that the applicant has adequately addressed the SIntP acceptance criteria in SRP BTP 7-14.

7.1.4.7.1.7 Software Installation Plan (SInstP)

Section B.3.1.5 of SRP BTP 7-14 and Section A.1.2.4 of IEEE Std 1074-2006, as endorsed by RG 1.173, Revision 1 provide an acceptable approach for software installation plans. Section A.4.1 of IEEE Std 1074-2006 states that an installation consists of the transportation and installation of the software system from the development environment (test bed) to the target environment (operational). It includes the necessary software modifications, checkout in the target environment, and customer acceptance. If a problem arises, it must be identified and reported by the customer. SRP BTP 7-14, Section B.3.1.5.4, states that there should be approved procedures for software installation, for combined hardware and software installation, and systems installation. In addition, since the safety-related system is complex, there should be a controlled process to identify, correct, and document errors in the installation procedures.

Section 9.0 of the SPM TeR provides requirements for the SInstP. The SPM TeR states that the Design Team is responsible for performing the installation activities and shall document the results. The Design Team will identify and analyze the plant installation environment, and provide plant installation procedures. The SPM TeR Section 9.4 lists the minimum installation activities that shall be described in the specific SInstP. The V&V Team is responsible for the Implementation and Installation Phase V&V activities and documents the results. The quality assurance department performs quality assurance audits to ensure that the Design Team and the V&V Team perform the installation activities as described in the SPM TeR. Data will be collected and analyzed to determine the success or failure of the installation activities.

The SPM TeR, Table 4-3, indicates that the SInstP, STrngP, and SOMP will be the responsibility of the utility. The staff could not identify a combined license (COL) item in DCD Tier 2 Table 1.8-2, specifying these plans are the responsibility of the COL applicant. In RAI 261-8253, Question 07.01-27, the staff requested the applicant to provide a COL item to address this issue. In the December 17, 2015 response (ML15351A198), to RAI 261-8253, Question 07.01-27, the applicant proposed changes to Table 1.8-2 and Section 7.1.4 of the DCD Tier 2 that adds a COL information item, “COL 7.1(1) The COL applicant is to provide the software installation plan, the STrngP, and the software operation and maintenance plan for the safety-related I&C systems, as described in the SPM Technical Report.” The staff finds the RAI response and proposed changes to the APR1400 DCD Tier 2 in RAI 261-8253, Question 07.01-27, acceptable based on the addition of a COL item described above. The incorporation of the proposed markup into the next revision of the DCD Tier 2 was a confirmatory item. The staff verified that the proposed markups have been incorporated into Revision 1 of DCD Tier 2 Section 7.1.4, and Table 1.8-2. As such, this confirmatory item has been satisfied.

The staff reviewed the criteria for the SInstP to verify its compliance with applicable regulatory requirements. Based on the staff’s evaluations detailed in the discussion above, the staff finds that the criteria for SInstP are acceptable and meet the relevant guidance of SRP BTP 7-14 and requirements in GDC 1 and 10 CFR 50.55a(h)(3).

7.1.4.7.1.8 Software Training Plan (STrngP)

Section B.3.1.7 of SRP BTP 7-14 and Section A.1.2.6 of IEEE Std 1074-2006, as endorsed by RG 1.173, Revision 1, provide an acceptable approach to STrngPs. Section A.1.2.6.2 lists typical activities for this software lifecycle activity: plan the training program, develop training materials, validate the training program, and implement the training program. If the licensee will be performing the digital system maintenance, the training plan(s) will be more involved since additional technical knowledge is required.

Section 10.0 of the SPM TeR provides criteria for the STrngP. The SPM TeR Section 10 outlines the training activities for the application software that shall be described in the STrngP. Roles and responsibilities are also discussed. The staff reviewed the criteria for the STrngP to verify its compliance with applicable regulatory requirements. Based on the staff's evaluations detailed in the discussion above, the staff finds that the criteria for the STrngP are acceptable and meet the relevant guidance of SRP BTP 7-14 and requirements in GDC 1 and 10 CFR 50.55a(h)(3).

7.1.4.7.1.9 Software Operations and Maintenance Plan (SOMP)

Section B.3.1.8 of SRP BTP 7-14 and Section A.4.2 of IEEE Std 1074-2006, as endorsed by RG 1.173, Revision 1, provide an acceptable approach for SOMP. Section A.4.2 states that the operation and support process involves user operation of the system and ongoing support. Support includes providing technical assistance, consulting with the user, and recording user support requests by maintaining a support request log; thus the operation and support process may trigger maintenance activities, which the software maintenance plan should address. Section 6.2.3.2 states that the installed software system will be utilized in the intended environment and in accordance with the operating instructions.

Section B.3.1.6 of SRP BTP 7-14 and Section A.4.3 of IEEE Std 1074-2006, as endorsed by RG 1.173, Revision 1 provide an acceptable approach for software maintenance plans. Section A.4.3 states a maintenance process is concerned with the resolution of software errors, faults, and failures; that the need for software maintenance initiates software lifecycle changes.

Section 11 of the SPM TeR provides requirements for the SOMP that shall be prepared in accordance with SRP BTP 7-14. The SPM TeR Sections 11.2 and 11.3 describe the roles and responsibilities to define the process of operating and maintaining the application software during the Operation and Maintenance Phase. The Design Team will develop and provide to the customer an Operations and Maintenance Manual that will cover the operations and maintenance activities listed in the SPM TeR Section 11.2 and 11.3.

The staff reviewed the SOMP to verify its compliance with applicable regulatory requirements. Based on the staff's evaluations detailed in the discussion above, the staff finds that the criteria for SOMP are acceptable and meet the relevant guidance of SRP BTP 7-14 and requirements in GDC 1 and 10 CFR 50.55a(h)(3).

7.1.4.7.1.10 Software Safety Plan (SSP)

SRP BTP 7-14 Section B.3.19 provides guidance for evaluating the SSP. The SSP should provide appropriate safety measures in the software requirements specification. The SSP should define the safety activities to be carried out for each set of lifecycle activities, from requirements through operation and maintenance. The SSP should describe the boundaries and interfaces between the software safety organization and others. It should show how the

software safety activities are coordinated with the development activities and the interactions between software safety organization and the software V&V organization. The SSP should designate a single safety officer that has clear responsibility for the safety qualities and has clear authority to accomplish the goals of the safety requirements in the SRS design, and implementation of the software. RG 1.173, Revision 1, Section C.3, "Software Safety Analyses," contains guidance on safety analysis activities. NUREG/CR-6101, "Software Reliability, and Safety in Nuclear Reactor Protection Systems," which was based on a draft of IEEE Std 1228-1994, "Software Safety Management," also contains guidance on SSPs.

Section 12.0 of the SPM TeR describes the requirements for SSP and states that the SSP shall be prepared in accordance with guidance in SRP BTP 7-14, and IEEE Std 1228-1994. In accordance with Clause 4.3.1 of IEEE Std 1228-1994, the SPM TeR, Section 12.3 describes the roles and responsibilities in supporting the SSP and discusses the coordination between the development and test organizations. The Design Team is responsible for the Software Safety Management and Software Safety Analysis activities as described in IEEE Std 1228-1994. The V&V Team ensures that the Design Team implements requirements of the SSP.

Section 12.4 of the SPM TeR discusses software safety analysis, which is performed for each lifecycle phase: requirements phase, design and implementation phase, test phase, and post development phase. These analyses shall be performed according to IEEE Std 1228-1994.

The staff reviewed the requirements for SSP to verify compliance with applicable regulatory requirements. Based on the staff's evaluations detailed in the discussion above, the staff finds that the requirements for SSP are acceptable and meets the relevant guidance of SRP BTP 7-14 and requirements in GDC 1 and 10 CFR 50.55a(h)(3).

7.1.4.7.1.11 Software Test Plan (STP)

SRP BTP 7-14 Section B.3.1.12 provides guidance for evaluation of an STP. IEEE Std 829-2008, "Standard for Software and System Test Documentation," as endorsed by RG 1.170, "Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," Revision 1, provides an acceptable method for providing test documentation. IEEE Std 1008-1987, "Standard for Software Unit Testing," as endorsed by RG 1.171, "Software Unit Testing for Digital Computer Software Used in Safety System of Nuclear Power Plants," Revision 1, provides an acceptable method for satisfying software unit test requirements. SRP BTP 7-14 Section B.3.1.12.4 states the STP should cover all testing done to the software, including unit testing, integration testing, factory acceptance testing, site acceptance testing, and installation testing. SRP BTP 7-14 Section B.3.1.12.1 states that management characteristics of the STP should exhibit purpose, organization, responsibility, and security.

Section 13.0 of the SPM TeR describes the requirements for STP and states that the STP shall be developed in accordance with RG 1.170, Revision 1, and refers to RG 1.171, Revision 1. The STP will cover component testing, integration testing, system testing (factory acceptance testing), and site acceptance testing. Test documentation will conform to IEEE Std 829-2008.

The staff found that Section 13 of the SPM TeR describes the requirements for software test plan, but does not describe the scope of systems that will be tested in the factory and site acceptance tests. For example, in the factory acceptance test, it was not clear whether the PPS be tested alone or whether it will be tested while connected to other I&C systems. In addition, it was not clear whether tests will be conducted with the safety-related and non-safety I&C

systems connected. In RAI 261-8253, Question 07.01-32, the staff asked the applicant to identify the scope of systems that will be connected and tested in an integrated fashion for the factory and site acceptance tests. In the September 21, 2016, response (ML16265A637) to the RAI, the applicant stated that the SPM TeR is intended to describe generic software engineering process and the scope of systems to be tested will be described in the actual planning document for the testing. The system testing (Section 13.3.3 of the SPM TeR) will verify that the software products meet the systems requirements for the software while the integration testing (Section 13.3.2 of the SPM TeR) will verify that the software products meet the software requirements. The applicant also stated that Section 13.4.1, "Test Plan," of the SPM TeR was revised to state that the test plan shall describe the scope of the system/software to be tested. The staff finds the RAI response and proposed changes to the SPM TeR in RAI 261-8253, Question 07.01-32, acceptable since requirements for the test plans are being clarified in the SPM TeR. The incorporation of the proposed markup into the next revision of the SPM TeR was a confirmatory item. The staff verified that the proposed markups have been incorporated into Revision 1 of the SPM TeR, Section 13.4.1. As such, this confirmatory item has been satisfied.

The staff reviewed the criteria for the STP to verify its compliance with applicable regulatory requirements. Based on the staff's evaluations detailed in the discussion above, the staff finds that the criteria for the STP are acceptable as they meet the relevant guidance of SRP BTP 7-14 and requirements in GDC 1, and 10 CFR 50.55a(h)(3).

7.1.4.7.1.12 Secure Development and Operational Environment

For digital safety-related systems, establishment of a secure development environment includes the protection of digital computer-based systems throughout the development lifecycle of the system to prevent unauthorized, unintended, and unsafe modifications. During development, operation, and maintenance, measures should be taken to protect safety-related systems from inadvertent actions that may result in unintended consequences to the system.

Secure Development Environment is defined as the condition of having appropriate physical, logical and programmatic controls during the system development phases (i.e., concepts, requirements, design, implementation, testing) to ensure that unwanted, unneeded and undocumented functionality (e.g., superfluous code) is not introduced into digital safety-related systems.

Secure Operational Environment is defined as the condition of having appropriate physical, logical and administrative controls within a facility to ensure that the reliable operation of digital safety-related systems are not degraded by undesirable behavior of connected systems and events initiated by inadvertent access to the system. Having a secure operational environment is a post-COL activity. The APR1400 design certification review focuses on securing the development environment.

In RG 1.152, Revision 3, the establishment of an SDOE for digital safety-related systems refers to: (1) measures and controls taken to establish a secure environment for development of the digital safety-related system against undocumented, unneeded and unwanted modifications and (2) 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-related system during operations. These SDOE actions may include adoption of protective design features into the digital safety-related

system design to preclude inadvertent access to the system and/or protection against undesirable behavior from connected systems when operational.

Section 14.0 of the SPM TeR describes design features for establishment of SDOE for the digital safety-related I&C systems during the software lifecycle phases (requirements, design, implementation, and test phases) in accordance with RG 1.152, Revision 3.

RG 1.152, Revision 3, provides guidance for designing digital systems (hardware and software) such that they are free from vulnerabilities that could affect the reliability of the system. In the context of this RG, vulnerabilities are considered to be (1) deficiencies in the design that may allow inadvertent, unintended, or unauthorized access or modifications to the safety-related system that may degrade its reliability, integrity or functionality during operations, or (2) an inability of the system to sustain the safety function in the presence of undesired behavior of connected systems. The considerations for hardware access control should include physical access control, configuration of modems, and connectivity to external networks, data links, and open ports. The applicant can provide an SDOE for digital safety-related systems by (1) designing features that will meet the secure operational environment requirements for the systems, (2) ensuring that the system is developed without undocumented codes (e.g., backdoor coding), unwanted functions or applications, and any other coding that could adversely affect the reliable operation of the digital system, and (3) maintaining a secure operational environment for digital safety-related systems in accordance with the station administrative procedures and other programs to protect against unwanted and unauthorized access or changes to these systems.

Regulatory Position 2 of RG 1.152, Revision 3, states that the digital safety-related system development process should identify and mitigate potential weaknesses or vulnerabilities in each phase of the digital safety-related system lifecycle that may degrade the SDOE or degrade the reliability of the system. In particular, Regulatory Positions 2.1 through 2.5 describe digital safety-related system guidance for the establishment of a secure environment during the design and development phases of the lifecycle to ensure reliable operation of digital safety-related systems in accordance with GDC 21. The staff's evaluation of the safety-related I&C design for conformance to GDC 21 is addressed in Section 7.1.4.5 of this SER.

7.1.4.7.1.12.1 Concepts Phase, Regulatory Position 2.1 of RG 1.152, Revision 3

<u>Regulatory Position 2.1, Part I</u>

Regulatory Position 2.1, Part I, of RG 1.152, Revision 3, states, "In the concepts phase, the licensee should identify digital safety-related system design features required to establish a secure operational environment for the system. A licensee should describe these design features as part of its application."

Section 14.2 of the SPM TeR describes the design features that prevent unintended changes to hardware or software code, and to detect unintended changes if they occur. It also provides the attributes of system design features that minimize the potential for security vulnerabilities, which includes; physical access controls, electronic access controls, software alteration controls, and deterministic performance controls.

The staff's evaluation of conformance to IEEE Std 603-1991, Clause 5.9 for control of access features of the I&C system is documented in Section 7.1.4.13 of this SER. The staff's evaluation of the SDOE provisions imposed on the design process for later lifecycle phases are discussed in this section. The staff finds the concept phase acceptable since there are design

features to secure the operational environment as discussed above. The applicant has adequately described the design features required to establish a secure operational environment consistent with Regulatory Position C.2.1 of RG 1.152, Revision 3.

Regulatory Position 2.1, Part II

Regulatory Position 2.1, Part II, of RG 1.152, Revision 3, states:

> The licensee should assess the digital [safety-related] system's potential susceptibility to inadvertent access and undesirable behavior from connected systems over the course of the system's [lifecycle] that could degrade its reliable operation. This assessment should identify the potential challenges to maintaining a secure operational environment for the digital [safety-related] system and a secure development environment for development [lifecycle] phases. The results of the analysis should be used to establish design feature requirements (for both hardware and software) to establish a secure operational environment and protective measures to maintain it.

Section 14.3 of the SPM TeR describes the processes implemented during each software lifecycle phase for the safety-related I&C system, which prevent inclusion of unintended functions in documents and software code. [

]. The staff finds the assessment process acceptable in identifying potential vulnerabilities and identifying measures to mitigate those undesired and unintended changes.

Section 14.3.2 of the SPM TeR, discusses defenses against unauthorized changes in the requirements phase – the software requirements specification (SRS) fully documents the security design requirements established during the concept phase. [

]. The staff finds this approach acceptable since the V&V team would be able to detect insertion of undesired requirements and initiate appropriate corrective actions.

Section 14.3.3 of the SPM TeR, discusses defense against unauthorized changes in design phase – the SDD is developed during this phase and reflects the requirements documented in the SRS. [

]. The staff finds the approach acceptable since the V&V team would be able to detect insertion of undesired designs and initiate appropriate corrective actions.

Section 14.3.4 of the SPM TeR, discusses defense against unauthorized changes in the implementation phase – software code is created during the implementation phase for the common digital platform and for the software that is implemented on each target safety-related I&C system processor, and reflects the detailed design documented in the SDD. [

]. The staff finds the approach acceptable because the V&V team would be able to detect additional functions that are not traceable to the SRS and SDD and initiate appropriate corrective actions.

Section 14.3.5 of the SPM TeR, discusses defense against unauthorized changes in the test phase – during this phase, common system platform operating system and application software is integrated with the common digital platform hardware for each system, and covers integration and system factory acceptance test (FAT) testing. [

].

In RAI 261-8253, Question 07.01-33, the applicant was asked to provide additional information on the SDOE of APR1400 safety I&C systems, including details on the vulnerability assessment and the use of commercial off-the-shelf (COTS) software. Section 14.0 of the SPM TeR, "SDOE," provides information on the establishment of SDOE for the digital safety-related I&C systems during the software lifecycle phases. The staff reviewed this SDOE and requested the applicant to provide the following information in order for the staff to determine whether the APR1400 safety-related I&C systems meet the requirements IEEE Std 603-1991, Clause 5.9:

1. Section 14.1 of the SPM TeR states that "this section provides the guidance for establishment of SDOE for the digital safety-related I&C systems during the software lifecycle phases in accordance with [RG 1.152, Revision 3]." It was not clear to the staff whether the applicant is committing to the information presented in this section or whether it is just guidance that may not be used during the lifecycle phases of safety-related I&C systems. Clarify that the digital safety-related systems will follow the criteria established in this section of the SPM TeR.

2. The staff reviewed the summary of the vulnerability assessment in Section 14.5 of the SPM TeR and finds that additional information is needed to evaluate this vulnerability assessment. Specifically, this vulnerability assessment is generic and does not seem to address potential vulnerabilities specific to the safety-related I&C system development and operational environment. In addition, it is unclear how each of the identified vulnerabilities is addressed by the security features described Sections 14.3.1 through 14.3.5 of the SPM TeR. Modify the SPM TeR to provide additional information regarding vulnerabilities specific to the safety-related I&C systems and provide a mapping of how each of these vulnerabilities are addressed in Sections 14.3.1 through 14.3.5 of the SPM TeR.

3. Section 14.4, "Security Processes for [COTS] Software," of the SPM TeR states, "This section describes the processes employed to (1) achieve high assurance that COTS software products are free of unwanted code that could degrade the security of the safety-related I&C system, and (2) to ensure that any unwanted code that may be introduced into the safety-related I&C system by the COTS software products is detected and eliminated." The staff reviewed the information presented and could not find what measures are employed to ensure that COTS software products are free of unwanted code that could degrade the security of the safety-related I&C system. Since most COTS software code is not available for review to determine if this code may

degrade the security or operation of the safety-related I&C system, what measures are in place to determine that the COTS software will not adversely impact the safety-related I&C system.

In the December 10, 2015, response (ML15344A244) to RAI 261-8253, Question 07.01-33, the applicant provided the following response:

1. The applicant stated that the criteria established in Section 14 of the SPM TeR are followed by the digital I&C systems, and proposed revisions to Section 14.1 that will now state, "This section describes the establishment of the SDOE for the digital I&C systems during the software lifecycle phases in accordance with [RG 1.152, Revision 3]. The phases include concept, requirements, design, implementation, and test, as defined in Section 2.2. The digital safety-related I&C systems will be developed in accordance with this section." The staff finds the RAI response and proposed changes to the SPM TeR in RAI 261-8253, Question 07.01-33, Part 1, acceptable since the applicant commits to establishing a SDOE in accordance with RG 1.152, Revision 3. The incorporation of the proposed markup into the next revision of the SPM TeR was a confirmatory item. The staff verified that the proposed markups have been incorporated into Revision 1 of the SPM TeR, Section 14.1. As such, this confirmatory item has been satisfied.

2. The applicant stated that Section 14.5 of the SPM TeR contains a general description of vulnerability assessment. Thus, "Summary" in the section title was removed. The vulnerability assessment is performed as a part of the secure analysis required by RG 1.168, Revision 2. The vulnerability assessment for each phase of the software development lifecycle process will be performed and the vulnerabilities will be addressed in the phase V&V report. Section 14.5 of the SPM TeR was revised to change the title as stated above, add a sentence at the end that states "The assessment shall be performed and addressed in the V&V report as a part of the secure analysis described in RG 1.168, Revision 2. It will assure that the security features and processes are protected from inadvertent manipulation of the development." The staff finds the RAI response to question 07.01-33, Part 2 to be incomplete and requested the applicant to fully address staff's question. Based on review of the vulnerability assessment discussion in Section 14.5 of the SPM TeR, the staff finds that additional information is needed to evaluate this vulnerability assessment. Specifically, this vulnerability assessment is generic and does not seem to address potential vulnerabilities specific to the safety-related I&C system development and operational environment. In addition, it is unclear how each of the identified vulnerabilities is addressed by the security features described Sections 14.3.1 through 14.3.5 of the SPM TeR. As a supplement question to this RAI, the applicant is requested to provide additional information regarding vulnerabilities specific to the APR1400 safety-related I&C systems and mapping of how each of these vulnerabilities are addressed in Sections 14.3.1 through 14.3.5 of the SPM TeR. Also, the applicant should describe measures to mitigate the identified vulnerabilities. The applicant may also consider modifying the proposed changes to the SPM TeR Section 14.5, from "The assessment shall be performed..." to "The vulnerability assessment shall be performed for each phase of the software development lifecycle process..." RAI 261-8253, Question 07.01-33, Part 2, was tracked as an open item.

   In the September 19, 2017, supplemental response to RAI 261-8253, Question 07.01-33 (ML1726A318), the applicant provided a new technical report, APR1400-E-J-NR-17001, "Secure Development and Operational Environment for APR1400 Computer-Based I&C

Safety Systems," (hereafter referred to as SDOE TeR). This technical report provides information on the vulnerabilities specific to the safety-related I&C systems both for the development and operational environment and a mapping of how each vulnerability is addressed. The applicant also included a reference for this technical report in the Safety I&C System TeR and IBR the SDOE TeR into the FSAR. Because the applicant provided a SDOE vulnerability analysis specific to the APR1400 safety-related I&C systems and demonstrated how each vulnerability will be controlled by the design in accordance with RG 1.152, Revision 3, the staff finds the safety-related I&C system meets the logical control of access requirements specified in IEEE Std 603-1991, Clause 5.9. As such the open item associated with RAI 261-8253, Question 07.01-33, Part 2, is closed and resolved. The incorporation of the proposed markups into the next revision of the DCD Tier 2 Table 1.6-2 and Sections 7.1.2.46 and 7.1.5, the Safety I&C System TeR and the submittal of the SDOE TeR was a confirmatory item. The staff verified the that the proposed markups have been incorporated into DCD Tier 2 Table 1.6-2 and Sections 7.1.2.46 and 7.1.5, the Safety I&C System TeR and the SDOE TeR has been submitted. As such, this confirmatory item has been satisfied.

3. Although the applicant stated that it is not possible to fully investigate the source code of the COTS, the applicant proposed to evaluate the COTS in accordance with the qualification process. The applicant proposed revisions to Section 14.4 of the SPM TeR to describe the qualification process for the COTS to determine that the COTS will not adversely impact the safety-related I&C system. The staff finds the RAI response and proposed changes to the SPM TeR in RAI 261-8253, Question 07.01-33 Part 3, acceptable since the applicant will ensure that the safety-related I&C system will only employ COTS system software after the COTS system software is qualified in accordance with the qualification process described in Sections 4.1.2 and 4.10.1 of the SPM TeR. The incorporation of the proposed markup into the next revision of the SPM TeR was a confirmatory item. The staff verified that the proposed markups have been incorporated into Revision 1 of the SPM TeR, Section 14.4. As such, this confirmatory item has been satisfied.

<u>Regulatory Position 2.1, Part III</u>

Regulatory Position 2.1, Part III, of RG 1.152, Revision 3, states the following.

> The licensee should not allow remote access to the [safety-related] system. For the purposes of this guidance, remote access is defined as the ability to access a computer, node, or network resource that performs a safety function or that can affect the safety function from a computer or node that is located in an area with less physical security than the [safety-related] system (e.g., outside the protected area).
>
> Other NRC staff positions and guidance govern unidirectional and bidirectional data communications between safety and non-safety digital systems.

Section 14.2.2 of the SPM TeR, states that [ ]. The staff finds this acceptable to meet this regulatory position. The staff evaluation of safety I&C systems with respect to Digital I&C Interim Staff Guidance-4, (DI&C-ISG-04), "Highly Integrated Control Room – Communications," Revision 1, is discussed in Section 7.9 of this SER.

7.1.4.7.1.12.2 Requirements Phase, Regulatory Position 2.2 of RG 1.152, Revision 3

Regulatory Position 2.2.1, System Features, Part I

Regulatory Position 2.2.1, Part I, of RG 1.152, Revision 3, states, "The licensee should define the functional performance requirements and system configuration for a secure operational environment; interfaces external to the system; and requirements for qualification, human factors engineering (HFE), data definitions, documentation for the software and hardware, installation and acceptance, operation and execution, and maintenance."

Section 14.3 of the SPM TeR, states that secure operational environment design concepts are developed into system requirements during the concept and requirements phases as described in the SPM TeR. Section 14.3.2 of the SPM TeR states the SRS fully documents the security design requirements established during the concept phase, including the design features discussed in Section 14.2 that minimize the potential for security vulnerabilities. The staff finds the applicant's approach acceptable to define functional performance requirements and system configuration for a secure operational environment and meets the guidance of RG 1.152, Revision 3.

Regulatory Position 2.2.1, System Features, Part II

Regulatory Position 2.2.1, Part II, of RG 1.152, Revision 3, states, "The design feature requirements intended to maintain a secure operating environment and ensure reliable system operation should be part of the overall system requirements. Therefore, the verification process of the requirements phase should ensure the correctness, completeness, accuracy, testability, and consistency of the system's SDOE feature."

Section 14.3.2 of the SPM TeR, states that [

]. The staff finds the approach acceptable to meet this regulatory position because the IV&V Team will confirm that design feature requirements are implemented correctly.

Regulatory Position 2.2.1, System Features, Part III

Regulatory Position 2.2.1, Part III, of RG 1.152, Revision 3, states "Requirements specifying the use of pre-developed software and systems (e.g., reused software and COTS systems) should address the reliability of the safety-related system (e.g., by using pre-developed software functions that have been tested and are supported by operating experience)."

Section 14.4 of the SPM TeR, describes the processes employed to (1) achieve high assurance that COTS software products are free of unwanted code that could degrade the security of the safety-related I&C systems, and (2) to ensure that any unwanted code that may be introduced into the safety-related I&C system by the COTS software products is detected and eliminated. [

]. The staff finds the approach acceptable to meet this regulatory position because the dedication of the COTS software product ensures the quality and reliability for performing its intended safety function is equal to the software products developed under 10 CFR Part 50, Appendix B quality assurance program.

Regulatory Position 2.2.2, Development Activities

Regulatory Position 2.2.2 of RG 1.152, Revision 3, states, “During the requirements phase, the licensee should prevent the introduction of unnecessary or extraneous requirements that may result in inclusion of unwanted or unnecessary code.”

Section 14.3.2 of the SPM TeR, states that [ ]. The staff finds this approach acceptable to meet this regulatory position.

7.1.4.7.1.12.3 Regulatory Position 2.3, Design Phase

Regulatory Position 2.3.1, System Features, Part I

Regulatory Position 2.3.1, Part I, of RG 1.152, Revision 3, states:

> The [safety-related] system design features for a secure operational environment identified in the SysRS should be translated into specific design configuration items in the SysDD.
>
> The [safety-related] system design configuration items for a secure operational environment intended to ensure reliable system operation should address control over (1) physical and logical access to the system functions, (2) use of [safety-related] system services, and (3) data communication with other systems. Design configuration items that incorporate pre-developed software into the [safety-related] system should address how this software will not challenge the secure operational environment for the [safety-related] system.

Section 14.3.3 of the SPM TeR, states that [

]. Since there are design features for controlling access and an IV&V activity to ensure such access, the staff finds this approach acceptable to meet this regulatory position.

Regulatory Position 2.3.1, System Features, Part II

Regulatory Position 2.3.1, Part II, of RG 1.152, Revision 3, states, “Physical and logical access control features should be based on the results of the assessment performed in the concepts phase of the lifecycle. The results of this assessment may identify the need for more complex access control measures, such as a combination of knowledge (e.g., password), property (e.g., key and smart card), or personal features (e.g., fingerprints), rather than just a password.”

Section 14.2 of the SPM TeR, discusses planned physical and logical access control features such as [ ]. During each development lifecycle phase, assessment shall be performed to confirm that there are adequate physical and logical controls to prevent unintended software changes, and as a result, the staff finds this approach acceptable to meet this regulatory position.

7.1.4.7.1.12.4 Regulatory Position 2.4, Implementation Phase

Regulatory Position 2.4.1, System Features

Regulatory Position 2.4.1 of RG 1.152, states "The developer should ensure that the transformation from the system design specification to the design configuration items of the secure operational environment is correct, accurate, and complete."

Section 14.3.4 of the SPM TeR, states that the software code created during implementation phase reflects the detailed designs documented in the SDD, which is developed during the design phase. All software codes are independently verified and validated on a component by component basis. The staff finds this approach acceptable to meet this regulatory position.

Regulatory Position 2.4.2, Development Activities, Part I

Regulatory Position 2.4.2, Part I, of RG 1.152, Revision 3, states:

> The developer should implement secure development environment procedures and standards to minimize and mitigate any inadvertent or inappropriate alterations of the developed system. The developer's standards and procedures should include testing, (such as scanning), as appropriate, to address undocumented codes or functions that might (1) allow unauthorized access or use of the system or (2) cause systems to behave outside of the system requirements or in an unreliable manner.
>
> The developer should account for hidden functions and vulnerable features embedded in the code, their purpose and their impact on the integrity and reliability of the [safety-related] system. These functions should be removed or (as a minimum) addressed (e.g., as part of the FMEA of the application code) to prevent any unauthorized access or degradation of the reliability of the [safety-related] system.

Section 14.4 of the SPM TeR, states that the safety-related I&C systems use pre-developed system software that runs within the operating system of the safety-related I&C system processors, which is designed to only accept authorized access and documented code. Section 14.3.4 of the SPM TeR describes defensive strategies planned for the implementation phase to prevent undocumented code, unauthorized and undocumented functions or applications. The staff finds this approach acceptable as it meets the aforementioned regulatory position.

Regulatory Position 2.4.2, Development Activities, Part II

Regulatory Position 2.4.2, Part II, of RG 1.152, Revision 3, states:

> COTS systems are likely to be proprietary and generally unavailable for review. In addition, a reliable method may not exist for determining the complete set of system behaviors inherent in a given operating system (e.g., operating system suppliers often do not provide access to the source code for operating systems and callable code libraries). In such cases, unless the application developer can modify these systems, the developer should ensure that the features within the operating system do not compromise the required design features of the secure

> operational environment so as to degrade the reliability of the digital [safety-related] system.

Section 14.4 of the SPM TeR, describes the processes employed to (1) achieve high assurance that COTS software products are free of unwanted code that could degrade the security of the safety-related I&C systems, and (2) to ensure that any unwanted code that may be introduced into the safety-related I&C system by the COTS software products is detected and eliminated. [ ]. The staff finds the approach acceptable as it meets the aforementioned regulatory position because the dedication of the COTS software product ensures the quality and reliability for performing its intended safety function is equal to the software products developed under 10 CFR Part 50, Appendix B quality assurance program.

7.1.4.7.1.12.5 Regulatory Position 2.5, Test Phase

Regulatory Position 2.5 of RG 1.152, Revision 3, states the following.

> The secure operational environment design requirements and configuration items intended to ensure reliable system operation should be part of the validation effort for the overall system requirements and design configuration items. Therefore, design configuration items for the secure operational environment are just one element of the overall system validation. Each system design feature of the secure operational environment should be validated to verify that the implemented feature achieves its intended function to protect against inadvertent access or the effects of undesirable behavior of connected systems and does not degrade the [safety-related] system's reliability.

Section 14.3.5 of the SPM TeR, states that the system test (FAT) of the fully integrated system to validate that the system meets the system requirements related to the software. The system test is conducted with all connected system interfaces, including those that pose security threats. The applicant also stated that the independent validation testing demonstrates that all system requirements related to the software function correctly in the final integrated system. Since there is independent testing performed to ensure design requirements and configuration items are implemented correctly, the staff finds this approach acceptable to meet this regulatory position.

The applicant also states that a vulnerability re-assessment will be conducted at the completion of the test phase to ensure that the security requirements established during the requirement phase are adequate to address known security threats, including new threats that were not previously identified during the concept phase.

Regulatory Position 2.5.1, System Features

Regulatory Position 2.5.1 of RG 1.152, Revision 3, states, "The developer should correctly configure and enable the design features of the secure operational environment. The developer should also test the system hardware architecture, external communication devices, and configurations for unauthorized pathways and system integrity. Attention should be focused on built-in original equipment manufacturer features."

Section 14.3.5 of the SPM TeR states that testing methodology, as described in the SPM TeR, ensures that the software and data secure operational environment design requirements

features have been designed and implemented in accordance with this regulatory position, including but not limited to external hardware connections and external communication gateways. This testing methodology includes application level testing and independent validation testing, and as a result, the staff finds this approach acceptable as it meets the aforementioned regulatory position.

7.1.4.7.1.12.6 Limitations and Conditions

Acceptability of software for safety-related system functions is dependent upon (1) confirmation that acceptable software plans were prepared to control software development activities as described in Section B.3.1 of SRP BTP 7-14, (2) evidence that the plans were followed in an acceptable software lifecycle as described in Section B.3.2 of SRP BTP 7-14, and (3) evidence that the process produced acceptable design outputs as described in Section B.3.3 of SRP BTP 7-14.

Section B.3.1 of SRP BTP 7-14 discusses acceptance criteria for planning activities. Since the SPM TeR only addresses the planning activities, the SPM TeR is reviewed using this set of acceptance criteria. Section B.3.2 of SRP BTP 7-14 discusses acceptance criteria for implementation activities and documentation. Section B.2.2 of SRP BTP 7-14 states that instances of software lifecycle process implementation may be contained in safety analyses, V&V reports, configuration management reports, and testing activities. Section B.3.3 of SRP BTP 7-14 discusses functional and process characteristics acceptance criteria for the design outputs. B.2.3 of SRP BTP 7-14 states that software lifecycle process design outputs may be contained in system requirements specifications, system architecture description, system design specifications, code listings, build documents, installation configuration tables, operation manuals, maintenance manuals, and training manuals.

Establishment of a secure development environment includes the protection of both physical and logical access to the safety-related system and its data such that controls should be provided to prevent unauthorized changes. Controls should address access through both network connections and maintenance equipment. Additionally, the design of the plant DCSs should ensure that the systems do not present an electronic path by which a person can make unauthorized changes to plant safety-related systems or display erroneous plant status information to the operators.

The staff reviewed the SPM TeR to verify its compliance with applicable regulatory requirements. Based on the resolution of the open item associated with RAI 261-8253, Question 07.01-33, and the provision of sufficient information to demonstrate that safety-related and ITS system software will be developed to quality requirements and processes as endorsed by RGs on software development, the staff has determined the applicant provided sufficient information in the SPM TeR to demonstrate the requirements in 10 CFR Part 50, Appendix A, GDC 1, and IEEE Std 603-1991, Clauses 5.3 and 5.9 are met.

7.1.4.8 Equipment Qualification

The staff reviewed the APR1400 design certification application to verify that GDC 2, “Design Bases for Protection Against Natural Phenomena,” GDC 4, “Environmental and Dynamic Effects Design Bases,” 10 CFR 50.49, “Environmental Qualification of Electric Equipment Important to Safety for Nuclear Power Plants,” and IEEE Std 603-1991, Clause 5.4 have been adequately addressed for the APR1400 safety-related systems. GDC 2 requires, in part, that SSCs important to safety shall be designed to withstand the effects of natural phenomena, such as

earthquakes, tornadoes, hurricanes, floods, tsunami, and seiches, without loss of capability to perform their safety functions. GDC 4 requires, in part, SSCs important to safety shall be designed to accommodate the effects of and to be compatible with the environmental conditions associated with normal operation, maintenance, testing, and postulated accidents, including LOCAs. 10 CFR 50.49 requires that safety be qualified to perform its intended safety functions. IEEE Std 603-1991, Clause 5.4, requires, in part, that safety-related system equipment 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 continually meeting the performance requirements, as specified in the design basis. The staff used the guidance of SRP Appendix 7.1-A, which indicates that the applicant's design bases should identify those systems and components that are qualified to accommodate the effects of environmental conditions. Also, the staff review included review of equipment qualification for environmental conditions in accordance with the guidance provided in SRP Appendix 7.1-C, Section 5.4, and SRP Appendix 7.1-D. Furthermore, regarding the staff determination of whether the design meets the requirements of GDC 4, the staff review of the application's equipment qualification for environmental conditions is conducted in accordance with the guidance in SRP Appendix 7.1-C, Section 5.4. Evaluation of conformance to IEEE Std 603-1991, Clause 5.4 is primarily addressed in the evaluation of conformance to IEEE Std 7-4.3.2-2003, Clause 5.4.

The ITAAC items associated with equipment quality or qualification in DCD Tier 1, Tables 2.5.1-5, 2.5.3-3, and 2.5.4-4, state, in part, that type tests, analyses, or a combination of type test and analyses will be performed for Class 1E equipment. It was not clear whether the above ITAAC items include all Class 1E equipment in the scope of the approved Common Q platform; whether type tests, analyses, or a combination of type test and analyses will be re-performed for all those types of Class 1E Common Q equipment; and whether the qualification in the approved Common Q platform will be credited for the safety-related I&C system during the stage of ITAAC closure. Therefore, the staff issued RAI 323-8281, Question 07.03-9, requesting the applicant to clarify whether the ITAAC items associated with equipment quality or qualification in DCD Tier 1, Tables 2.5.1-5, 2.5.3-3, and 2.5.4-4, include the Class 1E equipment in the scope of the Common Q platform which will be used for the safety-related I&C system. Also, the applicant was requested to clarify whether type tests, analyses, or a combination of type test and analyses will be performed again for those types of Class 1E Common Q equipment for plant-specific conditions or the qualification of the approved Common Q platform will be credited during the closure stage of ITAAC.

In the March 4, 2016 response to RAI 323-8281, Question 07.03-9 (ML16064A060), the applicant stated that the ITAAC associated with equipment quality or qualification in DCD Tier 1, Tables 2.5.1-5, 2.5.3-3, and 2.5.4-4, includes all Class 1E equipment in the scope of the Common Q platform for the safety-related I&C system. The applicant also stated in the response that the type tests, analyses, or combination of type test and analyses performed for all Class 1E equipment are not to be re-performed for the Common Q platform, and the qualification of the NRC-approved Common Q platform itself will be credited during the closure stage of the ITAAC. However, in this RAI response, the applicant did not address whether type tests, analyses, or a combination of type test and analyses will be performed for those types of Class 1E Common Q equipment for plant-specific conditions. The staff requested the applicant to provide supplemental information to address this issue. In the revised response dated March 9, 2017 (ML17068A069), the applicant stated that type tests, analyses, or a combination of type test and analyses will be performed for the safety-related I&C system cabinets, including the Common Q platform, for plant-specific conditions. The applicant also stated, in part, that the suitability of all new components is assessed to meet applicable requirements in accordance with the commercial grade dedicator's quality assurance program. The criteria include an

evaluation of the impact to equipment qualification consistent with the intended use of the components. In the revised response the applicant addressed the staff's concern on whether the equipment qualification testing for Class 1E Common Q equipment will be performed for plant specific conditions, as required in the ITAAC items discussed above. The applicant clarified in the revised response that type tests, analyses, or a combination of type test and analyses will be conducted for the Common Q platform for plant-specific conditions. Therefore, the staff found that the revised response is acceptable. The applicant stated that the proposed supplemental changes will be incorporated in the revised Safety I&C System TeR. But the staff found that the markups proposed in the revised response were not incorporated in Revision 1 of the Safety I&C System TeR. Therefore, RAI 323-8281, Question 07.03-9 was being tracked as a confirmatory item. The staff verified the proposed markups has been incorporated in Revision 2 of the Safety I&C System TeR. As such, this confirmatory item has been satisfied.

RG 1.180, "Guidelines for Evaluating Electromagnetic and Radiofrequency Interference in Safety-Related Instrumentation and Control Systems," Revision 1, states, in part, that either set of test methods (MIL-Std-461E, "Requirements for the Control of Electromagnetic Interference Characteristics of Subsystems and Equipment," or IEC 61000-6-4, "Electromagnetic Compatibility") should be applied in its entirety, without selective application of individual methods (i.e., no mixing and matching of test methods) for emissions testing. The Safety I&C System TeR identifies both MIL-Std-461E and IEC-61000, Part 4 Series standards are used for equipment qualification of safety-related I&C system equipment. However, it was not clear which sets of standards are used to demonstrate that the safety-related I&C system equipment, including the control system within the ESFAS, will meet the equipment qualification requirements for the EMC. In RAI 43-7887, Question 07.01-23, the staff requested the applicant to provide justification or clarification on whether the sets of standards are mixed, which is contrary to the guidance in RG 1.180, Revision 1. In the September 24, 2015, response to RAI 43-7887, Question 07.01-23 (ML15267A764), the applicant stated the EMI/RFI emissions test, EMI/RFI susceptibility/immunity test, and surge withstand capability test for qualification of the safety-related I&C system equipment are each performed based on the designated set of test methods either from MIL-Std-461E or from IEC-61000, Part 4 Series. The applicant further clarified in the above RAI response that for emissions testing on the safety-related I&C system equipment, the MIL-Std-461E test methods are applied without any individual test methods from IEC-61000, Part 4 Series. For the susceptibility and immunity testing, and surge withstand capability testing on the safety-related I&C system equipment, the IEC-61000, Part 4 series test methods are applied without any individual test methods from MIL-Std-461E. From the additional clarification provided in the above RAI response, the staff found that the equipment qualification on EMC for the safety-related I&C system conforms to the regulatory guidance in RG 1.180, Revision 1 and that either MIL-Std-461E test methods or IEC-61000 test methods will be used in their entirety for each required test.

RG 1.180, Revision 1, RG 1.100, Revision 3, RG 1.209, Revision 0, and EPRI TR-107330, "Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants "and EPRI TR-102323, "Guidelines for Electromagnetic Interference Testing in Nuclear Power Plants," state, in part, that tests for electrical fast transient, electrostatic discharge, surge withstand capability, and Class 1E to Non-Class 1E isolation should be included as part of the equipment qualification testing program for the safety-related I&C system equipment. The staff found that there was lack of design information in Section 6, "Equipment Qualification," of the Safety I&C System TeR on whether these equipment qualification tests are included or not. In RAI 43-7887, Question 07.01-24, the staff asked the applicant to provide necessary design information to demonstrate that the equipment qualification program of the safety-related I&C system

equipment will include those equipment qualification tests, and to clarify which associated ITAAC items in DCD Tier 1 will include these equipment qualification tests. In the September 24, 2015 response to RAI 43-7887, Question 07.01-24 (ML15267A764), the applicant stated that the equipment qualification testing includes electrical fast transient, electrostatic discharge, surge withstand capability, and Class 1E to Non-Class 1E isolation testing. This information was added to Section 6 of the Safety I&C System TeR. The related ITAAC items are Items 2 and 3 in Table 2.5.1-5 and Items 2 and 16 in Table 2.5.4-4 of DCD Tier 1. The safety-related I&C system equipment which is located in the mild environment is qualified to the guidance of IEEE Std 323-2003, which is endorsed by RG 1.209, Revision 0.

As included in the above the response to RAI 43-7887, Questions 07.01-23 and 07.01-24, the applicant proposed to revise Section 7.1.2.24 of DCD Tier 2 and the Safety I&C System TeR to replace the references to IEEE Std 323-1983 with references to IEEE Std 323-2003. The staff agrees with the proposed changes because the applicant commits to perform tests for electrical fast transient, electrostatic discharge, surge withstand capability, and Class 1E to Non-Class 1E isolation as specified in RG 1.180, Revision 1, RG 1.100, Revision 3, and RG 1.209, Revision 0. The staff verified that the proposed markups have been incorporated into Revision 1 of the Safety I&C System TeR. As such, this confirmatory item has been satisfied.

With regards to environmental qualification, DCD Tier 2 Section 7.2.2.8 discusses the applicability of environmental qualifications to the RPS. Section 7.2.2.8 states the RPS meets the requirements of IEEE Std 323-2003, for environmental qualification of Class 1E equipment. IEEE Std 323-2003 is endorsed by RG 1.209, Revision 0. The applicant state that the RPS meets seismic requirements as per guidance from RG 1.89, “Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants,” Revision 1. The applicant also commits to RPS meeting the requirements of RG 1.180, Revision 1, for EMI/RFI tolerances. Similarly for ESF Systems, the applicant states in DCD Tier 2 Section 7.3.2.8 that the ESF systems have been designed and tested to meet each of the above-mentioned equipment qualification requirements. For interlocks important to safety, the applicant states in DCD Tier 2 Section 7.6.2.2 that these components are implemented using Class 1E equipment and qualified to operate in worse case environmental conditions for the areas of the plant they reside in.

The Safety I&C System TeR, Section 6 provides more details on the environmental qualification of safety equipment. The report outlines three categories of focus for equipment qualification testing and validation: environmental, seismic and EMC.

<u>Environmental</u>

Section 6 of the Safety I&C TeR, states the safety equipment qualified to meet the requirements of IEEE Std 323-2003 are located in mild environments and are provided with qualified heating, ventilation, and air conditioning (HVAC) supporting systems. Testing with regard to rising temperatures with fully energized I&C cabinets is performed to demonstrate that, with supporting analysis individual equipment temperatures specifications are not exceeded when exposed to environmental conditions. Table 6-1 of the Safety I&C System TeR describes the environmental design requirements under the analysis. As evaluated above, the staff found that the supplemental response to RAI 323-8281, Question 07.03-9, is acceptable. Hence, the applicant provided sufficient information in the design certification application and within the initial and supplemental responses to demonstrate compliance with regulatory requirements for environmental qualification for safety-related I&C systems. Therefore the issue associated with the above RAI 323-8281, Question 07.03-9, has been closed. The incorporation of the

proposed markups into the Safety I&C System TeR, Revision 2 was being tracked as a confirmatory item. The staff verified the proposed markups have been incorporated into the Safety I&C System TeR, Revision 2. As such, this confirmatory item has been satisfied.

Seismic

The applicant states in Section 6 of the Safety I&C System TeR that equipment used to implement the safety-related I&C systems meet the guidance of IEEE Std 344-2004, which is endorsed by RG 1.100, Revision 3. The applicant also states that for verification of operability during seismic events, functional testing is performed with energized equipment using simulated input and interfaces. The applicant also accounts for equipment aging by cycling electro-mechanical equipment to end-of-life conditions prior to seismic qualification. Per the applicant, the safety equipment designated as Seismic Category I meets the guidance of RG 1.29, "Seismic Design Classification," Revision 4. RG 1.29, Revision 4, provides an acceptable methodology for identifying and classifying features of light-water cooled nuclear plants that should be designed to withstand a safe shutdown earthquake.

The applicant states that seismic testing and analysis demonstrates that qualified equipment will not loosen, bend or crack such that operations are affected during seismic events and safety plant parameters are maintained. As discussed above in this section, the staff found that the applicant provided sufficient information in the design certification application and within the initial and supplemental RAI responses to demonstrate compliance with regulatory requirements for seismic qualification for the safety-related I&C systems. Therefore, the issue associated with the above RAI 323-8281, Question 07.03-9, has been closed. The incorporation of the proposed markups into the Safety I&C System TeR, Revision 2 was being tracked as a confirmatory item. The staff verified the proposed markups have been incorporated into the Safety I&C System TeR, Revision 2. As such, this confirmatory item has been satisfied.

EMC

The applicant states that for EMC conformance, the testing is performed in three categories:

- EMI/RFI Emissions.
- EMI/RFI Susceptibility/Immunity.
- Surge Withstand Capability.

The EMC testing confirms that safety-related system function has not been affected and performs within specified requirements. The testing is conducted on equipment that is representative of the as-delivered configuration of the system being tested. The testing and qualification is based on conformance to RG 1.180, Revision 1.

Section 3.4.22 of the Safety I&C System TeR states that the safety-related I&C system design complies with the guidance of RG 1.204, "Guidelines for Lightening Protection of Nuclear Power Plants," Revision 0. RG 1.204, Revision 0 endorses, IEEE Std 1050-1996, "Guide for Instrumentation and Control Equipment Grounding in Generating Stations," as an acceptable method for the design and installation of lightening protection systems in nuclear power plants. The applicant does not identify the revision for which the design commitment applies. In addition, DCD Tier 2 Table 7.1-1, "Regulatory Requirements Applicability Matrix," references RG 1.204, Revision 0, but does not have the document apply to any safety-related system. The

applicant also mentions that instrument sensing lines for safety equipment conforms to the guidance of RG 1.151, “Instrument Sensing Lines,” Revision 1, which endorses ANSI/ISA-67.02.01-1999, “Nuclear Safety-Related Instrument-Sensing Line Piping and Tubing Standard for Use in Nuclear Power Plants.” The applicant does not reference the revision of this document for which the design commitment applies.

SRP Section 7.1-C states, in part, that lightning protection should be addressed as part of the EMC review and conforms to the guidance of RG 1.204, Revision 0. Section 3.4.22 of the Safety I&C System TeR states the safety-related I&C system design complies with the guidance of RG 1.204, Revision 0. DCD Tier 2 Table 7.1-1, describes the applicability of regulations and guidance the safety-related and non-safety I&C systems. RG 1.204, Revision 0, is listed on this table, but the applicant does not state that this document applies to any I&C systems (it refers to Chapter 8 of the FSAR). DCD Tier 1 Table 2.5.1-5, for example, has an ITAAC Item for EMC compliance, but does not incorporate lightning protection, nor does any other item in this table. Also, 10 CFR 50.49 is not captured as a regulatory requirement in this table. The staff issued RAI 356-7881, Question 07-19, to address these topics.

In the April 5, 2016 response to RAI 356-7881 Question 07-19 (ML16096A179), the applicant clarified its position regarding requirements for lightning protection and 10 CFR 50.49. Regarding lightning protection, the applicant provided the following information in its response:

> Section B, “Discussion,” of NRC RG 1.204, [Revision 0] identifies IEEE Std 1050-1996 as describing design and installation practices regarding grounding methods for generating station I&C equipment. Accordingly, [DCD] Tier 2 Section 7.1.2.56, was updated to state that the I&C systems comply with IEEE Std 1050-1996, as endorsed by NRC RG 1.204, [Revision 0]. Also, IEEE Std 1050-1996 was added in [DCD] Tier 2 Section 7.1.5. As the Safety I&C System technical report, Section 3.4.22, “Guidelines for Lightning Protection of Nuclear Power Plants,” states that the [safety-related] I&C system equipment is designed to comply with the guidance of RG 1.204, [Revision 0], the “I&C System” columns in [DCD] Tier 2 Table 7.1-1 item 56 will be checked for requirement applicability. Item 2 in [DCD], Tier 1 Section 2.5.1.1 and Table 2.5.1-5 will include the lightning strikes condition to indicate that the Class 1E equipment identified in Table 2.5.1-1 are to be able to withstand lightning strikes, electrical surge, EMI, RFI, and [electric static discharge].

The staff reviewed the proposed changes and found the proposed changes adequate because the applicant properly identified and updated Tier 1 design information to include specific language for design requirements of and testing for lightning protection and included commitments to conform to RG 1.204, Revision 0, for lightning protection in DCD Tier 2 as well as the Safety I&C System TeR.

Regarding 10 CFR 50.49, the applicant stated, in part, that DCD Tier 2 Table 7.1-1 is exactly based on Item 1, “10 CFR Parts 50 and 52,” of Table 7-1 in SRP Revision 5. This table does not include 10 CFR 50.49 as an applicable requirement. The applicant states that Section 3.1 of the Safety I&C System TeR specifies that the criterion of 10 CFR 50.49 is not applicable since the safety-related I&C system will be installed in a mild environment. This response is acceptable as the applicant is following prescribed staff guidance on requirements applicability in the SRP. SRP Section 7.1-C, Section 5.4, also states that for I&C reviews the focus is principally on mild environment qualification and that 10 CFR 50.49 reviews will be designated towards equipment residing in harsh environment, which is beyond the scope of this section of

the evaluation. As such, the staff finds that 10 CFR 50.49 is not an applicable requirement for this design since all safety-related I&C systems will be installed in mild environments.

DCD Tier 2, Sections 7.2.2.8 and 7.3.2.8, (RPS and ESF-CCF respectively), state that these systems meet the requirements of IEEE Std 323-2003 for environmental qualification, IEEE Std 344-2004 for seismic qualification, RG 1.89, Revision 1, and RG 1.209, Revision 0, as well as emission and susceptibility acceptance criteria of EMI and RFI from RG 1.180, Revision 1. Section 6 of the Safety I&C System TeR states that the safety-related I&C system (e.g., PPS, CPCS, ESF-CCS) are qualified to meet the guidance of IEEE Std 323-2003, as endorsed by RG 1.209, Revision 0, for equipment located in mild environment conditions. Overall, the staff finds the applicant's response to RAI 356-7881, Question 07-19 and associated proposed changes acceptable as discussed in the preceding two paragraphs. The staff verified that that the proposed markups have been incorporated into Revision 1 of the Safety I&C System TeR. As such, this confirmatory item has been satisfied.

The applicant adequately identified the SSCs as well as the appropriate level of qualification for the equipment based upon staff-endorsed guidance. The applicant has committed to comply with the appropriate guidance for safety-related system equipment based upon review of applicable design commitments made in the FSAR and applicable technical reports. As discussed above in this section, the staff found that the applicant provided sufficient information in the design certification application and within the initial and supplemental responses to demonstrate compliance with regulatory requirements for EMC qualification for the safety-related I&C systems. Therefore, the issue associated with the RAI 323-8281, Question 07.03-9, has been closed. The incorporation of the proposed markups into the Safety I&C System TeR, Revision 2 was being tracked as a confirmatory item. The staff verified the proposed markups have been incorporated into the Safety I&C System TeR, Revision 2. As such, this confirmatory item has been satisfied.

7.1.4.9 System Integrity

The staff reviewed the APR1400 design certification application to verify that IEEE Std 603-1991, Clause 5.5, and GDC 23 have been adequately addressed for the APR1400 safety-related systems. IEEE Std 603-1991, Clause 5.5 requires that the safety-related system accomplishes its safety functions under the full range of applicable conditions enumerated in the design basis. A special concern for digital computer-based systems is confirmation that system real-time performance is adequate to ensure completion of protective action within the critical points of time identified as required by IEEE Std 603-1991, Clause 4.10. GDC 23 requires that the protection system be designed to fail into a safe state or into a state demonstrated to be acceptable on some other defined basis if conditions such as disconnection of the system, loss of energy, or postulated adverse environments are experienced. SRP BTP 7-21, "Guidance on Digital Computer Real-Time Performance," provides supplemental guidance on evaluating response time for digital computer-based systems, and describes design constraints that allow greater confidence in the results analyses or prototype testing to determine real-time performance. Sections 7.9.4.1 and 7.3 of this SER provide additional discussion of the staff review of how the applicant addresses response time testing, as well as discussion of the applicant's response to RAIs associated with response time testing.

IEEE Std 7-4.3.2-2003 indicates that design for computer system integrity and design for test and calibration should be addressed as part of safety-related system integrity. Evaluation of computer system hardware integrity should be included in the evaluation against the requirements of IEEE Std 603-1991. Computer system software integrity (including the effects

of hardware-software interaction) should be demonstrated by the applicant's software safety analysis activities. SRP BTP 7-14, Sections B3.1.9 and B3.2.1, describe the acceptable characteristics of software safety plans and analyses.

Safety I&C System TeR, Appendix A, Section A.5.5, provides a description of how the safety-related I&C system meets the requirements of IEEE Std 603-1991, Clause 5.5. This section states that type testing of components, separation of sensors and channels, and qualification of cabling will be performed to ensure that the channels maintain functional capability. The applicant states that the PPS and ESF-CCS will meet the requirements of IEEE Std 7-4.3.2-2003 such that critical failures of hardware and software will be detected by the self-diagnostic capabilities of the system and outputs of the PPS and ESF-CCS go to fail-safe states.

The guidance of SRP Appendix 7.1-C, Section 5.5, “System Integrity,” states, in part, that a special concern for digital computer-based systems is confirmation that system real-time performance is adequate to ensure completion of protective action within the critical points of time. The Safety I&C System TeR, Section C.5.1.3.7, “DI&C-ISG-04 Staff Positions,” states that the NRC-approved Common Qualified Platform Topical Report, WCAP-16097-P-A, Revision 3 (ML13112A108), dated February 2013 (Common Q Platform Topical Report), central processing unit (CPU) maximum loading limit of 70 percent will be exceeded for the CPUs of the CPCS. The Safety I&C System-TR states that a 75 percent CPU load limit has been imposed on all CPCS processors to allow for the complex algorithms of CPCS. The staff concluded and noted in the Common Q Platform SER (ML13112A108) for Common Q Platform process design and implementation approval, that:

- If the single processor load is maintained at less than 70 percent and the processor does not malfunction, then control module overruns will be avoided and all tasks can be guaranteed to be fully accomplished.

- …[T]he predictability of program execution is established by determining whether the measured load of the application in a single processor is less than 70 percent, which will avoid control module overruns.

In RAI 43-7887, Question 07.01-25, the staff requested the applicant to:

1. Provide adequate design information and accompanying analysis to demonstrate predictable and repeatable operation of the CPCS CPUs when processor loading exceeds 70 percent. The description should include the basis for the CPU loading criteria, analysis, and/or outline of the analysis to be performed that demonstrates reliable performance for CPU loading once the software is completed.

2. Include an ITAAC item to include the necessary analysis and test to ensure predictable and repeatable operation of the CPCS system once software development has been completed and for support of future software maintenance.

On June 27, 2016, the applicant provided a supplemental response (ML16179A427) to RAI 43-7887, Question 07.01-25. **[**

]. The staff's review finds that these listed restrictions include a description of each restriction as well as a statement on the CPCS compliance to the restriction. The response of RAI 43-7887, Question 07.01-25, also stated **[**

].

The staff also concluded in the Common Q Platform SER (ML13112A108) for WCAP-16097 approval, that, "[F]or each Common Q application a timing analysis will be performed to ensure that the multiple control modules in the system design are executing deterministically. The licensee is required to review this analysis per PSAI [Plant-Specific Action Items] 6.6 of this SER."

The staff's Common Q Platform SER, PSAI 6.6, states that when implementing a Common Q safety-related system (i.e., CPCS), the licensee must review the timing analysis and validation tests for that Common Q system in order to verify that it satisfies its plant-specific requirements for accuracy and response time presented in the accident analysis in Chapter 15 of the safety analysis report. The applicant submitted the Common Q Platform Disposition TeR, Revision 0, with the APR1400 certification application, which provides a discussion on how the PSAIs will be addressed for the APR1400 design. Section 3.6, "PSAI 6.6," of the Common Q Platform Disposition TeR, states that the resolution to the staff's PSAI 6.6 is that the Common Q setpoint analysis and response time are covered by DCD Tier 1 Table 2.5.1-5, "Reactor Trip System and Engineered Safety Features Initiation ITAAC," design commitment Items 10 and 16, and Table 2.5.4-4, "Engineered Safety Features-Component Control System ITAAC," design commitment Item 21. However, upon the staff's review of the listed ITAAC, the staff did not find that the above listed ITAAC would confirm that the required CPCS configuration restrictions and required tests to ensure CPCS deterministic behavior above 70 percent CPU loading would be verified to have been implemented and performed. Therefore, Part 2 (listed above) of staff's request (i.e., 75 percent CPCS design confirmatory ITAAC) in RAI 43-7887, Question 07.01-25, has not been addressed. Therefore, RAI 43-7887, Question 07.01-25, was tracked as an open item. In the June 29, 2017, revised response to RAI 43-7887, Question 07.01-25 (ML17180A473), the applicant provided DCD Tier 1 Table 2.5.1-5, ITAAC Item 27 in a FSAR markup which would verify that the CPCS configuration restrictions and required tests to ensure CPCS deterministic behavior above 70 percent CPU loading have been implemented and performed in the as-built plant. The staff finds that the proposed DCD Tier 2 Table 2.5.1-5, ITAAC Item 27 markup satisfies the staff's request and conforms to the 10 CFR 52.47(b)(1)

ITAAC requirements. Thus, this part of RAI 43-7887, Question 07.01-25, has been satisfied and the incorporation of the DCD Tier 1 Table 2.5.1-5, ITAAC Item 27 markup into the next revision of the FSAR was confirmatory item. The staff verified the proposed markups to DCD Tier 1 Table 2.5.1-5, ITAAC Item 27 have been incorporated into Revision 2, of the FSAR. As such this confirmatory item has been satisfied. The staff also noted in the Common Q Platform SER (ML13112A108) that during operation of the Common Q application, [

].

The response of RAI 43-7887, Question 07.01-25, also provided FSAR mark-ups to incorporate by reference, the Common Q Supplemental TeR and Common Q Platform Disposition TeR, into the APR1400 design certification application. However, the applicant's June 29, 2017, response to this RAI did not provide adequate design information and accompanying analysis to demonstrate predictable and repeatable operation of the CPCS CPUs when processor loading exceeds 70 percent. Therefore, this portion of RAI 43-7887, Question 07.01-25, was an open item. The staff evaluation's evaluation documenting the resolution of the open item associated with RAI 43-7887, Question 07.01-25, is provided below as part of the evaluation for response time analysis.

Section C.5.1.3.7, "DI&C-ISG-04 Staff Positions," of the Safety I&C System TeR states [

]. The result of applying that penalty factor may or may not result in a plant trip. Based on the staff's review of the CPCS, the staff requested in RAI 274-8277, Question 07.01-37, for the applicant to clarify the following in order to determine if the requirements of GDC 23 have been met:

- During normal plant operation, explain how the predetermined CEA penalty factor value provides assurance that it will be a penalty factor value that is an accurate representation of the actual core CEA penalty factor.

- Discuss why, after sensing that both RPST1 and RSPT2 signals have failed, the safety-related system would not automatically place the affected channel(s) in trip. By not placing the affected channel in trip, the applicant should explain how the requirements of GDC 23 are being met.

- Discuss why, after sensing that both CEAC1 and CEAC2 are inoperable, the safety-related system would not automatically place the affected channel(s) in trip. By not placing the affected channel in trip, the applicant should explain how the requirements of GDC 23 are being met.

The staff requested the applicant to include this clarification in the FSAR or its referenced documents. In the December 29, 2015, response to RAI 274-8277, Question 07.01-37 (ML15363A340), the applicant discussed how penalty factors are calculated if RSPTs have failed. However, the staff was unable to verify this information based on documents reviewed at a CPCS audit as documented in the audit report (ML16061A027). As such, the staff closed RAI 274-8277, Question 07.01-37. The staff issued a follow-on question in RAI 328-8422, Question 04.04-8. The staff's review of the response to RAI 328-8422, Question 04.04-8, is documented in Section 4.4 of this SER.

SRP Section 7.1-C, Section 5.5 states that safety-related systems should be designed to fail in a safe state in the event of a loss of power, system disconnection, or other adverse environmental scenarios. Specifically, the RTS should fail into a tripped state and ESFAS functions should fail in a state that is predefined, based on the specific function. With regard to computer-based systems, the review should confirm that upon detection of inoperable components, place the protective functions in a tripped state (for example, resulting in a change in trip logic from 2 out of 4 to 2 out of 3). Self-diagnostics should detect hardware or software failures and place the system in a safe state. During system initialization or shutdown after loss of power, control output to actuators should fail to a predefined state. System restart should not cause actuators to transfer out of the predefined failure state.

Safety I&C System TeR, Section A.5.5 states that type testing of components, separation of sensors and channels, and qualification of the cabling are utilized to ensure that the channels maintain functional capability required under applicable extremes of environment, power supplied, malfunction, and DBE conditions. The applicant states:

> Loss of any one channel will not prevent the protective action of the PPS and ESF-CCS. Sensors are connected so that blockage or failure of any one connection does not prevent protective system action. The process transducers located in the containment building are specified and rated for the intended service. Components that must operate during or after a limiting fault (postulated accident) are qualified for the most limiting environment for the period of time for which they must maintain functional capability. Results of type tests are used to verify this. The system response time test is performed before and after installation to ensure to complete protective function within predefined time. The PPS and ESF-CCS meet the requirements of IEEE [Std 7-4.3.2-2003] for design considering computer system integrity, test and calibration.

Safety I&C System TeR, Section A.5.5 states that when a critical failure of hardware or software is detected by safety-related I&C platform, the PPS and ESF-CCS outputs will go to a fail-safe state and generate appropriate alarms. The PPS provides alarms to the QIAS-N and IPS to indicate system abnormalities. Section A.5.5 states that upon restart, the PPS will set all outputs to trip or initiation condition and the ESF-CCS to non-actuated condition. The initial conditions are maintained until the application program is executing properly. The test and maintenance equipment such as MTP/ITP is designed not to affect processor that is performing safety functions.

Safety I&C System TeR, Section B.5.5.1 states the safety-related I&C systems are designed for fail-safe operation under component failure or loss of electrical power. The safety-related I&C systems software integrity is assured by software development process and activities described in Section 5 of the SPM.

Safety I&C System TeR, Section B.5.5.3 states that upon power-up, diagnostics are performed including processors, input/output and memory to confirm readiness of the safety-related I&C systems. A complete set of these diagnostics are executed during initialization. This will detect any fatal errors prior to execution of the process loop. During initialization, the applicant states the watchdog function remains in the actuated state. Upon completion of the initialization tests, the processors will start automatically and run. Upon entry to the run mode, the watchdog function will automatically reset to the non-actuated state. Processor operability is continuously tested in the run mode and the watchdog function is actuated upon detection of failure.

Safety I&C System TeR, Section B.5.5.2 states:

> All processor stations have self-diagnostics that continuously monitor the hardware modules and software functions. This diagnostic information is sent to the ITP/MTP FPD for display and alarm processing. The IPS monitors the process values and setpoint values received from all channel ITPs. These features do not interfere with normal system operation. Channels are maintained and calibrated in a bypassed condition without initiating a protective action at the system level. Lifting electrical leads or installing jumpers need not be done to accomplish this process. Periodic testing is permitted during power operation.

DCD Tier 2, Tables 7.2-7 and 7.3-8 depict the FMEAs for the PPS and ESF-CCS and the compensating provisions for failures in those systems, including modification of trip logic. Automatic trip logic modification is also applicable to channel bypasses, as committed to by the applicant in Section 7.2.1.6 of DCD Tier 2. This includes bypasses initiated manually. DCD Tier 1 Table 2.5.1-5 provides ITAAC items to verify automatic trip logic modification due to bypassed instrument channels (e.g., 2 out of 4 control logic modifies to 2 out of 3 control logic).

Regarding system restart, the applicant states in Section A.5.5 of the Safety I&C System TeR that all PPS outputs are set to the trip or initiation condition and the ESF-CCS to a non-actuated state. The section also states that initial conditions are maintained until the application program is executing properly. DCD Tier 1 Table 2.5.1-5 also provides ITAAC that verify fail safe operation of the PPS upon a loss of power and does not result in equipment actuation. The staff finds that because the PPS outputs to trip and ESF-CCS to non-actuated state, the design meets the requirements of IEEE Std 603-1991, Clause 5.5 with respect failing to a safe-state upon conditions that would trigger a restart of the system.

Response Time Analysis

The Response Time Analysis TeR, provides for the response time philosophy and analysis for the FSAR. Specifically, Appendix A of this report described specific compliance to SRP BTP 7-21. SRP BTP 7-21, states, in part, that if certain criteria are met, the staff may conclude that the design or completed system will meet timing requirements which can be verified or that that prototype system correctly reflects the expected performance of the actual plant design fully implemented. The acceptance criteria are outlined below:

To address the guidance on limiting response times in SRP BTP 7-21, the Response Time Analysis TeR, Appendix A states, in part, that the analytical limits in the Setpoint Methodology for Safety-Related Instrumentation, and the response times in DCD Tier 2, Tables 7.2-5 and 7.3-7 are credited in the safety analysis of DCD Tier 2 Chapter 15. This appendix states that if the results of the safety analysis are acceptable, then such an outcome will confirm that these items are acceptable as well. The Response Time Analysis TeR also states that the allocated response times of the safety-related I&C system are determined to meet the response time requirements shown in Tier 2, Tables 7.2-5 and 7.3-7 of the FSAR. The allocated response times are based on the specification of individual equipment that are used in the as-built APR1400. Section 5 of Response Time Analysis TeR describes the signal path of various components that comprise the individual reactor trip and ESFAS functions. The response time allocated to each component and its basis are described in Sections 6 and 7 of the Response Time Analysis TeR. The performance requirements for the reactor trip and ESFAS functions flow from the requirements of the safety analysis. If the analytical limit and responses times are confirmed by the positive results of the safety analysis, this would demonstrate that they are

consistent with system timing and safety requirements. Therefore, the staff finds the applicant has demonstrated that the guidance for limiting response times in SRP BTP 7-21 has been adequately addressed.

For the guidance on digital computer timing requirements in SRP BTP 7-21, the Response Time Analysis TeR, Appendix A states, "Components covered by the limiting response time are typically composed of sensor, signal processing device, digital computer system, and final actuator. The sum of allocated response times does not exceed the limiting response time. The allocated response times are described in Section 6. The response time of the digital systems including the Plant [PPS], [CPCS], and [ESF-CCS] are specifically analyzed in Section 7 to ensure that each allocated response time covers the worst case response times of computer hardware, software, and communication equipment. Software requirements specifications will address the computer system timing requirements in detail."

In Section 7 of the Response Time Analysis TeR, the applicant presents a calculation of the worst case time delay for each component in the trip signal path for a given function. This worst case time is then compared to the allocated response time to ensure that this time is not exceeded. This demonstrates that specific digital timing allocations to specific components of RTS/ESFAS are consistent with the limiting response times, as described in Section 5 and Section 6 of this TeR and conforms to the guidance for digital computer timing requirements in SRP BTP 7-21.

To address the guidance on architecture in SRP BTP 7-21, the Safety I&C System TeR describes the architecture of the safety-related I&C systems. Additional details on the architecture of the overall I&C architecture is provided in DCD Tier 2 Chapter 7. DCD Tier 1 Section 2.5 and the Response Time Analysis TeR account for the time delays allotted to each portion of the reactor trip/ESFAS trip path, down to the individual unit level and these values are considered representative values until detailed design, implementation, and actual equipment are procured to adjust for actual equipment delay times.

In Section A.3.2 of the Response Time Analysis TeR, the applicant commits that the response time delays of all components in the safety-related I&C system have deterministic characteristics. This sections states, "The digital computer systems including the PPS, CPCS, and ESF-CCS are designed so that databases, disk drives, printers, or other equipment or architectural elements subject to halting or failure do not prevent the protective system action. When the critical failure of hardware or software detectable by diagnostic function occurs, the outputs of the digital safety-related I&C system fail to trip for PPS and fail as-is for ESF-CCS and generate alarms." The staff finds that the applicant has adequately identified for and provided design description of the overall I&C architecture and provided design information on required time allocations. The staff finds the applicant's commitment that failures of supporting portions of systems (e.g., databases, disk drives, etc.) do not affect the ability of the safety-related systems to provide their design function is acceptable. Therefore, the staff finds that the applicant has adequately addressed the guidance on architecture in SRP BTP 7-21.

Regarding performance verification guidance in SRP BTP 7-21, the applicant states, in part, that the safety-related I&C systems are designed and verified through the software lifecycle design process, in particular the software verification and validation activities. These activities have requirements for independent verification and validation performance as specified in Sections B.5.3.3 and B.5.3.4 of the Safety I&C System TeR. These referenced sections state conformance to IEEE Std 1012-2004, as endorsed by RG 1.168, Revision 2. Section 3.2.4 of

the Response Time Analysis TeR states the following with regard to the timing analysis assumptions:

> In order to ensure 75% maximum [CPU] load, configuration restrictions and tests required by Reference 5 [(Common Q Supplemental TeR)] will be incorporated into the CPCS design. The PPS and ESF-CCS will be designed not to exceed 70% of CPU full load.

In Section 7 of the Response Time Analysis TeR, the above assumptions are represented by two separate multipliers: 1.75 for CPCS functionality and 1.70 for all other functionality. This represents a specific design commitment by the applicant to ensure that individual portions of the safety-related I&C systems meet the timing requirements. The applicant did not have an ITAAC item that verifies the CPCS configurations restrictions and tests required by Reference 5 have been incorporated into the final design. If these design restrictions for the CPCS are not verified, the staff finds that the timing analysis calculations for the CPCS cannot be verified in the as-built CPCS since the multipliers used in the timing calculations would potentially be inaccurate. Therefore, as stated above, RAI 43-7887 Question 07.01-25, tracked this issue regarding verification that the CPCS restrictions have been implemented in the as-built CPCS system as an open item. In the September 15, 2017, revised, proprietary, supplemental (Revision 2) response for RAI 43-7887 Question 07.01-25 (ML17258A695), the applicant documented and provided the results of the tests that demonstrate that the CPCS's CPUs, when implemented with the required configuration restrictions as listed in Section 2 of the Common Q Supplemental TeR, does not experience a CPU overload condition. These test results confirm that once the CPCS has been implemented with the required configuration restrictions, that the CPCS CPU load limit can be increased greater than the approved Common Q Platform Topical Report 70 percent CPU load limit and still operate in a deterministic manner and that the CPCS CPU load will not exceed 75 percent. In addition, the applicant has provided an ITAAC markup in the response that verifies the CPCS configurations restrictions and tests have been implemented and performed. Therefore, the ITAAC markup and the test results satisfy this part of the staff's RAI 43-7887 Question 07.01-25, request. Therefore, the open item associated with this portion of RAI 43-7887 Question 07.01-25, is considered closed. The incorporation of the RAI 43-7887 Question 07.01-25, response ITAAC markup into the next revision of the FSAR was a confirmatory item. The staff verified the proposed markups have been incorporated into the FSAR, Revision 2. As such this confirmatory item has been satisfied. However, the staff finds that due to the applicant taking a deviation from the approved Common Q Platform Topical Report for the CPCS CPUs by increasing the CPU maximum load limit from 70 percent to 75 percent, and requiring that the CPCS be designed and developed with sixteen (16) additional programming configuration restrictions and several additional tests to assure deterministic operations (i.e., ensure all safety function tasks are performed within the required response time) above the 70 percent CPU load limit, the staff finds that the additional sixteen configuration restrictions, as listed in Section 2 of the Common Q Supplemental TeR, are safety significant. SRP Section 14.3.5, "Instrumentation and Controls - Inspections, Tests, Analyses, And Acceptance Criteria," Section II, "Acceptance Criteria," Item 2 states that:

> Tier 1 Design Descriptions ... and ITAAC Design Descriptions ... should describe the top-level I&C design features and performance characteristics that are significant to safety. For safety-related systems, this should include a description of system purpose, safety functions, equipment quality … equipment qualification … and design features ... provided to achieve high functional reliability.

Therefore, the staff issued RAI 554-9146, Question 07.02-18, requesting the applicant to either:

- Include the 16 configuration restrictions in Section 2.5.1, "Reactor Trip System and Engineered Safety Features Initiation," Tier 1, of the FSAR or,

- Incorporate by reference, the proprietary Common Q Supplemental TeR, and identify it as a "Tier 1" document.

Pending the resolution of this request, RAI 554-9146, Question 07.02-18, was tracked as an open item. The applicant submitted a response to RAI 554-9146, Question 07.02-18, on November 27, 2017 (ML17331A231). In the response, [

]. As such, the open item associated with RAI 554-9146, Question 07.02-18 is closed and resolved. The incorporation of the proposed Tier 1 markups into the next revision of the FSAR was a confirmatory item. The staff verified the proposed markups have been incorporated into the DCD, Tier 1, Revision 2. As such, this confirmatory item has been satisfied.

The applicant provided a supplemental response to RAI 554-9146, Question 07.02-18, on May 17, 2018 (ML18142A303) to correct the reference to Item 28 in ITAAC Table 2.5.1-5. The applicant modified this ITAAC to correctly reference Item 28 in Section 2.5.1.1, DCD Tier 1 and specify that the inspection will be performed on the "as-built" CPCS. The staff finds this correction is acceptable. The incorporation of the proposed markups in Section 2.5.1.1 and Table 2.5.1-5 of the DCD Tier 1, Revision 3, was a confirmatory item. The staff verified the proposed markups have been incorporated into Section 2.5.1.1 and Table 2.5.1-5 of DCD Tier 1, Revision 3. As such this confirmatory item has been resolved.

The applicant states, in part, that the safety-related I&C system uses the Common Q platform which includes a real-time operating system, task scheduler, diagnostic functions, communication interfaces, and user application programs. The software to implement these functions reside on flash PROM in the PM646A processor module. The details are described in Section 5.2.1.2 of Common Q Platform Topical Report, Revision 3. The Common Q platform adopts a watchdog timer that is described in Section 4.1.5 of the SER for the Common Qualified Platform Topical Report, Revision 3, and Sections 5.2.1.2 and 5.2.1.3 of the Common Qualified Platform Topical Report, Revision 3. The Safety I&C System TeR, Section 4.0, describes the design and implementation of WDTs for the PPS, ESF-CCS and CPCS specifically for the APR1400 design

The safety-related I&C system design is based on the Common Q platform. As stated in Section 10.2.1.3, Item 3.j, of the Common Q Platform Topical Report, the Common Q platform allocates a response time budget to the overall system architecture so that the system is to be

designed to meet this response time allocation. Based upon this description, the response time required for the application module, the support module, and the self-diagnostic module would not exceed the allotted time given in the architecture timing allocation. This information is supported by the response timing analysis as provided in this the Response Time Analysis TeR, which describes the time allocations for each portion of the PPS, CPCS and ESF-CCS. WDTs are considered to be part of the overall self-testing/self-diagnostic functionality of the Common Q platform. The platform itself is commercial grade dedicated and in the April 5, 2016 response to RAI 356-7881, Question 07-1 (ML16096A181), the applicant stated that ITAAC Item 24 in DCD Tier 1, Sections 2.5.1, 2.5.3, and 2.5.4, and Tables 2.5.1-5, 2.5.3-3, and 2.5.4-4, will be added to verify safety grade protection systems are installed in accordance with the dedication process of commercial grade hardware and software. These ITAAC will provide verification of WDT functionality as part of the base hardware of the APR1400 design. Based on the addition of these ITAAC, the staff finds the as-built APR1400 systems that use the Common Q platform will be verified to meet the commercial grade dedication process. The design and implementation of the WDT is evaluated below.

To address guidance on use of part-scale prototypes in SRP BTP 7–21, in Section A.7.2 of the Response Time Analysis TeR, the applicant states, in part, that the safety-related I&C systems using the Common Q platform for Shin-Kori nuclear plant Units 3 and 4 have been implemented and tested full-scale during commissioning testing before they went into commercial operation. Shin-Kori Units 3 and 4 were implemented with the generic APR1400 platform, the platform which is the subject of this design certification review. APR1400 will necessarily undergo some changes as a result of the NRC's review process. With that in mind, it is still reasonable to conclude that Shin-Kori Units 3 and 4 represent full scale prototypical (prototype and fully operational) implementations of the APR-1400 design. The I&C platform used in the APR1400 has been implemented and tested on operating power plants, thus demonstrating the adequacy of the generic design described in the APR1400 design certification application. Although the Shin-Kori Units 3 and 4 are full scale implementation using the same I&C platform as the APR1400 design certification, the staff finds this information is adequate to address the intent of the guidance for use of part-scale prototypes for SRP BTP 7-21 because it provides a more accurate representation of the design for the purpose of response timing analysis.

Based upon a review of design commitments made within licensing documents (as described above), the staff finds the APR1400 design adequately conforms to the guidance of SRP BTP 7-21.

Watchdog Timer Implementation

The SRP Appendix 7.1-D, Section 5.7 states, in part, that a non-software WDT is critical in the overall diagnostic scheme of a computer system. A software-based WDT can fail to operate if the processor freezes and no instructions are processed. To ensure system integrity, the only software input is reset after the safety processor completes its function. It is NRC policy that devices that are implemented using software tools would also be considered software, and would be subject to the same failure modes as the operating system it was intended to monitor.

Section 4.2.2 of the Safety I&C System TeR, states the following, "Each PPS LCL reactor trip processor is supervised by the PLC watchdog timer." According to the Safety I&C System TeR, "PLC" stands for programmable logic controller. This would imply that, for the LCLs, the WDTs are implemented with programmable technology and it was not clear whether other WDTs are also implemented using a PLC based upon the applicant's description. This implementation would not conform to the guidance on WDT in SRP Appendix 7.1-D and IEEE Std 7-4.3.2-2003,

which the applicant states the APR1400 design complies with. Section 4.2.2 of the Safety I&C System TeR also states, in part, the watchdog timer outputs are hardwired to a separate PLC rack to ensure appropriate trip signals are generated for the reactor trip function. There does not appear to be a figure in the safety-related I&C system report that shows this configuration. A figure that showed this configuration may demonstrate that the functionality of the WDT, the initiation of reactor trip or safe state for ESFAS components, is not dependent on software or software-based components to perform its safety function. In RAI 356-7881, Question 07-14, the staff requested the applicant to clarify the WDT design and implementation for the APR1400 design. In addition, in RAI 356-7881, Question 07-01, the staff requested the applicant to provide an ITAAC item to verify the fail-safe operation of the safety-related I&C system, specifically for a loss of power condition, to verify design claims made regarding this topic and ensure that system integrity is maintained.

In the September 27, 2016, response to RAI 356-7881 Question 07-14 (ML16271A349), the applicant stated that with respect to the PPS, the trip path of the WDT that initiates a fail-safe condition does not include any software dependent portion of PPS nor any other type of programmable technology. The applicant committed to revising Figure 4-7, "Watchdog Timer for PPS," and Figure 4-16, "Watchdog Timer for ESF-CCS" of the Technical Report , revision 0, "Safety I&C System," to clarify the design layout, trip path and output interface of the WDTs. The WDT interface is provided by an output relay, which is a hardwired component located on the processor module. It is the output relay on the processor module that either annunciates failures or sets outputs to a pre-defined fail-safe condition. The revised figures consolidate design information in various licensing documents regarding WDT functionality. The applicant also committed to revising Section 4.2.2.1 of the Safety I&C technical report to add design detail on the interface between the WDT and the reactor trip initiation circuity. The applicant also clarified in its response that the WDT timers were hardware components and are identical in all applications they are implemented within the APR1400 design. Specifically, the applicant states, in part, that each WDT is strictly hardware and does not employ programmable technology such as FPGAs.

The staff reviewed the proposed revisions by the applicant and found the proposed revisions acceptable. The applicant states in the proposed revision to Section 4.2.2.1 of the Safety I&C technical report the following: "If the WDT contained in the LCL reactor trip processor module fails to be reset in the predefined time, the WDT will block the power going through the interposing relay. This will result in opening the interposing relay of the undervoltage trip device in the reactor trip initiation circuit." This design description aligns with the information provided on the revised version of Figure 4-7 of the Safety I&C Technical Report. The revised Figure 4-7 depicts enhancements such as the 'CPU' input into the WDT mechanism of the LCL processor module, signifying the resetting function of processor module in order to prevent the WDT from disabling the reactor trip undervoltage relay, which demonstrates proper processor module operation for the LCLs. The revised Figure 4-7 also has a new note number 4 which is a pointer to the Common Q Platform Topical Report section describing WDT functionality. The revisions to the figure, combined with the added note and additional design description adequately consolidate design information in the APR1400 design regarding WDT implementation. Based upon the adequacy of proposed revisions, as well as the clarifications provided, the staff finds the applicant's response to RAI 356-7881, Question 07-14, is acceptable. The incorporation of the proposed markup into the next revision of the Safety I&C System TeR was a confirmatory item. The staff verified that the proposed markups have been incorporated into Revision 1 of the Safety I&C System TeR. As such, this confirmatory item has been satisfied. However, new Common Q Platform WDT design information was submitted to the NRC via a Westinghouse Nuclear Safety Advisory Letter (NSAL)-17-2, dated July 5, 2017 (ML17213A208). The

NSAL-17-2 information states the following, for the NRC-approved Common Qualified Platform Topical Report, Revision 3.

- The software stall timer was never activated in the AC160 base software, as designed;
- The inactivated software stall timer also disabled the hardware stall timer.

Thus, both Common Q platform stall timers are not operational, as designed and approved, and do not perform diagnostic functions as approved in WCAP-16097-P-A. This issue affects both variants of ABB processor modules, PM646A and PM646B. The effect of these non-activated stall timers, as stated in the NSAL-17-2, are:

- The processor module does not automatically halt the application and restart the processor module to the error state due to a severe software fault;
- The processor module instead responds to a severe software fault by continuing to display the normal operating 'P1' state instead of the diagnostic code '09' on the processor module seven-segment display.

Therefore, due to the new and conflicting design information presented in NSAL-17-2 and the docketed APR1400 design certification application information, the staff issued RAI 555-9163, Question 07.02-19, requesting the applicant to review the applicable safety Common Q platform based systems design descriptions of the APR1400 design certification application (DCA) and demonstrate that the APR1400 DCA is not affected by the design information contained within NSAL-17-2. Specifically, the staff requested the applicant to:

1) Review information presented in NSAL-17-2 against information presented in the FSAR and referenced technical reports design descriptions to determine if the information present in NSAL-17-2 affects the APR1400 DCA;

2) Review and clarify whether the specified WDTs referenced in the DCD Tier 2 and the Safety I&C System TeR, Revision 1, are the window WDTs referenced in the Common Qualified Platform Topical Report, Revision 3, and make appropriate modifications in DCD Tier 2 and its referenced technical reports to reflect this clarification;

3) Verify that the window WDTs are hardware-based (i.e., does not contain software and do not rely upon software for activation), as specified in the DCA and Common Q Platform Topical Report, Revision 3, and include the definition for the term "hardware" provided in the response to RAI 356-7881, Question 07-14, into the DCD Tier 2 or the Safety I&C System TeR; and

4) Expand the design descriptions in DCD Tier 1, Sections 2.5.1.1, Item 13 and 2.5.4.1, Item 10 and corresponding Inspections, Tests, Analyses and Acceptance Criteria in Tier 1, Tables 2.5.1-5, Item 13 and 2.5.4-5, Item 10, respectively, to verify that the WDTs used to generate trip and fail-safe conditions for reactor trip and ESFAS functions, respectively, are hardware based.

Pending the resolution of this request, RAI 555-9163, Question 07.02-19, was tracked as an open item. The applicant submitted a response to RAI 555-9163, Question 07.02-19, on November 27, 2017 (ML17331A399). The applicant's response clarified that:

- The APR1400 safety functions of the safety-related systems do not utilize the stall timer addressed in NSAL-17-2, that the Common Q platform based systems design descriptions of the APR1400 DCA are not affected or conflicted by the design information contained within NSAL-17-2, and that there is no impact to the APR1400 safety function or operability;

- The WDT related design information contained in DCD Tier 2, and the Safety I&C System TeR are all "window WDT" as listed in the Common Q Platform Topical Report, Revision 3; and

- Each window WDT is strictly a hardware device (e.g., does not employ a programmable hardware device like an FPGA or contain software) and that each window WDT does not rely upon software for activation.

The applicant's response also provided markups to show the expanded and additional design descriptions to be added to DCD Tier 1 Section 2.5.1.1 design descriptions and its corresponding ITAAC Table 2.5.1-5, Item 13, as well as Tier 1, Section 2.5.4.1 design descriptions and its corresponding ITAAC Table 2.5.4-5, Item 10. The response also included revised design description markups to include the WDT clarifications for DCD Tier 2 Table 7.2-7, as well as revisions to design descriptions and figures contained in the Safety I&C System TeR. The staff finds that the RAI 555-9163, Question 07.02-19 response's markups and revisions listed above satisfy the staff's request to provide clarity in the APR1400 application's references to WDT safety functions, implementation, design, and operation, as it relates to the technical information provided in NSAL-17-2. It should be noted that before the applicant officially submitted a RAI 555-9163, Question 07.02-19 response, NSAL-17-2 was updated to a November 9, 2017, Revision 1 document (ML17313B194). This November 9, 2017, NSAL-17-2, Revision 1 update provided clarification to the July 5, 2017, NSAL-17-2 information, with the most notable updates being that:

- The hardware stall timer is not inactive as previously stated;

- The hardware stall timer remains fully functional.

The staff's review of the Revision 1 updates to the information contained in NSAL-17-2 found that the updates did not alter or have any impact to the safety conclusions and resultant safety functionality that remains, due to the discovery that the software stall timer was never activated (i.e., non-functional component), as documented in NSAL-17-2. Thus, the staff finds that the response to RAI 555-9163, Question 07.02-19, is still applicable and a supplemental response for the NSAL-17-2 Revision 1 updates is not necessary. As such, the open item associated with RAI 555-9163, Question 07.02-19, is closed and resolved. The incorporation of the proposed markups into the next revision of the DCD and the Safety I&C System TeRwas a confirmatory item. The staff verified the incorporation of these changes in Revision 2 to the Safety I&C System TeR and Revision 2 to the DCD. As such, this confirmatory item has been satisfied.

The applicant submitted two supplemental responses (ML18102B220 and ML18124A146) to RAI 555-9163, Question 07.02-19. The first supplemental response removed the statement regarding not activating the software stall timer in order to be consistent with the licensing basis. The second supplemental response modified design description in DCD Tier 1 Section 2.5.1.1, Item 13 and the ITAAC in Table 2.5.1-5, Item 13 to separate design descriptions for the RT logic from those for the ESFAS logic. In addition, the ITA for Table 2.5.1-5, Item 13 was clarified to indicate that two separate tests will be performed, one for simulating a lock up of the processor,

the other to disconnect the electrical power. Similar changes were made to the ESF-CCS design descriptions and corresponding ITAAC in Tier 1 Section 2.5.4.1, Item 10 and Table 2.5.4-5, Item 10, respectively. The staff finds the added clarifications to the RAI response and to the Tier 1 design descriptions and corresponding ITAAC are acceptable because these changes ensure consistency within the licensing documents and provide clarity for verifying the as-built design to the design commitments. The staff finds ITAAC in DCD, Tier 1 Table 2.5.1-5, Item 13 and Table 2.5.4-5, Item 10 meet the requirements of 10 CFR 52.47(b)(1). The incorporation of the proposed of changes to (1) DCD Tier 1, Section 2.5.1.1, Item 13, and the corresponding ITAAC in DCD Tier 1, Table 2.5.1-5, Item 13 and (2) to DCD Tier 1, Section 2.5.4.1, Item 10, and the corresponding ITAAC in DCD Tier 1, Table 2.5.4-5, Item 10 was a confirmatory item. The staff verified these markups have been incorporated into DCD Tier 1, Revision 3, Section 2.5.1.1, Item 13, Table 2.5.1-5, Item 13, Section 2.5.4.1, Item 10, and Table 2.5.4-5, Item 10. As such, this confirmatory item has been satisfied.

The applicant's response to RAI 356-7881 Question 07-01, is addressed in 7.1.4.11, "Capability for Test and Calibration," of this safety evaluation.

In RAI 356-7881, Question 07-03, the staff requested the applicant to describe the diagnostic programs used to test digital computer channels in the APR1400 design, including how the design ensures that online testing does not result in an unplanned component or spurious actuation of a component(s) while testing. In the September 29, 2016, response to RAI 356-7881, Question 07-03 (ML16273A581), the applicant clarified design attributes to address the staff's concerns with the potential with unintended equipment actuations as a result of single or multi-channel testing. The applicant refers to DCD Tier 2 Section 7.2.2.5, which states, in part, that the test equipment (MTP, ITP, and associated interface circuits are divisionalized and simulated test signals injected into a division will only affect the division under test. The SDN is used to communicate test injection and monitoring points (i.e., test feedback). As per Section 4.6.2 of the Safety System I&C TeR, the SDN is contained within a division and does not cross safety division boundaries as the design of the SDN does not provide for cross-divisional communication. The applicant also stated that there are multiple secured steps and operator would need to perform to initiate testing that provide additional barriers to this potential hazard. The staff finds the applicant's responses to RAI 356-7881, Question 07-03, acceptable. The use of dedicated MTPs for each division of PPS logic, in conjunction with independence requirements (no cross-divisional communications) between divisions being met ensure that there will not be unintended equipment movement in non-tested divisions while performing maintenance in a single division with manually initiation of test signals or the potential of a fault caused by maintenance to affect any non-tested divisions. This RAI question is therefore considered closed and resolved.

Based on the provision of design features to ensure deterministic operations (e.g., WDTs, CPU load limits, design configurations), and the resolution of the open items associated with RAI 554-9146, Question 07.02-18 and RAI 555-9163, Question 07.02-19, the staff finds the APR1400 design meets the system integrity requirements of IEEE Std 603-1991, Clause 5.5. The full review of automated self-testing features is in Section 7.1.4.11 of this SER. Conformance of the APR1400 design to SRP BTP 7-14 is addressed in Section 7.1.4.7 of this SER.

7.1.4.10 Independence

The staff reviewed the APR1400 design certification application to verify that the requirements of IEEE Std 603-1991, Clause 5.6, GDC 21, GDC 22, and GDC 24 have been adequately

addressed for the APR1400 safety-related systems. GDC 21 requires redundancy and independence designed into the protection system to be sufficient to ensure no single failure results in a loss of the protection function and removal from service of any component or channel does not result in loss of the required minimum redundancy. GDC 22 requires the protection system be designed to assure the effects of natural phenomena, and of normal operating, maintenance, testing, and postulated accident conditions on redundant channels do not result in loss of the protection function. 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 removal from service of any protection system component or channel common to control and protection systems leaves intact a system satisfying all reliability, redundancy, and independence requirements of the protection system. IEEE Std 603-1991, Clause 5.6 requires independence between (1) redundant portions of a safety-related system, (2) safety-related systems and effects of DBE, and (3) safety-related systems and other systems. SRP Appendix 7.1-C, provides acceptance criteria for the requirements of IEEE Std 603-1991. SRP Appendix 7.1-C, Section 5.6 states that three aspects of independence should be addressed, including physical independence, electrical independence, and communications independence. The staff also identified functional independence as an additional aspect that should be addressed. RG 1.75, "Criteria for Independence of Electrical Safety Systems," Revision 3, describes a method acceptable to the staff for complying with NRC regulations with respect to the physical independence requirements of the circuits and electrical equipment that comprise or are associated with safety-related systems. RG 1.75, Revision 3, endorses IEEE Std 384-1992, "Standard Criteria for Independence of Class 1E Equipment and Circuits," as an acceptable method for satisfying the regulatory requirement concerning physical independence of circuits and electrical equipment that comprise safety-related systems. SRP BTP 7-11, "Guidance on Application and Qualification of Isolation Devices," provides guidance on application and qualification of isolation devices used to ensure electrical independence for safety-related systems. In addition, DI&C-ISG-04, Revision 1, provides design criteria for communication and functional independence between redundant divisions of safety-related systems.

7.1.4.10.1 Independence Between Redundant Portions of the Safety System

IEEE Std 603-1991, Clause 5.6.1, requires redundant portions of the safety-related system to be independent and physically separated from each other to the degree necessary to retain the capability to accomplish the safety function. As stated above, RG 1.75, Revision 3, provides guidance on acceptable means to meet physical independence requirements.

Section 3.4.6 of the Safety I&C System TeR states conformance to IEEE Std 384-1992 for APR1400 I&C systems, which is endorsed by RG 1.75, Revision 3. The technical report states the PPS and ESC-CCS are divided into four divisions which are physically separated and provide electrical independence. Section 3.4.6 of this technical report further states:

> the independence and separation of redundant Class 1E circuits within and between the PPS divisions or ESF-CCS divisions are accomplished through the use of fiber optic technology and barriers or conduits…the optical technology ensures that no single credible electrical fault in the PPS or ESF-CCS division can prevent the circuity in any other redundant divisions from performing its safety function.

Section A5.6 of the Safety I&C System TeR discusses compliance to Clause 5.6.1 of IEEE Std 603-1991, and states:

> …cabling for the four safety divisions are routed separately…safety divisions do not share power to preserve electrical separation and isolation…the LCL in the PPS receives the signals from redundant channel and the [group controller] in the ESF-CCS receives signals from each division through fiber optic modem.

The staff finds the safety-related I&C system design meets the physical and electrical independence requirements of IEEE Std 603-1991, Clause 5.6.1 because the safety-related system conforms to RG 1.75, Revision 3. APR1400 design precludes the use of components that are common to redundant portions of the safety-related system, ARP1400 safety-related systems have adequate physical separation and physical barriers, and ARP1400 safety-related systems utilize separate power sources.

DCD Tier 1, ITAAC Table 2.5.1-5, Items 3.a and 3.b provide a means to verify that the I&C system designs are implemented to meet the independence requirement of Clause 5.6.1 of IEEE Std 603-1991. The evaluation of these ITAAC are documented in Section 14.3.5 of this SER.

7.1.4.10.2 Communication and Functional Independence

The evaluation of communication and functional independence requirements to meet the requirements of GDC 21, GDC 22, GDC 24 and IEEE Std 603-1991, Clause 5.6.1, is provided in Section 7.9.4.6 of this SER.

7.1.4.10.3 Independence between Safety Systems and Effects of Design Basis Event

IEEE Std 603-1991, Clause 5.6.2, states that safety-related system equipment required to mitigate the consequences of a specific DBE must be independent of, and physically separated from, the effects of the DBE to the degree necessary to retain the capability to meet the requirements of this standard. This clause specifies that equipment qualification in accordance with IEEE Std 603-1991, Clause 5.4, is one method that can be used to meet this requirement. In addition, 10 CFR Part 50, Appendix A, GDC 22, requires the protection system to be designed to assure that the effects of natural phenomena, and of normal operating, maintenance, testing, and postulated accident conditions on redundant channels do not result in loss of the protection function.

To meet the requirements of IEEE Std 603-1991, Clause 5.6.2, safety-related systems shall meet the equipment qualification requirements of IEEE Std 603-1991, Clause 5.4, and, accordingly, provide sufficient diversity to prevent the loss of the safety functions.

Section A.5.6 of the Safety I&C System TeR states, “independence of the components in the safety-related I&C system to the effects of a DBE is provided by qualifying the equipment in accordance with the requirements in Section 6 [Equipment Qualification] of this [technical] report.”

The staff’s evaluation of Equipment Qualification is in Section 7.1.4.8 of this safety evaluation.

7.1.4.10.4 Independence between Safety and Non-Safety Systems

IEEE Std 603-1991, Clause 5.6.3, requires safety-related system design to be such that credible failures in and consequential actions by other systems shall not prevent the safety-related systems from meeting the requirements of this standard. This clause consists of the following considerations:

- Interconnected Equipment.
- Equipment in Proximity.
- Effects of a Single Random Failure.

Section 4.2.4 of the Safety I&C System TeR discusses PPS cabinet interfaces. The applicant provided descriptions for some of the system interfaces and types (e.g., APC-S connects to PPS cabinets via hardwire cables, the CPCS connects to PPS cabinets via hardwire cables, and PPS sends initiation signals to ESF-CCS group controllers through fiber optic SDL). It was not clear to the staff how other safety-related systems and non-safety systems are connected. The staff issued RAI 45-7883, Question 07.09-2, to request the applicant list all safety-related to safety-related system interfaces and interface types, and to list all safety-related to non-safety system interfaces and interface types, and provide information on how these interfaces meet the requirements of IEEE Std 603-1991, Clause 5.6, or provide a reference to sections of the FSAR or technical reports where this information resides. In the November 3, 2015, response to RAI 45-7883, Question 07.09-2 (ML15307A679), the applicant committed to clarifying the system interfaces and connection types in the FSAR. However, the staff needed additional clarification and requested a supplemental the response to incorporate the list of all non-safety signals to the ESF-CCS into the Safety I&C System TeR and CCF TeR, and to include a functional diagram of Type 1 signal control (non-safety signal which acts in same direction as ESFAS) in the FSAR. In addition, the staff requested the applicant to also include in the supplemental response a description of how the I&C system interfaces with external networks (e.g., IPS interface to emergency offsite facilities as depicted in DCD Tier 2, Figure 7.7-12). Specifically, the staff requested the applicant to identify the interface, the purpose of the interface, the direction of the data flow, and how the data flow is enforced (e.g., software-based/configurable). Pending the resolution of this issue, RAI 45-7883, Question 07.09-2, was tracked as an open item.

In the August 21, 2017, supplemental response to RAI 45-7883, Question 07.09-2 (ML17233A372), the applicant provided a description of all interfaces between safety-related and non-safety systems, including the interface type. The applicant committed to include this description in the Safety I&C System TeR. In addition, the applicant stated that Section 4.4.4.12 of the Safety I&C System will be revised to include additional clarification that the non-safety signals cannot block the operation of the ESF-actuation signals and will reference Section 7.3.1.9 of the DCD Tier 2. To address external interfaces, the applicant provided a modified Figure 4-1 which depicts the interfaces between the I&C systems to external networks (i.e., emergency operation facility (EOF), nuclear emergency response center, and NRC operations center). The applicant also added a description of these interfaces in Section 4.6.2.7 and described how the interface is uni-directional between the I&C systems and external networks. [

]. In response to RAI 323-8281, Question 07.03-20 (ML16124B195), the applicant already modified the functional diagram (Figure 4-17) in the Safety I&C System TeR for ESF-1 and ESF-2 (Type 1 and Type 2) commands and provided Table 4-4 to identify components with each type of signal. Because the applicant provided additional information to (1) identify all interface between safety and non-safety-related I&C systems and (2) demonstrated how I&C system interfaces to external networks are uni-directional, the staff finds the applicant has addressed the guidance of DI&C-ISG-04, Revision 1, and thus meets the requirements for IEEE Std 603-1991, Clause 5.6. As such, the open item associated with RAI 45-7883, Question 07.09-2, is closed and resolved. The incorporation of the proposed markups into the next revision of the Safety I&C System TeR was a confirmatory item. The staff verified the proposed the incorporation of the proposed marksups in Revision 2 of the Safety I&C System TeR. As such, this confirmatory item has been resolved.

The applicant submitted a supplemental response to RAI 45-7883 for the Question 07.09-2 (ML18124A110), in response to ACRS recommendations stated in the ACRS's interim letter (ML17265A792) regarding the SER with open items associated with Chapter 7 and 18 of the APR1400 design certification application. In this response, the applicant provided additional detail regarding the interface between the I&C systems and external interfaces. The response describes how the one way data diode is implemented to ensure that the data flow cannot be changed via software or software configuration. The response also included proposed markups to Section 4.6.2.7 and Figure 4-1 of the Safety I&C System TeR include the description of this interface. The proposed markups also include a new figure (Figure 4-25) in the Safety I&C System TeR that illustrates the one-way interface from the I&C System DCN-I network to external interfaces for transmitting plant data to end clients (EOF, nuclear data link, and nuclear emergency response center). Additional proposed markups to Figure 7.1-1 of the DCD Figure 4-1 of the D3 TeR and CSCCF Coping Analysis TeR and Figure 4.1-1 of the CSCCF TeR were included to incorporate the additional details regarding this one-way external interface. The staff finds the additional descriptions and proposed markups adequately describe the one-way interface between the I&C systems and external networks by demonstrating how this interface is one-way and prevent data flow changes using software/software configuration. The incorporation of the proposed markups into the next revision to Section 4.6.2.7 and Figures 4-1 and 4-25 of the Safety I&C System TeR, Revision 3, Figure 7.1-1 of the DCD Tier 2, Revision 3, Figure 4-1 of the D3 TeR, Revision 3 and CCF Coping Analysis TeR, Revision 3, and Figure 4.1-1 of the CSCCF TeR, Revision 3, was a confirmatory item. The staff verified the incorporation of the proposed marksups in Section 4.6.2.7 and Figures 4-1 and 4-25 of the Safety I&C System TeR, Revision 3, Figure 7.1-1 of the DCD Tier 2, Revision 3, Figure 4-1 of the D3 TeR, Revision 3, and CCF Coping Analysis TeR, Revision 3, and Figure 4.1-1 of the CSCCF TeR, Revision 3. As such, this confirmatory item has been satisfied.

7.1.4.10.4.1 Interconnected Equipment

For interconnected equipment, IEEE Std 603-1991, Clause 5.6.3.1, requires:

- Equipment that is used for both safety and non-safety functions to be classified as part of the safety-related systems. Isolation devices used to affect a safety-related system boundary shall be classified as part of the safety-related system.

- No credible failure on the non-safety side of an isolation device shall prevent any portion of a safety-related system from meeting its minimum performance requirements during and following any DBE requiring that safety function. A failure in an isolation device

> shall be evaluated in the same manner as a failure of other equipment in a safety-related system.

The SRP BTP 7-11 specifies that fiber optical cables provide acceptable electrical isolation to prevent propagation of credible faults. Section A.5.6 of the Safety I&C System TeR states

> a non-Class 1E instrumentation circuits and cables that are in proximity of Class 1E circuits without adequate physical separation or electrical isolation are classified as an associated circuit regardless of whether or not analyses or tests can demonstrate that credible failures therein cannot adversely affect Class 1E circuits….protection division is physically separated and electrically isolated from the other three protection divisions. All connections to non-safety equipment are through isolation devices and are one way during plant operation.

Section 4.1.3.1 of the Safety I&C System TeR, states, in part, "…DPS ESF actuation signals are hardwired to the CIM through the isolation device," and Section 4.1.3.3 states, in part, "The DMA switches signals are hardwired to the CIM through the isolation device."

The current application does not describe how these isolation devices are qualified to provide isolation between safety and non-safety-related I&C systems. As such, the staff issued RAI 45-7883, Question 07.09-1, to request the applicant describe how these isolation devices address the isolation guidance in SRP BTP 7-11, RG 1.75, Revision 3, and DI&C-ISG-04, Revision 1, in order to demonstrate compliance to IEEE Std 603-1991, Clause 5.6. The staff also requested the applicant to address independence criteria and isolation guidance for isolation devices discussed in other sections of the Safety I&C System TeR. In the September 23, 2015, response to RAI 45-7883, Question 07.09-1 (ML15266A521), the applicant committed to updating the DCD Tier 2, Safety I&C System TeR and CIM TeR. The markups in the technical reports addressed the staff's question regarding isolation devices between redundant safety divisions and between safety-related and non-safety systems, and how isolation devices conform to NRC guidance to comply with independence requirement. As a result, the staff considers the response to RAI 45-7883, Question 07.09-1, acceptable. The verification that the proposed markups are incorporated into the next revision of the FSAR was a confirmatory item. The staff verified that the proposed markups have been incorporated into the Safety I&C System TeR, Revision 1 and the CIM TeR, Revision 1. As such, this confirmatory item has been satisfied.

The staff finds the safety-related I&C system design meets the interconnected equipment requirements in Clause 5.6.3.1 of IEEE Std 603-1991.

7.1.4.10.4.2 Equipment in Proximity

For equipment in proximity of safety-related systems, IEEE Std 603-1991, Clause 5.6.3.2 requires:

- Equipment in other systems that is in physical proximity to safety equipment, but that is neither an associated circuit nor another Class 1E circuit, shall be physically separated from the safety-related system equipment to the degree necessary to retain the safety-related 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.

- Physical barriers used to effect a safety-related system boundary shall meet the requirements of Clauses 5.3, 5.4 and 5.5 for the applicable conditions specified in Clauses 4.7 and 4.8 of the design basis.

Appendix Section A.5.6 of the Safety I&C System TeR states, "Physical separation is achieved by physical barriers or acceptable separation distance. The separation distance of Class 1E equipment is designed in accordance with the requirements of IEEE Std 384-1981.

This section is supplemented by DCD Tier 2 Table 7.1-1 and Section 7.1.2.42, which states that applicable I&C systems listed in the table will be designed to meet the guidance RG 1.75, Revision 3, which endorses IEEE Std 384-1992. Based on the applicant's commitment to provide physical separation between safety-related I&C systems and non-safety I&C systems in accordance with RG 1.75, Revision 3, the staff finds the applicant has adequately addressed the physical separation requirements of IEEE Std 603-1991, Clause 5.6.3.

The staff's evaluation of DCD Tier 1 Table 2.5.1-5 (2 of 10), ITAAC 3.b, to verify adequate physical separation exists between the Class 1E equipment and non-Class 1E equipment is documented in Section 14.3.5 of this SER.

7.1.4.10.4.3 Effects of a Single Random Failure

For effects of a single random failure, IEEE Std 603-1991, Clause 5.6.3.3, stipulates that where a single random failure in a non-safety system can result in a DBE, and also prevent proper action of a portion of the safety-related system designed to protect against that event, the remaining portions of the safety-related system shall be capable of providing the safety function even when degraded by any separate single failure.

Section 7.1.240 of the FSAR states the applicable I&C systems listed in Table 7.1-1 will be designed to meet the guidance of RG 1.53, "Application of the Single Failure Criterion to Nuclear Power Plant Protection Systems," Revision 2, which endorses IEEE Std 379-2000, "Application of the Single Failure Criterion to Nuclear Power Generating Station Safety Systems." This is supplemented by discussion of the application of the single failure criterion in Section 7.2.3.1 of the FSAR which states the reactor protection system is designed with four independent and redundant divisions, and that any single failure does not prevent a system-level reactor protection system trip. Likewise, Section 7.3.3.1 of the FSAR states "any single failure does not prevent a system-level ESFAS function due to four division redundancy." Table 7.2-7 is the system-level FMEA for RPS and Table 7.3-8 is the system-level FMEA for the ESF-CCS.

To summarize, APR1400 safety-related I&C systems are implemented in four independent divisions. The safety-related I&C systems retain the ability to perform their function given a single failure of a common element to both the safety related and non-safety systems concurrent with another single failure. Section 7.7.1 of the FSAR states:

> the control systems are implemented on a digital platform that is diverse in both hardware and software from the safety common platform…non-safety systems that interface with [safety-related] systems are designed so that credible failures do not impact the operation of [safety-related] systems…interfaces between safety and non-safety systems use isolation devices…in general, non-safety control system sensors and signal conditioning devices are separated from those used in the safety-related control systems.

These design characteristics help to minimize the possibility of a single failure that results in a DBE that also reduces the redundancy of the safety-related systems. The safety-related systems implement error detection algorithms to detect and address failures.

As required by Clause 5.6.3.3 of IEEE Std 603-1991, safety-related systems must retain the ability to perform safety functions in the presence of DBEs and single random failures of non-safety-related systems. Sections 7.1.4.10.4.1 and 7.9 of this SER documents the evaluations that the APR1400 safety-related I&C systems will function independent of credible failures in interconnected equipment. Based on the information presented in Section 7.1.4.10.4.3 of the FSAR the staff concluded that there is no single random failure common to a non-safety system and a portion of the safety-related system that can result in a DBE and also prevent proper action of the remaining redundant portions of safety-related I&C equipment. As such, the staff finds the APR1400 I&C systems design satisfies Clause 5.6.3.3 of IEEE Std 603-1991.

7.1.4.11 Capability for Test and Calibration

The staff's review included the determination of whether IEEE Std 603-1991, Clause 5.7, has been adequately addressed for the APR1400 safety-related I&C systems. IEEE Std 603-1991, Clause 5.7 requires capability for testing and calibration of safety-related system equipment while retaining the capability of the safety-related I&C systems to accomplish their safety functions. The capability for testing and calibration of safety-related system equipment shall be provided during power operation and shall duplicate, as closely as practicable, performance of the safety function. The capability should be provided to permit testing during power operation. GDC 21 requires, in part, that the protection systems shall be designed to permit periodic testing of its functioning when the reactor is in operation, including a capability to test channels independently to determine failures and losses of redundancy that may have occurred. RG 1.118, "Periodic Testing of Electric Power and Protection Systems," Revision 3, which endorses IEEE Std 338-1987, "Criteria for the Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems," and RG 1.22, "Periodic Testing of Protection System Actuation Functions (Safety Guide 22)," Revision 0, provide guidance on periodic testing of the safety-related systems. The periodic testing should replicate, to the extent possible, the overall performance required of the safety-related systems. SRP Appendix 7.1-C, SRP Appendix 7.1-D, and SRP BTP 7-17, "Guidance on Self-Test and Surveillance Test Provisions Review Responsibilities," provide additional guidance on the capability for test and calibration for digital computer-based safety-related systems, which includes test provisions to address the increased potential for subtle digital system failures, and capabilities of the software to perform self-test.

<u>Automated Fault Detection Features</u>

DCD Tier 2 Section 7.2.2.5 the applicant states that system integrity is accomplished through a combination of self-diagnostics and surveillance testing. In DCD Tier 2 Section 7.2.3.1, the applicant states, in part, that any single failure is detectable by diagnostic or periodic testing. The use of the term "diagnostic" in this case is equivalent to self-diagnostics. The Safety I&C System TeR Section A.5.7 states, in part, that, "The PPS incorporates continuous system self-checking features that minimize required manual surveillance and periodic testing. System self-checking features include on-line diagnostics for the computer system, hardware, and the communications systems."

The applicant has not provided a comprehensive list of automated self-testing and self-diagnostic features that are incorporated into the I&C systems for the APR1400 design to justify claims of full coverage through self-diagnostics and surveillance testing. The applicant also does not describe what was intended when it states that continuous self-checking features minimize required periodic testing. The applicant has not provided an argument to support this statement and has not specifically stated in applicable parts of the FSAR that the APR1400 design credits certain self-testing features in lieu of performing some surveillance or periodic testing. In addition, the applicant has not stated how it intends to periodically verify self-diagnostic/self-testing features functionality, as per the guidance set forth in SRP BTP 7-17, nor the ability of automated checking features to detect postulated single failures in hardware or software.

DCD Tier 2 Chapter 16, Technical Specification bases, B 3.3.1 for RPS Instrumentation, states, in part, that the channel functional test surveillance requirement (SR) 3.3.1.10 for the CPCs testing frequency will be 18 months and that the basis for the 18 month frequency is that the CPCs perform a continuous self-monitoring function that eliminates the need for more frequent testing. This section also states that the channel functional test essentially validates self-monitoring function and checks for, *"....a small set of failure modes that are undetectable by the self-monitoring function*." This would imply that automated fault detection features are being used to justify a lowered frequency of surveillance testing for the CPCs. However, there is no technical basis provided for why this is an acceptable approach such as relating the bases to the CPC watchdog timer implementation shown in Figure 4-11 in the Safety I&C System TeR.

RAI 356-7881, Questions 07-01 and 07-02 requested the applicant to describe the full set of self-diagnostic and self-testing capabilities incorporated within the APR1400 for the safety-related I&C systems. Question 07-02 also requested the applicant to provide more information on the set of failure modes that are undetectable by the automated self-testing features as well as how self-testing features are credited in periodic testing and surveillance activities.

In the April 5, 2016, response to RAI 356-7881, Questions 07-01 (ML16096A179), the applicant stated that the automated self-checking features incorporated into the APR1400 Safety I&C Platform are provided in detail in Section 5.2.1.1.1 of the Common Q Platform Topical Report, Revision 3. The applicant stated that Section 5.2.1.2.1 of the Common Q Platform Topical Report describes the standard AC160 system software functions performed included diagnostics and communications interfaces. Additional information regarding diagnostics performed by system application software is provided in Section 5.4.1 of the Common Q Platform Topical Report. The Common Q internal diagnostics are provided in the base software of the AC160 modules, self-contained diagnostics included with each input/output module and CIM. They both are used to report error conditions associated with module operations, which are collected and reported by the application program.

The applicant stated that DCD Tier 2 Table 7.2-7, "Failure Modes and Effects Analysis for the Plant Protection System," identifies failure associated with application program memory are detected by cyclic redundancy checks (CRCs) performed on the memory and this is an automated feature provided by the application software CRC calculations and checks. The applicant also stated that the application software itself was developed using the software lifecycle development process as defined in the SPM. The safety-related I&C platform is implemented on the Common Q platform, which was commercially grade dedicated and qualified for nuclear power plants in the United States. Therefore, application software that performs self-checking functionality, as stated above, would also be part of the safety

qualification under commercial grade dedication process as well as the other aspects of the safety-related I&C platform for the APR1400 design.

The response to RAI 356-7881, Question 07-01, references the response to RAI 301-8280, Question 07.01-44. In the April 22, 2016, response to RAI 301-8280, Question 07.01-44 (ML16113A458), the applicant proposed a modification of DCD Tier 1 to add ITAAC Item 24 in Sections 2.5.1, 2.5.3, and 2.5.4, and Tables 2.5.1-5, 2.5.3-3, and 2.5.4-4 to ensure safety grade protection systems are installed in accordance to approve commercial grade dedication process for hardware and software. In addition to these changes, the applicant stated that Item 13 of DCD Tier 1 Section 2.5.1.1 and Table 2.5.1-5, and Item 10 of Tier 1, Section 2.5.4.1 and Table 2.5.4-4 provide verification that system integrity is maintained during events such as a loss of power or component failure.

The Common Q platform, as described in the associated topical report, has been previously reviewed and approved for use by the NRC. This would necessarily include all aspects of the platform including application software used to implement automated self-checking features. The applicant has committed that the automated self-checking features implemented in the APR1400 design are implemented in accordance to the functionality described in the Common Q Platform Topical Report. The applicant has identified ITAAC that verifies the design functionality of the self-testing and diagnostic features in the as-built system. As such, the staff finds applicant's response to RAI 356-7881, Question 07-01, and associated proposed changes are acceptable. The incorporation of the proposed changes into the next revision of the FSAR was a confirmatory item. The staff verified that that the proposed markups have been incorporated into Revision 1 of the FSAR. As such, this confirmatory item has been satisfied.

In the April 5, 2016, response to RAI 356-7881, Questions 07-02 (ML16096A179), the applicant addressed staff queries regarding the relationship of automated testing features and periodic surveillance activities. The applicant stated that the PPS does not credit automated self-testing features or self-diagnostics to reduce surveillance testing frequency. However the applicant stated that CPCS credits automated self-diagnostic features of the algorithms that calculate the DNBR and LPD reactor trips. The applicant stated that the technical basis for the 18 month surveillance frequency is aligned with that of NUREG 1432, "Standard Technical Specifications Combustion Engineering Plants," Revision 4, Volume 2, "Bases," for SR 3.3.1.11 (equivalent to APR1400 surveillance requirement 3.3.1.10) which states:

> The basis for the 18 month Frequency is that the CPCs perform a continuous self-monitoring function that eliminates the need for frequent CHANNEL FUNCTIONAL TESTS. This CHANNEL FUNCTION TEST essentially validates the self-monitoring function and checks for a small set of failure modes that are undetectable by the self-monitoring function. Operating experience has shown that undetected CPC or CEAC failures do not occur in any given 18 month interval.

The CPCS calculates DNBR and LPD for reactor trips and if there is a failure within the CPCS, the applicant stated that this will produce an effect in the above-mentioned calculations. SR 3.3.1.1 is the surveillance requirement that requires the operator perform 12- hour channel checks of each RPS channel. This check examines the calculations performed in each channel and if there is a difference in calculated value for each channel, it is alarmed to the operator. The applicant also stated that the major trip functions of the CPCS are periodically tested under SR 3.3.1.7 every 31 days, which includes the DNBR and LPD trips.

Regarding potential undetected failures, the applicant stated, in part, that failures that are not detected by AC160 self-checking and diagnostic functions are failures of components that are not a part of the Common Q platform (e.g., circuit breakers, interposing relays, keyboards, etc.). For failures of these types, the applicant stated that there are other indications available to operators such as unexpected trip conditions, indication of invalid plant data, spurious alarms, etc. These types of failures would be captured during periodic surveillance testing. The applicant clarified in the April 5, 2016, response to RAI 356-7881, Question 07-02, that the only portion of the APR1400 design for which there is crediting of automated self-checking features to alter surveillance frequency is the CPCS. To credit these automated self-checking features, the applicant has demonstrated that it is adhering to pre-approved staff guidance. The applicant demonstrated that CPCS functionality is verified both through automated features and through periodic, manual channel checks as per guidance provided in NUREG-1432, Volume 2, Revision 4. For these reasons, the staff finds applicant's response to RAI 356-7881, Question 07-02, is acceptable. The staff considers this RAI closed and resolved.

Periodic Testing

DCD Tier 2 Table 7.1-1, "Regulatory Requirements Applicability Matrix" states that the guidance of RG 1.118, Revision 3, has been applied to the RTS, ESF-CCS, QIAS-N and QIAS-P. The Safety I&C System TeR, Section A.5.7 states that the PPS and ESF-CCS design complies with IEEE St. 338-1987, "Standard Criteria for the Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems," and RG 1.22, Revision 0.

With regards to conformance to IEEE Std 338-1987, the applicant states in Section 3.4.10 of the Safety I&C System TeR that a complete channel can be tested without causing a spurious safety-related system action or affecting operability of the system under test. Testing does not interfere with the ability of the safety-related system to provide its safety function as testing is done on a per-division basis.

The Safety System TeR, Section 4.2.1.10 describes the MTP. The MTP is the primary means to initiate and perform maintenance and surveillance testing for the safety-related I&C systems. DCD Tier 2 Section 7.1.2-71 states the MTP, ITP, and associated communication path software are qualified to meet the requirements of IEEE Std 7-4.3.2-2003, which is endorsed by RG 1.152, Revision 3. Because these systems are used to periodically test safety-related systems, they each have ITS software class as per requirements of the SPM TeR.

DCD Tier 2 Section 7.2 states that the MTP and the ITP cabinet are divisionalized and located in I&C equipment room. The MTPs and ITPs are shared by the PPS, ESF-CCS, CPCS, QIAS-P. With regard to the MTP design implementation, the applicant goes on to state that:

> The bistable trip channel bypasses, all-bypass, operating bypass, and setpoint reset switches are provided on the MTP switch panel. These switches are directly connected to the digital input module of the [bistable processors] or LCL processors. The MTP also provides a unidirectional data communication gateway function to send a selected [safety-related] system division status to the [IPS].

DCD Tier 2 Section 7.3 states the MTP provides the indication for ESF-CCS status, ESFAS reset, and the HSIs for maintenance, testing, and diagnostics.

Section A.5.7 of the Safety I&C System TeR states that overlap testing confirms operability of each hardware modules and specifically verifies operability for components that are not tested through automated testing features. According to the applicant, the overlapping portion of the testing is accomplished by injection of test signals just before the monitoring point used for the previous test within the channel being tested. This is used to verify processor operability and communication paths. Figure 4.2-4 of the Safety I&C System TeR depicts the overlap testing philosophy for the RTS and ESF-CCS. IEEE Std 338-1987, states, in part, that the channel testing should be as close to practicable from sensor to final actuation device.

The Safety I&C System TeR, Section 3.4.1, provides more information on the conformance of the APR1400 design to RG 1.22, Revision 0. The applicant states in part, the following:

- The APR1400 design contains provisions to permit periodic testing of the entirety of the safety-related I&C systems at power or in shutdown modes of operation.
- Periodic testing of the PPS is from sensor to final actuating device.
- Manual testing is administratively controlled to prevent potential equipment actuations in more than one channel due to testing.
- Bypassed equipment status is provided in the MCR.
- ESF actuation devices that cannot be tested when the reactor is at power are tested during reactor shutdown.

Section 3.4.10 of the Safety I&C System TeR provides more information on the conformance of the APR1400 design to RG 1.118, Revision 3. The applicant states, in part, that the safety-related I&C is design to facilitate periodic testing in conformance to RG 1.118, Revision 3. The system design support periodic testing to verify operability and that a complete division without causing a reactor trip, ESF actuation nor will the testing affect operability or availability of the system under test. With any one division of logic is under test, the remaining three division will still provide their safety functions. The testing scheme is described in Section 4.2.2 of the Safety I&C System TeR. Section 4.2.2 states, in part, that monitoring, testing and maintenance of the PPS is provided by the MTP and ITP located in each individual safety division. Bistable trip inputs from the BP to the LCL processors are bypassed in order to perform maintenance and/or testing activities for instrument channel inputs. This allows for continued operation with a channel in bypass. The applicant states that the trip channel bypass changes the 2oo4 coincidence logic to 2oo3 coincidence logic.

The Safety I&C System TeR, Section A.5.7 states that overlap testing confirms operability of each hardware module and specifically verifies operability for components that are not tested through automated testing features. According to the applicant, the overlapping portion of the testing is accomplished by injection of test signals just before the monitoring point used for the previous test within the channel being tested. This is used to verify processor operability and communication paths. Figure 4.2-4 of the Safety I&C System TeR depicts the overlap testing philosophy for the RTS and ESF-CCS. IEEE Std 338-1987, states, in part, that the channel testing should be as close to practicable from sensor to final actuation device.

Section A.5.7 of the Safety I&C System TeR also states that PPS bypasses are initiated via channel bypass switches on the MTP switch panel. The ability to initiate bypasses and verify that usage of the MTP does not affect safety-related system functionality is not specifically

identified in the Tier 1 ITAAC for RPS and ESF-CCS (DCD Tier 1, Sections 2.5-1, 2.5-3, and 2.5-4, respectively).

DCD Tier 1 Table 2.5.1-5 contains ITAAC that provides for verification of the following:

- Manual control functionality at the MTP as well as verification of trip channel bypasses.
- Bypassed/inoperable instrument status indication in the MCR.
- PPS logic modification in presence of a bypassed channel.
- Reactor trip and ESF actuation initiation in the presence of a single bypassed channel.
- RTS and ESF automated self-testing functions for malfunctioning equipment.

Based upon the design information provided on the inherent design features of the APR1400 related to testing safety-related I&C system channels, the staff finds the APR1400 design meets the requirements IEEE Std 603-1991, Clause 5.7, GDC 21, as well as relevant guidance associated with meeting these criteria. The applicant has demonstrated and detailed the methodology and equipment used to perform maintenance and testing on the safety-related I&C systems, with the plant both at power and in shutdown. The applicant described the entirety of its overlapping test program that verifies the operability of safety channels from sensor to final actuation device, along with description of testing equipment (e.g., divisional MTPs) and process for how testing will be performed to eliminate potential for unintentional equipment operation. The applicant also adequately described how automated self-testing and self-monitoring features aid in detecting faulted hardware and/or software through the use of WDTs, application program and data communication error CRC checks, self-diagnostics inherent to the input/output modules and processor modules, etc. The staff finds that the above-referenced Tier 1 ITAAC provides reasonable assurance of the verification of proper implementation of design criteria and information presented in the as-built PPS to meet the requirements of IEEE Std 603-1991, Clause 5.7 and GDC 21.

7.1.4.12 Information Displays

The staff reviewed APR1400 design certification application to verify that IEEE Std 603-1991, Clause 5.8, has been adequately addressed for the APR1400 safety-related I&C systems. IEEE Std 603-1991, Clause 5.8.1, states, in part, that the display instrumentation provided for manually controlled actions for which no automatic control is provided and the display instrumentation required for the safety-related systems to accomplish their safety functions shall be part of the safety-related systems and shall meet the requirements of IEEE 497-1981, “IEEE Standard Criteria for Accident Monitoring Instrumentation for Nuclear Power Generating Stations.” The design shall minimize the possibility of ambiguous indications that could be confusing to the operator. IEEE Std 603-1991, Clause 5.8.2 states:

> Display instrumentation shall provide accurate, complete, and timely information pertinent to [safety-related] system status. This information shall include indication and identification of protective actions of the sense and command features and execute features. The design shall minimize the possibility of ambiguous indications that could be confusing to the operator. The display instrumentation provided for [safety-related] system status indication need not be part of the [safety-related] systems.

IEEE Std 603-1991, Clause 5.8.3 states, "[i]f the protective actions of some part of a [safety-related] system have been bypassed or deliberately rendered inoperative for any purpose other than an operating bypass, continued indication of this fact for each affected safety group shall be provided in the control room."

In addition, IEEE Std 603-1991, Clause 5.8.3.1, states, in part, that the display instrumentation need not be part of the safety-related systems. IEEE Std 603-1991, Clause 5.8.3.2, states, in part, that the indication shall be automatically actuated if the bypass or inoperative condition; a) is expected to occur more frequently than once a year, and b) is expected to occur when the affected system is required to be operable. IEEE Std 603-1991, Clause 5.8.3.3, states, in part, that the capability shall exist in the control room to manually activate this display indication. IEEE Std 603-1991, Clause 5.8.4, states, in part, that the information displays shall be located accessible to the operator. Information displays provided for manually controlled protective actions shall be visible from the location of the controls used to effect the actions.

SRP Appendix 7.1-C provides acceptance criteria to address the clauses of IEEE Std 603-1991. SRP Appendix 7,1-C, Clause 5.8, states that the review of information displays for manually controlled actions should include confirmation that displays will be functional (e.g., power will be available and sensors are appropriately qualified) during plant conditions under which manual actions may be necessary and that the safety-related system bypass and inoperable status indication should conform with the guidance of RG 1.47, "Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems," Revision 1.

To address the requirements of IEEE Std 603-1991, Clause 5.8.1, the Safety I&C System TeR, Section A.5.8, states that the QIAS-P (safety) provides the displays of all RG 1.97, Revision 4, Types A, B, and C variables including the inadequate core cooling (ICC) monitoring variables. The QIAS-N provides the displays of Type A, B, and C variables and selected variables of Type D and E to support performing plant safe shutdown and EOPs. The IFPD displays for all variables for Type A, B, C, D and E, and provides recording function for Type A, B, and C variables. The staff's evaluation regarding the displays for the QIAS-P, QIAS-N, and the IFPD that support manually controlled actions are evaluated Section 7.5.4.1 of this SER.

To address the requirements of IEEE Std 603-1991, Clause 5.8.2, the Safety I&C System TeR, Section A.5.8, states that system status indication is provided for all protective actions, including division trips, at the operator module, IPS and MTP. The staff evaluation for task analysis and human-system interface is in Sections 18.4 and 18.7 of this SER. In addition, Section 7.5.4.1.2 of this SER evaluates the APR1400 conformance to RG 1.97, Revision 4 and its endorsement of IEEE Std 497-2002, which provides performance based criteria for selecting variables and determining the variable type according to its accident management function.

To address the requirements of IEEE Std 603-1991, Clause 5.8.3, the Safety I&C System TeR, Section A.5.8, states that the operating bypass and trip channel bypass status is available for display at the IPS display (non-safety) and operator module in the MCR (safety), and MTP in the I&C equipment room at all times. The indications are provided in the Large Display Panel (LDP) and the IFPD (by navigating). In Section 7.5.4.2, the staff evaluated the bypassed and inoperable status indication (BISI) for the conformance to RG 1.47, Revision 1. The BISI provides system-level indication of deliberately introduced inoperability of the protection system. Alarms are actuated when a component actuated by a protection system is bypassed or deliberately rendered inoperable.

The Safety I&C System TeR, Section A.5.8, for Clause 5.8.4, states that the status information including input variable value, setpoint, trip, pre-trip, initiation, trip channel bypass and operating bypass is displayed on the IPS, the operator module FPD in the MCR, and MTP in the I&C equipment room. The staff evaluation for task analysis and human-system interface is in Sections 18.4 and 18.7 of this SER.

The staff's evaluation regarding the displays for the QIAS-P, QIAS-N, and the IFPD that support manually controlled actions, the conformance to RGs 1.97, Revision 4, RG 1.47, Revision 1, and IEEE Std 497-2002, are evaluated in Section 7.5.4.1 of this SER. Based on the conclusions in Section 7.5.4.1, the staff determined the APR1400 design meets the IEEE Std 603-1991, Clause 5.8 requirements.

7.1.4.13 Control of Access

IEEE Std 603-1991, Clause 5.9 requires that the safety-related system design permit the administrative control of access to safety-related system equipment. These administrative controls shall be supported by provisions within the safety-related systems, by provision in the generating station, or by a combination thereof. SRP Appendix 7.1-C provides acceptance criteria to address the clauses of IEEE Std 603-1991. SRP Appendix 7,1-C, Clause 5.9, states that administrative control is acceptable to assure that the access to the means for bypassing safety-related system functions is limited to qualified plant personnel and that permission of the control room operator is obtained to gain access. The review of access control should confirm that design features provide the means to control physical access to safety-related system equipment, including access to test points and means for changing setpoints. Typically, such access control includes provisions such as alarms and locks on safety-related system panel doors, or control of access to rooms in which safety-related system equipment is located. Review of digital computer-based systems should consider controls over electronic access to safety-related system software and data. Controls should address access via network connections, and via maintenance equipment.

Safety I&C System TeR, Appendix A, Section A.5.9, "Control of Access," states, in part, the [safety-related] I&C system has several design features to control physical access…via key locks and administrative procedures…keys or built-in features are provided to control access to setpoints, calibration data, and test point adjustments.

The staff finds the physical control of access features (e.g., key locks) provided are acceptable based on their ability to prevent inadvertent or unauthorized physical access to the safety-related system.

Control of the software development and operational environment is addressed in Section 7.1.4.7 of this SER. Also, conformance to DI&C-ISG-04, Revision 1, with regards to control of access is addressed in Section 7.9.4.6 of this SER. Physical security is addressed in Section 13.6 of this SER. Based upon the information provided to demonstrate conformance to SDOE guidance within RG 1.152, Revision 3, the staff determined the safety-related I&C system design meets control of access requirements of IEEE Std 603-1991, Clause 5.9.

7.1.4.14 Repair

The staff reviewed APR1400 design certification application to verify that IEEE Std 603-1991, Clause 5.10 has been adequately addressed for the APR1400 safety-related systems. IEEE Std 603-1991, Clause 5.10 requires that the safety-related systems be designed to facilitate

timely recognition, location, replacement, repair, and adjustment of malfunctioning equipment. SRP Appendix 7.1-C, Section 5.10 states that digital safety-related systems may include self-diagnostic capabilities to aid in troubleshooting. However, the use of self-diagnostics should not replace the need for the capability for test and calibration systems. SRP BTP 7-17 describes characteristics that digital computer-based diagnostic systems should exhibit. For the digital computer-based systems, the surveillance testing with automatic self-testing should be provided to detect all detectable failures and assist the repair work.

DCD Tier 2 Table 7.1-1 states, that the RPS, ESF-CCS, and QIAS-P conform to the guidance of SRP BTP 7-17. SRP BTP 7-17 states that digital safety-related systems can include self-diagnostic features to aid in troubleshooting activities. The Safety I&C System TeR, Section A.5.7 states that the PPS, CPCS and ESF-CCS contains self-checking features for the computer system, hardware and communications. Examples of these features include watchdog timers, internal hardware diagnostics, and CRC checks for software integrity.

Safety I&C System TeR, Section A.5.10 states, "[i]dentification of a defective input channel will be accomplished by observation of system status indication or by testing. Replacement or repair of components is accomplished with the affected input channel bypassed. The affected trip function then operates in a [2oo3] trip logic while maintaining the coincidence of two required for trip or actuation. For the [1oo2] ESFAS (BOP portion), the affected trip function then operates in single active channel trip logic."

Section 3.4 of the Safety I&C System TeR states, in part, that safety-related I&C systems comply with the guidance of RG 1.22, Revision 0, which provides criteria for the design to incorporate provisions to permit periodic testing of the complete safety-related I&C system as well as bypassed channel status indication being available in the MCR.

The SPM TeR, Section 14.2.3 describes software controls in place to detect potential alteration of various system aspects including memory alteration. This section states that operating system software and application software that are initially installed in each processor memory have CRC values associated with the software that are stored along with the actual software. The CRC values for the actual software are periodically recalculated and then compared to the original CRC values by continuous self-test features. Any discrepancies between the compared values is alarmed to operators. In the case that both the CRC stored value and newly calculated CRC value both match, but are incorrect, a manual periodic diverse software check will detect the errors. The diverse software check involves comparing the installed software to a software baseline that is independently maintained outside the safety-related I&C system. The diverse method of comparison is accurate to the bit level (e.g., bit by bit comparison or CRC). Where a CRC is employed, the CRC value of the installed software is calculated and compared to a CRC value of the independently maintained software outside the safety-related I&C system. SRP BTP 7-17 guidance states that self-testing functionality should be periodically verified. CRC checks of memory that contains self-testing software is one method that could accomplish this check. However, the applicant has not specifically stated within the licensing documents that CRC checks are utilized in this manner. RAI 356-7881, Question 07-02, was issued to the applicant to clarify its approach to meeting the guidance of SRP BTP 7-17.

In the April 5, 2016, response to RAI 356-7881, Question 07-02 (ML16096A179), the applicant stated that the integrity of the memory containing all of the diagnostics, self-checking features and provisions inherent to the system for periodic manual maintenance testing is verified by CRC checks via the AC160 module as described in Section 2.1, 2.2 and 2.4 of the Common Q Platform Topical Report. Including manual periodic testing, CRC checks of system memory

containing automated self-testing features software is an adequate means of periodically verifying self-testing functionality. Once safety-related system software lifecycle design is commenced and completed through to commissioning testing, CRC checks verifying that memory containing self-checking software has not degraded or been corrupted in anyway is sufficient to fulfill guidance of SRP BTP 7-17. Software defects notwithstanding, software generally does not degrade. However, the physical memory containing this software can degrade and the CRC checks, automatic checks, or manually initiated checks evaluate for this failure vector. Based on the use of CRC to periodically verify the physical memory containing software has not degraded, the staff finds applicant's response to RAI 356-7881, Question 07-02, is acceptable. The staff considers this RAI question is closed and resolved.

The staff finds the APR1400 design meets the requirements of IEEE Std 603-1991, Clause 5.10. The applicant has adequately stated compliance to relevant guidance with regard to testing of the safety-related I&C systems. The applicant has adequately demonstrated that the APR1400 design contains both automatic fault tolerance features, manual (e.g., MTPs) testing measures and equipment status indication to facilitate timely repairs of the safety-related I&C systems.

7.1.4.15 Identification

The staff reviewed the APR1400 design certification application to verify that IEEE Std 603-1991, Clause 5.11 has been adequately addressed for the APR1400 safety-related systems. IEEE Std 603-1991, Clause 5.11 requires that (1) safety-related system equipment be distinctly identified in accordance with the requirements of IEEE Std 384-1981, (2) components or modules mounted in equipment or assemblies that are clearly identified as being in a single redundant portion of a safety-related system do not themselves require identification, (3) identification of safety-related system equipment be distinguishable from other purposes, (4) identification of safety-related system equipment does not require frequent use of reference material, and (5) the associated documentation be distinctly identified in accordance with the requirements of IEEE Std 494-1974. SRP Section 7.1, Appendix 7.1-C provides staff review criteria on meeting the requirements of IEEE Std 603-1991. Section 5.11 of this appendix states, "Guidance on identification is provided in RG 1.75, [Revision 3] which endorses IEEE Std 384-1992. The preferred identification method is color coding of components, cables, and cabinets."

Section A.5.11 of Appendix A of the Safety I&C System TeR states that all equipment, including panels, modules, and cables associated with the RPS and ESF systems, are marked in order to facilitate identification. The safety-related I&C system is configured in accordance with specific identification requirements which provide a standardized method for identifying equipment. The safety-related I&C system is also configured using diagrams and signals for the purpose of consistency during the installation process. Interconnecting cabling is color-coded. The physical identification is provided so that an operator can confirm if the safety-related I&C system cabinets and related cable are the safety class. The safety-related I&C system cabinets are distinguished by name plates. The safety-related I&C system components are uniquely identified by designations per project procedures and as defined in contract specifications. The physically isolated cable which connects sensor to actuation devices is identified by different colors between divisions. The identification of software is assured by identification provisions as discussed in the SPM TeR.

Based on the staff's review of the information presented in Section A.5.11 of Appendix A of the Safety I&C System TeR the staff finds that the application did not state that these specific

identification requirements of the safety-related I&C system will conform to the guidance of RG 1.75, Revision 3. In RAI 43-7887, Question 07.01-20, the staff requested that the applicant verify whether the specific identification requirements discussed in Section A.5.11 of Appendix A of the Safety I&C System TeR will conform to the guidance of RG 1.75, Revision 3 or if an alternate method is proposed. If an alternate method is used, the staff requested the applicant to provide justification as to why the method provides a comparable level of safety to the guidance in RG 1.75, Revision 3. In the September 24, 2015, response to this RAI (ML15267A764), the applicant stated,

> The RPS and ESF systems meet the identification requirements stated in Section 6.1.2, "Identification" of IEEE Std 384-1992, which is endorsed by RG 1.75, Revision 3. The conformance analysis for identification requirements is provided in Section A.5.11 of the Safety I&C System Technical Report. The following will be added to Section A.5.11, "Identification," of the Safety I&C System TeR: "The safety-related I&C system design meets the identification requirements of IEEE Std 384-1992, as endorsed by RG 1.75, Revision 3."

Based on the commitment to revise the Safety I&C System TeR to include the above statement, the staff finds the issues identified in RAI 43-7887, Question 07.01-20, is closed and resolved. The verification that the proposed markups are incorporated into the next revision of the Safety I&C System TeR was a confirmatory item. Based on the information provided in Section A.5.11 of Appendix A of the Safety I&C System TeR, commitments to conform to the guidance of RG 1.75, Revision 3 and the proposed changes in RAI 43-7887, Question 07.01-20, the staff finds the safety-related I&C system design meets the identification requirements in IEEE Std 603-1991, Clause 5.11. The staff verified that the proposed markups have been incorporated into Revision 1 of the Safety I&C System TeR. As such, this confirmatory item has been satisfied.

7.1.4.16 Auxiliary Features

The staff reviewed the APR1400 design certification application to verify that IEEE Std 603-1991, Clause 5.12 has been adequately addressed for the APR1400 safety-related systems. IEEE Std 603-1991, Clause 5.12 states that (1) auxiliary supporting features shall meet all requirements of this standard, and (2) other auxiliary features that perform a function that is not required for the safety-related systems to accomplish their safety functions, and are part of the safety-related system by association, shall be designed to meet those criteria necessary to ensure that these components, equipment, and systems do not degrade the safety-related systems below an acceptable level.

The staff finds that additional information is required regarding the auxiliary features that are designed to not affect the protection system from accomplishing their safety function. Specifically, in RAI 43-7887, Question 07.01-21, the staff requested the applicant to identify and describe how the auxiliary features (bypass, CWP signal, test, and calibration functions) within the protection system do not affect the protection system from accomplishing their safety functions. In addition, the application states that the HVAC and electrical power systems, built-in test equipment, and isolation devices are examples of safety auxiliary support systems. The staff requested the applicant to provide a comprehensive list of all safety auxiliary supporting features in the APR1400 design in order to meet the requirements of IEEE Std 603-1991, Clause 5.12. In the September 24, 2015 response (ML15267A764) as supplemented by the April 25, 2016 response (ML16116A440) to RAI 43-7887,

Question 07.01-21, the applicant stated the following are auxiliary supporting features and other auxiliary features:

Auxiliary Supporting Features

- Electric power supply system for the RPS and ESF systems.
- I&C portions of the component cooling water system (CCWS), essential service water system (ESWS), and ultimate heat sink.
- I&C portions of safety HVAC systems.

Other Auxiliary Features

- Equipment protection devices (monitoring for door open and cabinet high temperature)
- Operating bypass, trip channel bypass
- Setpoint reset/change function
- Built-in test functions
- Diagnostic functions
- Trip, pre-trip, sequence of events, and status indications/alarms
- Qualified isolators to interface with non-safety systems
    - EDG support systems
    - EDG fuel oil system
    - EDG cooling water system
    - EDG starting air system
    - EDG lubrication system
    - EDG combustion air intake and exhaust system

The applicant provided references in the FSAR that describes how the safety-related system supports auxiliary functions to perform setpoint changes, and testing, bypass, and calibration functions. The applicant stated that the PPS includes other auxiliary features beside the reactor trip function and ESF initiation function. The other auxiliary features conform to the independence requirements described in Section A.5.6 of the Safety I&C System TeR. Section 4.2.4 of the Safety I&C System TeR states that the "DRCS remote input/output cabinet receives a CWP signal from the PPS division D only….This signal is treated as an associated circuit and isolated at the DRCS remote input/output cabinet." It is unclear how a "CWP signal" can be an associated circuit. IEEE Std 384-1992 defines associated circuits as "Non-Class 1E circuits that are not physically separated or are not electrically isolated from Class 1E circuits by acceptable separation distance, safety class structures, barriers, or isolation devices. Circuits

include the interconnecting cabling and the connected loads." Based on the description provided by the applicant it was not clear to the staff how the DRCS remote input/output cabinet is an associated circuit. The staff requested the applicant to supplement the response to RAI 43-7887, Question 07.01-21, to describe how the DRCS remote input/output cabinet is an associated circuit. In addition, the staff requested the applicant to modify the FSAR or its referenced documents to include the list of other auxiliary supporting features and other auxiliary features as described in the RAI response. This issue was tracked as an open item.

In the October 5, 2016, supplemental response to RAI 43-7887, Question 07.01-21 (ML16279A503), the applicant described how the DRCS remote input/output cabinet is an associated circuit. Specifically, the applicant stated that the DRCS remote input/output cabinet is a non-class 1E cabinet, but it is directly connected with the power from the Class 1E vital bus power supply system and safety class equipment without any isolation. The applicant stated that the DRCS remote input/output cabinets are designated as quality Class 1 and are subject to the qualification requirements placed on Class 1E equipment in accordance with IEEE Std 384, Section 5.5.2. This qualification process will ensure that the DRCS remote input/output cabinets do not affect the safety functions of the safety-related system under environmental, EMI, and/or seismic conditions. In addition, the applicant proposed markups to Section A.5.12 of the Safety I&C System TeR that include the safety auxiliary supporting features described in the RAI response. Because the applicant clarified why the DRCS remote input/output cabinet is considered an associated circuit and the commitment to qualify the DRCS remote input/output to the requirements of IEEE Std 384-1992, as endorsed by RG 1.75, Revision 3, the staff finds the issues identified in RAI 43-7887, Question 07.01-21, is closed and resolved. In addition, the staff finds the proposed markups in the RAI response to include auxiliary supporting features into the Safety I&C System TeR is acceptable for demonstrating the requirements of IEEE Std 603-1991, Clause 5.12 (for ensuring safety auxiliary features meet the requirements of this standard and the non-safety auxiliary features cannot degrade the safety-related system) are satisfied. The staff verified that the proposed markups were included in the Safety I&C System TeR, Revision 1. Therefore, the staff finds the I&C design satisfies the requirements of IEEE Std 603-1991, Clause 5.12.

7.1.4.17 Derivation of System Inputs

The staff reviewed the application to verify that IEEE Std 603-1991, Clause 6.4, has been appropriately addressed. IEEE Std 603-1991, Clause 6.4 requires, in part, that sense and command features of the PS be direct measures of specified process variables shown in the design basis, when practical. Specifically, minimize the number of variables or derivatives of direct measured variables and secondary calculations required to provide the required measurement. The staff used SRP Appendix 7.1-C as guidance for this area of the evaluation.

The Safety I&C System TeR, Appendix A, Section A.6.4, states "in so far as is practicable, system inputs are derived from signals that are direct measures of the desired variables," and that the "process variables and derived parameters used for the PPS actuation functions are set by the safety analysis." Neutron flux, temperatures, and pressures are direct measurements. Level information is derived from differential pressure measurements. Flow information is derived from reactor coolant pump speed measurement, SG differential pressure, and reactor coolant temperature. It was not clear to the staff why flow information is based on derived measurements as opposed to be measured directly. The staff issued RAI 301-8280, Question 07.01-42, to request the applicant to provide rationale as to why it is acceptable to base flow information on derived measurements. In the December 28, 2015, response to RAI 301-8280, Question 07.01-42 (ML15362A593), the applicant stated "in the [CPCS], flow

information is derived from reactor coolant pump speed and density of the coolant in the hot leg because no method that directly measures the flow information is available in modern engineering." The staff finds the response acceptable because system inputs are derived from signals that are direct measurements to the extent practicable. The staff requested the applicant to incorporate the first sentence of the response into the FSAR as part of a supplemental response to this RAI. Pending the receipt and acceptability of the supplemental response, RAI 301-8280, Question 07.01-42, was tracked as an open item. The staff reviewed the measured variables documented in DCD Tier 2 Section 7.2 and Section 7.3, and confirmed that system inputs, are, to the extent feasible and practical, direct measures of the desired variables. The review of the identification of the necessary design performance requirements such as variable ranges and system response times, the conformance to guidance in SRP Appendix 7.1-C, and the verification of the design requirements in the ITAAC is documented in Section 7.1.4.4 and Section 14.3.5, respectively. In the October 26, 2016, supplemental response to RAI 301-8280, Question 07.01-42 (ML16300A371), the applicant provided a markup that incorporated the first sentence of the response into DCD Tier 2 Section 7.2.1.1. The verification that the proposed markup is incorporated into the next revision of the FSAR was a confirmatory item. The staff verified that that the proposed markup had been incorporated into the DCD Tier 2, Revision 1. As such, this confirmatory item has been satisfied. Based on the use direct measures of specified process variables to the extent practicable and the resolution of the open item associated with RAI 301-8280, Question 07.01-42, the staff has determined that the APR1400 I&C systems design meets the requirements of IEEE Std 603-1991, Clause 6.4.

7.1.4.18 Multi-Unit Stations

The staff reviewed the application to verify whether IEEE Std 603-1991, Clause 5.13 has been adequately addressed for the APR1400 I&C safety-related systems. IEEE Std 603-1991, Clause 5.13 allows sharing of SSCs between units at multi-unit generating stations provided that the ability to simultaneously perform required safety functions in all units is not impaired.

Section A.5.13 in Appendix A of the Safety I&C System TeR states that the requirement of IEEE Std 603-1991, Clause 5.13, "Multi-Unit Stations," is not applicable as there is no planned sharing between units. In addition, DCD Tier 2 Table 1.9-1 states that the design is going to be a single unit plant. As such, the staff agrees that IEEE Std 603-1991, Clause 5.13, is not applicable to the review for Chapter 7.

7.1.4.19 Human Factors Considerations

IEEE Std 603-1991, Clause 5.14 requires, in part, that human factors be considered throughout the design process. Safety I&C System TeR, Appendix A, Section A.5.14, states "the [safety-related] I&C system is designed for the operator and maintenance personnel to accomplish their assigned functions successfully during the various plant conditions," and that the "verification and validation activities are performed under the conditions specified in [APR1400-E-I-NR-14008, "APR1400 Human Factors Verification and Validation Implementation Plan"] (hereafter referred to as Human Factors V&V Plan TeR). Human factors are evaluated in Chapter 18 of this SER.

7.1.4.20 Reliability

The requirement of IEEE Std 603-1991, Clause 5.15, states that for the systems for which either quantitative or qualitative reliability goals have been established, appropriate analysis of the

design shall be performed in order to confirm that such goals have been achieved. GDC 29 requires that the protection and reactivity control systems be designed to assure an extremely high probability of accomplishing their safety functions in the event of AOOs. Guidance on the application of this criterion for safety-related system equipment employing digital computers and programs or firmware is found in IEEE Std 7-4.3.2-2003.

GDC 21 states, in part, that the protection system shall be designed for high functional reliability. SRP Section 7.1-C, Section 5.15 states, in part, that the assessment of reliability should consider the effect of possible hardware and software failures and the design features provided to prevent or limit the effects of these failures. Section 5.15 references SRP Section 7.1-D for the staff's position on software reliability as well as the insufficiency of quantitative reliability goals for digital computer use in safety-related systems as the sole means of addressing reliability requirements.

Section A.5.15 of the Safety I&C System TeR states that, with regard to meeting the requirements of IEEE Std 603-1991, Clause 5.15, the reliability attributes of PPS and ESF-CCS is described in Section 7 of this report. The applicant also states that the reliability of software will be assured by implementing the requirements of the Safety I&C System TeR. For conformance to SRP Section 7.1-D, the applicant states that the reliability analysis method for safety I&C systems is found in Section 7 of the Safety I&C System TeR.

Section 7 of the Safety I&C System TeR describes two types of analyses the applicant has performed to assess reliability of the safety-related systems:

- FMEA –FMEA is a qualitative method for identifying failure modes that can occur to components, the means by which the failure is detected (e.g., self-testing features, surveillance testing), compensating provisions built into the system (e.g., redundant divisions, fail-safe configuration), and the effects of the failure on the plant. FMEAs for the RPS and ESF-CCS can be found in DCD Tier 2 Section 7.2 and 7.3, respectively. The review of these FMEAs can be found in Sections 7.2 and 7.3 of this evaluation.

- Unavailability analysis using the fault tree model – The applicant states a quantitative analysis assesses the unavailability of the PPS and ESF-CCS when a demand on either function is present. This analysis also quantifies the probability of failure upon demand of the ESF-CCS. The fault tree contains failures/faults which could render the affected system (PPS or ESF-CCS) unavailable when a valid demand on either system is present.

The applicant did not provide the unavailability analysis within the Safety I&C Technical Report or within DCD Tier 2 Chapter 7. The applicant stated that this analysis, along with the FMEA of the safety-related I&C systems provides an overall means to demonstrate reliability. In RAI 356-7881, Question 07-20, the staff requested the applicant to present this analysis for the staff's evaluation of the reliability attributes of the safety-related I&C systems.

In a June 2, 2016, response to RAI 356-7881, Question 07-20 (ML16154A868), the applicant stated that the Unavailability Analysis, as described in the Safety I&C System TeR, Section 7.2, is not intended to address the reliability requirements of IEEE Std 603-1991. The applicant stated that Section 7.2 of the Safety I&C System TeR will be removed. The staff finds this response acceptable given that this analysis was not intended to be used to demonstrate reliability requirements are met and that reliability requirements for the APR1400 I&C design were intended to be demonstrated through other means such as system FMEAs, self-testing

and diagnostic features and maintenance activities. The staff finds the proposed changes to the Safety I&C System TeR contained in the applicant's response to RAI 356-7881, Question 07-20, are acceptable. The incorporation of the proposed markup into the next revision the Safety I&C System TeR was a confirmatory item. The staff verified that the proposed markups have been incorporated into Revision 1 of the Safety I&C System TeR. As such, this confirmatory item has been satisfied.

The SRP Appendix 7.1-D states, in part, that the NRC does not endorse quantitative reliability goals as the sole means of demonstrating reliability of digital computer systems, and has not endorsed any specific methodologies by which to quantify digital computer system reliability. Therefore, the review should focus on the qualitative means of demonstrating reliability goals as well as a high quality software lifecycle design process. Safety system FMEAs described in DCD Tier 2, Sections 7.2 and 7.3 demonstrate safety-related system actuation is assured in the presence of single failures in the software/hardware portions of the systems in questions. The SPM TeR describes the software engineering process for this design, which includes the development of reliable software based on design, verification, validation, testing as described in endorsed NRC standards. These endorsed standards specify criteria for high quality software design and implementation. The D3 TeR, Revision 0, describes the DAS and accompanying D3 analysis that provides a diverse means to accomplish protective functions in case of a CCF of the safety-related systems. The safety-related I&C systems also incorporate a suite of self-testing/self-diagnostic features (e.g., alarms, watchdog timers) that help ensure safety-related system operation and operator notification of hardware and software failures within the I&C platform.

The Safety System TeR, Appendix B describes the conformance of the APR1400 design to IEEE Std 7-4.3.2-2003. Appendix B, Section B.5.5.3 provides more information on design features incorporated to ensure safety-related I&C system reliability. The applicant states in this section that reliability requirements of the safety-related systems are used to establish self-diagnostics and self-testing features. The applicant commits that these features will be subjected to the same V&V requirements as the safety-related system functions. Typical self-testing functions would include:

- Memory functionality and integrity tests (e.g., PROM checksum and RAM tests).
- Computer system instruction set (e.g., calculation tests).
- Computer peripheral hardware tests (e.g., watchdog timers and keyboards).
- Communication link diagnostics (e.g., CRC checks).

The applicant states that self-testing features will be incorporated into the safety-related system design in the following ways:

- Self-testing during system startup
- Periodically during system operation
- Self-test failure reporting

With regard to system startup, the applicant states that during power up, testing is performed on processors, input/output and system memory to confirm readiness of the safety-related system itself. The complete set of self-testing is executed during startup. This serves to detect any

fatal errors prior to execution of the process loop. During this time, the WDTs remain in an actuated state, resetting automatically when processors enter into the run mode. Processors only begin run mode after completion of the initialization self-testing.

Based upon the design descriptions, along with accompanying ITAAC to verify compliance with software lifecycle design, response time testing, safety-related system self-testing functions etc., with the accompanying safety-related system FMEAs, the staff finds that the applicant has adequately demonstrated that, when implemented, APR1400 safety-related I&C systems will perform in a reliable manner. Inherent self-testing and self-diagnostic features described, when implemented, will aid in reliability by detecting and dispositioning hardware and software faults while alerting operators to existence of faults in the safety-related I&C systems. Safety system FMEAs demonstrate that safety functions will perform their required functions in the presence of failures of varying types within portions of the safety-related I&C system. As such, the staff finds the APR1400 I&C design adequately meets the requirements of IEEE Std 603-1991, Clause 5.15.

7.1.4.21 Diversity and Defense-in-Depth

10 CFR Part 50, Appendix A, GDC 22 requires, in part, that design techniques, such as functional diversity or diversity in component design and principles of operation be used to the extent practical to prevent loss of the protective function.

DCD Tier 2 Section 7.1.2.24, "Conformance with GDC 22" states, "[t]he I&C systems that are applicable to GDC 22, as shown in Table 7.1-1, are designed in accordance with GDC 22. The protection systems comply with the independence requirements of IEEE [Std] 603 except for the CEA position inputs described in [Section] 7.1.2.3."

The staff finds that the applicant did not describe the design techniques (e.g., functional diversity and other design techniques) that are used to prevent loss of the protection function. As such, the staff requested in RAI 43-7887, Question 07.01-15, for the applicant to modify the FSAR to include this information. In the September 24, 2015 response to this RAI (ML15267A764), the applicant proposed to revise DCD Tier 2 Section 7.1.2.24 to state: "The conformance to the requirements of IEEE Std 603 and GDC 22 regarding independence and functional diversity is described and provided in Sections 7.2.2.3 and 7.3.2.3 as well as in Section 4.1 of Safety I&C System [TeR]." The staff finds this response unacceptable. Specifically, DCD Tier 2, Sections 7.2.2.3 and 7.3.2.3 of the only address independence and Section 4.1 of the Safety I&C System TeR does not discuss functional diversity. Section 4.2.2.1 of the Safety I&C System TeR does state that "Each [bistable processor] processes the bistable logic in the reverse order to that of the other [bistable processor] for software functional diversity." However, there was no definition provided for what is meant by "software functional diversity." NUREG/CR-6303, "Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems," provides guidance for meeting the requirements of GDC 22 for computer-based nuclear reactor protection systems. Section 2.6.4, "Functional Diversity, of this NUREG, states two systems are functionally diverse if they perform different physical functions though they may have overlapping safety effects. In accordance with NUREG/CR-6303, designing each bistable processor such that it processes the bistable logic in reverse order does not constitute functional diversity as the bistable processors do not have different purposes, functions, or actuation means. Also, reversing the processing order does not constitute different control logic. As such, the staff issued follow-up RAI 460-8554, Question 7.1-53, for the applicant to demonstrate how functional diversity is achieved in the design.

In the June 22, 2016, response to RAI 460-8554, Question 7.1-53 (ML16174A176), the applicant stated that the term software diversity will no longer be used in the application document. DCD Tier 2 Section 3.1.18 describes how the APR1400 design conforms to the requirements of GDC 22. The applicant proposed to modify DCD Tier 2 Section 7.1.2.24 to reference DCD Tier 2 Section 3.1.18 with respect to how the design meets the functional diversity requirements of GDC 22. Based on the proposed revisions to the FSAR to provide references in the application regarding how the design meets the requirements of GDC 22, the staff finds the applicant has resolved the issues identified in RAI 460-8554, Question 7.1-53. The verification that the proposed markups are incorporated into the next revision of the FSAR was a confirmatory item. The staff verified that the proposed markups have been incorporated into Revision 1 of DCD Tier 2 Section 7.1.2.23. As such, this confirmatory item has been satisfied.

> DCD Tier 2 Section 7.1.2.35 states, "[a]nalyses and design features for diversity and defense-in-depth for the instrumentation and control systems are provided in accordance with SECY-93-087, Item II.Q (Reference 22), as referenced by NUREG-0800, BTP 7-19 (Reference 70)."

This statement does not reference the SRM to this SECY which is the Commission's position on D3 for digital systems. As such, in RAI 43-7887, Question 07.01-16, the staff requested the applicant to clarify in the FSAR how the APR1400 I&C design conforms to the SRM to SECY-93-087, Item 18, II.Q. In the August 12, 2015 response to this RAI (ML15224B643), the applicant proposed to modify DCD Tier 2, Sections 7.1.36, 7.1.5, 1.2.16(4), 1.5.4, 1.5.5(4), 7.1.2.35, 7.3.2.4, 7.3.5(9), 7.8, 7.8.2.2, 7.8.5(2), and 18.7.2.1(g)(5), and Table 7.1-1(35), D3 TeR and the Safety I&C System TeR to reference the SRM to SECY-93-087. The applicant provided markups to these FSAR sections, and to the D3 TeR and the Safety I&C System TeR. Based on the commitment to modify the applicable FSAR sections, and the D3 TeR and the Safety I&C System TeR to reference the SRM to SECY-93-087, Item 18, II.Q, the staff finds that that the issue identified in RAI 43-7887, Question 07.01-16, is closed and resolved. The verification that the proposed markups are incorporated into the next revision of the FSAR, D3 TeR and the Safety I&C System TeR was a confirmatory item. The staff verified that the proposed markups have been incorporated into Revision 1 of DCD Tier 2, Chapters 1, 7, and 18, the D3 TeR, Revision 1, and Safety I&C System TeR, Revision 1. As such, this confirmatory item has been satisfied.

The staff evaluation on how the applicant addressed software CCF is discussed in Section 7.8 of this SER.

Based on the description of how the design provides sufficient diversity to address software CCF as described in Section 7.8.4.2.3 of this SER, the staff determined that the APR1400 I&C system design meets the diversity requirements in GDC 22 and the SRM to SECY-093-87, Item 18, II.Q.

7.1.4.22 Automatic and Manual Control

"IEEE Std 603-1991, Clause 6.1 requires that means shall be provided to automatically initiate and control all protective actions except as justified in IEEE Std 603-1991, Clause 4.5.
IEEE Std 603-1991, Clause 7.1 requires that capability shall be incorporated in the execute features to receive and act upon automatic control signals from the sense and command features consistent with IEEE Std 603-1991, Clause 4.4 of the design basis.
IEEE Std 603-1991, Clause 6.2 requires that means shall be provided in the control room to

implement manual initiation at the division level of the automatically initiated protective actions. Clause 6.2 also requires that means shall be provided in the control room to implement manual initiation and control of the protective actions identified in Clause 4.5 that have not been selected for automatic control under Clause 6.1. In addition, Clause 6.2 requires that means shall be provided to implement the manual actions necessary to maintain safe conditions after the protective actions are completed as specified in Clause 4.10. IEEE Std 603-1991, Clause 7.2 requires, in part, that capability shall be provided in the execute features to receive and act upon manual control signals from the sense and command features consistent with the design basis. GDC 20 requires the protection system to be designed to: (1) initiate automatically the operation of appropriate systems including the reactivity control systems to assure that specified acceptable fuel design limits are not exceeded as a result of AOOs, and (2) sense accident conditions and to initiate the operation of systems and components important to safety.

The guidance of SRP Appendix 7.1-C for IEEE Std 603-1991, Clause 6.1 and 7.1 indicates, in part, that the applicant's analysis should confirm that the safety-related system has been qualified to demonstrate that the performance requirements are met, and that the evaluation of the precision of the safety-related system should be addressed to the extent that setpoints, margins, errors, and response times are factored into the analysis. The guidance of SRP Appendix 7.1-C for IEEE Std 603-1991, Clause 6.2 and 7.2 states, in part, that the review of manual controls should confirm that the controls will be functional during plant conditions under which manual actions may be necessary.

The design of the APR1400 safety-related I&C system, which mainly includes the PPS and ESF-CCS, provides the functions for the automatic control (bistable logic, local coincidence logic, and circuits) in each division to initiate the required protective actions. The operator does not need to perform any action while the automatic control function is active. The PPS performs sense and command functions by automatically providing trip and actuation signals for use by the RTSS and ESF-CCS, respectively. The RTSS circuit breaker is automatically actuated when it receives the automatic reactor trip signals. The ESF-CCS automatically performs the execute functions for the ESF systems.

The safety-related I&C system is designed with means in the MCR for manual actuation at the division/system-level for automatically initiated protective actions. The manual ESF actuation switches are wired to the ESF-CCS. The manual reactor trip switches and DMA switches are provided downstream of the PPS and ESF-CCS, respectively.

For the RPS, four manual reactor trip switches (per division) are provided to permit the operator to trip the reactor. Single failure does not prevent the manual trip function from being performed properly. For the ESF systems, manual ESF system-level actuation switches are provided for each ESFAS function included in the APR1400 design. All ESF actuation signals can be manually initiated by operators using these switches from the MCR in accordance with procedures. Manual reactor trip switches and a main steam isolation system actuation switch are also provided in the RSR.

Minimum inventory switches and ESCM on the safety console are also provided as manual control means to maintain plant safe shutdown under transient and accident conditions. Minimum inventory manual switches are provided at both system-level and component-level. The minimum inventory indications and alarms are used to support the required operator actions under accident conditions.

The minimum inventory switches are designed to provide manual controls for credited safety functions. However, there is lack of design information on what the credited safety functions are for those minimum inventory switches in the application. Figure 7.3-1 in DCD Tier 2 Section 7.3 shows that both minimum inventory system-level and component-level manual switches are connected in the same way to the CPM. There is no design information in the design certification application to illustrate on how both types of minimum inventory manual switches are implemented in the same way but are used to provide manual safety functions at different levels. Figure 7.3-3 of DCD Tier 2 Section 7.3 shows both local manual and remote actuation signals. There is also lack of design information on where the local manual and remote actuation signals are originated from. The indication of minimum inventory manual switches is not consistently shown in diagrams in both Chapter 7 of DCD Tier 2 and the Safety I&C System TeR. The applicant did not describe whether there are any credited manual controls for which no automatic safety function exists. As such, the staff requested in RAI 323-8281, Questions 07.03-10 and 07.03-17 that the applicant provide adequate information as described above, so the staff could make safety findings with reasonable assurance on whether the APR1400's safety-related I&C design meets requirements in Clauses 6.1, 6.2, 7.1, and 7.2 of IEEE Std 603-1991 on automatic and manual control requirements.

In the March 15, 2016, response to RAI 323-8281, Question 07.03-10 (ML16075A425) and Question 07.03-17 (ML16075A425), the applicant states, in relevant part, that the minimum inventory switches consist of component-level and system-level minimum inventory switches on the safety console. System-level minimum inventory switches are manual ESFAS switches to initiate system-level ESFAS actuations. The system-level minimum inventory switch signals are input to the ESF-CCS group controller via the CPM, and acquired as the input of 2oo4 voting logic in the group controller. System-level actuation signals downstream of voting logic are split in ESF-CCS group controller, and each split signal is transmitted to the corresponding ESF-CCS Loop Controller via the SDL. Component-level minimum inventory switches provide manual control of the components used for safe shutdown by the MCR operators when the operator consoles are not available. The signals from the component-level minimum inventory switches are input to the loop controller via the CPM and CCG, and acquired as the input of component logic in the loop controller. In addition, the applicant revised Figures 7.1-43, 7.3-1, and 7.9-1 in DCD Tier 2, and Figures 4-13 and 4-28 in the Safety I&C System TeR to incorporate the additional design information provided in the RAI responses. The staff finds that the design information in the FSAR and its referenced technical reports and the additional information in the RAI responses are adequate and acceptable to meet the regulatory requirements on automatic and manual control in Clauses 6.1, 6.2, 7.1, and 7.2 of IEEE Std 603-1991, and GDC 20. The incorporation of the proposed markup into the next revision of FSAR and the Safety I&C System TeR was a confirmatory item. The staff verified that the proposed changes have been incorporated into Revision 1 of DCD Tier 1, Sections 7.1, 7.3, 7.9 and the Safety I&C System TeR. As such, this confirmatory item has been satisfied.

7.1.4.23 Operating Bypass

The staff reviewed the APR1400 application to determine whether IEEE Std 603-1991, Clause 6.6, "Operating Bypasses," and Clause 7.4, "Operating Bypass," design criteria has been adequately addressed. These requirements state, in part, that whenever the applicable permissive conditions are not met, a safety-related system shall automatically prevent the activation of an operating bypass or initiate the appropriate safety function(s) and that if plant conditions change so that an activated operating bypass is no longer permissible, the safety-related system shall automatically remove the appropriate active operating bypass. The guidance of SRP Appendix 7.1-C, Section 6.6, "Operating Bypasses," states that the

requirement for automatic removal of operational bypasses means that reactor operator shall have no role in such removal. DCD Tier 1, Section 2.5.1.1, “Design Description,” and Table 2.5.1-4, “Reactor Trip System and Engineered Safety Features Initiation Bypasses,” and DCD Tier 2 Section 7.2.1.6, “Bypasses,” Section 7.3.1.5, “Bypasses,” Table 7.2-1, “Reactor Protection System Operating Bypass Permissive,” and Table 7.3-1, “ESFAS Operating Bypass Permissive,” list and describe the safety-related system operating bypasses. The staff reviewed the design descriptions of the operating bypasses, the functional logic operating bypass diagrams provided in DCD Tier 2, Revision 0, Section 7.2, and the listing of the operating bypasses in the above listed FSAR tables. The staff found that all listed operating bypasses have an operating bypass setpoint (i.e., preset field parameter value) that, if plant conditions exceed the operating bypass setpoint, the safety-related system would automatically remove the applicable operating bypass without operator action. However, the staff was not able to identify in DCD Tier 1 Table 2.5.1-4, “Reactor Trip System and Engineered Safety Features Initiation Bypasses,” a listing for the ESFAS operating bypass for the operating bypass function to disable the low pressurizer pressure actuation for SIAS and CIAS. The staff issued RAI 272-8313, Question 07.02-14 to request the applicant to update DCD Tier 1 Table 2.5.1-4, with the applicable Tier 2 Table 7.3-1, operating bypass information. In the December 11, 2015, response to this RAI (ML15345A357), the applicant provided an FSAR mark-up updating Tier 1 Table 2.5.1-4, with the requested information. The staff finds this response is acceptable. The staff verified that the proposed markups have been incorporated into Revision 1 of DCD Tier 1 Table 2.5.1-4. As such, this confirmatory item has been satisfied.

In addition, the Safety I&C System TeR, Section A.7.4, “Operating Bypass,” states that the operating bypasses have automatic features that provide a permissive range at which they can be actuated. While plant conditions are within this range, the operator can manually initiate an operating bypasses. If the operating bypass permissive range is exceeded, the operating bypass is automatically removed.

Based on the design descriptions regarding how operating bypasses are automatically removed in the APR1400 safety-related I&C systems, the staff concludes that the operating bypass design meets the automatic bypass removal requirements of IEEE Std 603-1991, Clauses 6.6 and 7.4.

7.1.4.24 Maintenance Bypass

The staff reviewed the APR1400 design certification application to determine whether IEEE Std 603-1991, Clauses 6.7 and 7.5 on maintenance bypass requirements have been adequately addressed. In Clauses 6.7 and 7.5 it states, in part, that the capability of a safety-related system to accomplish its safety function shall be retained while sense and command and execute features equipment is in maintenance bypass. During such operation, the features shall continue to meet the requirements of IEEE Std 603-1991, Clauses 5.1 and 6.3. The guidance of SRP Appendix 7.1-C states that the review of bypass and removal from operations requirements should be coordinated with the organization responsible for reviewing Technical Specification format and content to confirm that the provisions for this bypass are consistent with the required actions of the proposed plant Technical Specifications.

The APR1400 PPS, which consists of the RPS and ESFAS initiation systems, is designed to permit an inoperable channel to be placed in a bypass condition for the purpose of troubleshooting or periodic testing of a redundant channel. If the PPS channel has been bypassed for any purpose, a signal is provided to allow this condition to be continuously indicated in the MCR.

The APR1400 PPS supports maintenance activities, such as periodic maintenance, instrument loop testing, troubleshooting, etc. Access to features beyond displaying data such as the maintenance bypass will be under administrative and physical controls. These activities will be performed in accordance with site-specific administrative (procedural) and physical-access controls to set and/or change addressable constants, setpoints, and testing while the channel is in bypass mode. Such procedures would require manipulation of the functional enable key switch. The bypasses are always set manually as there are no automatic bypass provisions for maintenance bypasses for the APR1400 PPS.

The RPS and ESFAS parameters can be bypassed for maintenance. When one channel is in a bypass mode, the coincidence logic in the LCL voting logic of the PPS is changed from 2oo4 to 2oo3 voting logic. The bypass of one channel for the BOP ESFAS changes from one-out-of-two logic to one-out-of-one voting logic. The administrative procedure prohibits more than one channel from being placed in a bypass mode.

However, there is no design information on how the LCL would be changed when one channel is put in bypass mode while another channel fails at the same time. Also, the staff found that it was not clear in the application where the bypass mode would be set and re-set for a channel. In addition, in DCD Tier 2 Section 7.3, 1oo2 voting logics is used for some BOP ESFAS systems, such as FHEVAS, but there is no design information found in the application to justify exceptions to criteria in Clauses 5.1, 6.3, and 6.7 of IEEE Std 603-1991. As such, the staff requested in RAI 323-8281, Questions 07.03-6 and 07.03-7, for the applicant to provide additional information and justification for its maintenance bypass design for the APR1400 safety-related I&C system.

In the April 25, 2016, response to RAI 323-8281, Question 07.03-6 (ML16116A402), the applicant states, in relevant part, that the safety-related portion of the I&C system for the FHEVAS has the required redundancy to meet the single failure criterion of Clause 5.1 of IEEE Std 603-1991. Having two divisions of initiating FHEVAS ensures that if there is a loss of safety-related I&C equipment that takes one safety division out of service, the other safety division will remain in service to perform the required ESFAS initiation. The safety-related portion of the FHEVAS I&C system is designed as Class 1E, seismic Category I, and remains functional during and following a safe shutdown earthquake. Controls, interlocks, sensors, and devices of the safety-related I&C system for FHEVAS are also functionally checked, adjusted, and tested to provide reasonable assurance of intended operation and performance.

In the March 4, 2016 response to RAI 323-8281, Question 07.03-7 (ML16064A060), the applicant also states, in part, that the resulting voting logic would become 1oo2 if the single failure of one channel causes a spurious channel trip condition while another channel is placed in bypass mode. However, the resulting voting logic would become 2oo2 if a single failure does not cause a spurious channel trip condition while another channel is placed in bypass mode. In addition, if a bypass is applied to one channel where a single failure has occurred to avoid spurious reactor trip and ESF initiation due to that channel, the voting logic would become 2oo3. If the bypass is not applied to the channel experiencing a single failure, then the resulting voting logic would remain as 2oo4, if the single failure does not cause a spurious trip condition. However, the resulting voting logic would become 1oo3 if the single failure causes a spurious trip condition.

In the September 19, 2016, supplemental response to RAI 323-8281, Question 07.03-7 (ML16263A434), the applicant further clarified that a single failure of one channel normally occurs in either side of the two redundant PPS cabinets within one channel. If a single failure

occurs in one PPS cabinet of that channel and does not cause a spurious trip condition, then the resulting voting logic would remain as 2oo3 while another channel is placed in bypass because the other PPS cabinet of the channel with the single failure is capable of performing its safety function.

The applicant also clarified in the above RAI responses that both the maintenance bypass and channel bypass are implemented on the MTP. Trip channel bypass is activated by a hardwired channel bypass switch on the MTP switch panel. Channel bypass switches on the MTP switch panel in the MTP/ITP cabinet are connected to the bistable processor digital input module. The applicant proposed to revise Section 7.3.1.3 of DCD Tier 2, and Sections 4.2.2.1 and A.6.7 of the Safety I&C System TeR to include the additional design information provided in the RAI responses.

Based on the proposed changes to the FSAR and the Safety I&C System TeR, the staff finds that the issues identified in RAI 323-8281, Questions 07.03-6 and 07.03-7 are closed and resolved. The staff also finds that the additional information in the RAI responses combined with the design descriptions in the FSAR and its referenced technical reports provide sufficient information on how the regulatory requirements in Clauses 5.1, 6.3, and 6.7 of IEEE Std 603-1991 are met for the APR1400 I&C design. The staff verified that the proposed changes have been incorporated into Revision 1 of DCD Tier 1, Section 7.3.1.3 and the Safety I&C System TeR, Sections 4.2.2.1 and A.6.7. As such, this confirmatory item has been satisfied.

7.1.4.25 Setpoints

In support of the APR1400 DCA, the applicant submitted Setpoint Methodology TeR, Revision 1 and modified the title of this TeR to “Setpoint Methodology for Safety-Related Instrumentation.” This technical report documents the methodology used in the PPS and DPS, “to ensure that the PPS and DPS setpoints are consistent with the assumptions made in the safety analysis and conform to current licensing requirements and industry standard.”

In addition, the applicant submitted APR1400-F-C-NR-14001, Revision 1, “CPC Setpoint Analysis Methodology for APR1400” (hereafter referred to as CPC Setpoint Analysis Methodology TeR). To be used for the setpoint calculations for DNBR and LPD reactor trips.

The following regulatory requirements and guidance documents are applicable to the staff’s review of Setpoint Methodology TeR and CPC Setpoint Analysis Methodology TeR.

7.1.4.25.1 Regulatory Basis

1. 10 CFR Part 50, Appendix A.

2. GDC 13, “Instrumentation and Control,” requires, in part, that instrumentation be provided to monitor variables and systems over the anticipated ranges for, normal operation, for AOOs, and for accident conditions as appropriate to assure adequate safety, and that appropriate controls be provided to maintain these variables and systems within prescribed operating ranges.

3. GDC 20, “Protection System Functions,” requires, in part, that the protection system be designed to initiate operation of appropriate systems to ensure that specified acceptable fuel design limits are not exceeded as a result of AOOs.

4. 10 CFR Part 50, Appendix B, Criterion XI, “Test Control,” and Criterion XII, “Control of Measuring and Test Equipment,” provide requirements for tests and test equipment used in maintaining instrument setpoints.

5. 10 CFR 50.36(c)(1)(ii)(A) requires, in part, that if a limiting safety system setting (LSSS) is specified for a variable on which a safety limit has been placed, the setting be chosen so that automatic protective action will correct the abnormal situation before a safety level is exceeded. LSSSs are settings for automatic protective devices related to variables with significant safety functions. Additionally, 10 CFR 50.36(c)(1)(ii)(A) requires that a licensee take appropriate action if it is determined that the automatic safety-related system does not function as required.

6. 10 CFR 50.36(c)(3), “Technical Specifications,” states that surveillance requirements are requirements relating to, test, calibration, or inspection to assure that the necessary quality of systems and components is maintained, that facility operation will be within safety- limits, and that the limiting conditions for operation will be met.

7. 10 CFR 50.55a(h)(3), “Safety Systems,” requires compliance with IEEE Std 603-1991, “IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations,” and the correction sheet dated January 30, 1995. Section 4.4 of IEEE Std 603-1991 requires identification of the analytical limit associated with each variable. Section 6.8.1 of IEEE Std 603-1991 requires that allowances for uncertainties between the analytical limit of the safety-related system and device setpoints be determined using a documented methodology. Section 6.8.2 of IEEE Std 603-1991 requires that for processes which may be subject to multiple setpoints, the design shall provide positive means of ensuring that the more restrictive setpoint is used when required.

7.1.4.25.2 Relevant Guidance

1. RG 1.105, Revision 3, “Setpoints for Safety-Related Instrumentation,” provides guidance for ensuring that instrument setpoints for safety instrumentation are initially - and remain - within the technical specification limits. This RG endorses ISA-S67.04-1994, Part I, “Setpoints for Nuclear Safety-Related Instrumentation,” with clarifications.

2. ISA-S67.04-1994, Part II, “Methodology for the Determination of Setpoints for Nuclear Safety-Related Instrumentation,” provides additional guidance, however, RG 1.105, Revision 3, does not endorse or address Part II of ISA-S67.04-1994.

3. In SRP BTP 7-12, there are guidelines for reviewing the process an applicant/licensee follows to establish and maintain instrument setpoints.

4. NRC Regulatory Issue Summary (RIS) 2006-17, “NRC Staff Position on the Requirements of 10 CFR 50.36, ‘Technical Specifications,’ Regarding Limiting Safety System Settings during Periodic Testing and Calibration of Instrument Channels,” discusses issues that could occur during testing of LSSSs and which therefore, may have an adverse effect on equipment operability.

5. Generic Letter 91-04, Enclosure 1, “Guidance on Preparation of a License Amendment Request for Changes in Surveillance Intervals to Accommodate a 24-Month Fuel Cycle,” provides guidance on issues that should be addressed by the setpoint analysis when

calibration intervals are extended from an 18-month or other refueling outage interval to 24 months.

6. Technical Specification Task Force Traveler 493, Revision 4, “Clarify Application of Setpoint Methodology for LSSS Functions.”

7.1.4.25.3 CPC Setpoint Analysis Methodology TeR

The safety setpoints that are generated by the CPC Setpoint Analysis Methodology TeR are required to meet the guidance provided by RG 1.105, Revision 3. The evaluation for the CPC Setpoint Analysis Methodology TeR is provided in Section 4.4 of this SER. The staff agrees that the data points described in Sections 2.1.1 and 2.1.2 would conform to the 95/95 probability/confidence value as described in RG 1.105, Revision 3. However, Section 2.1.3, Equation 2.3, uses a one-sided tolerance limit factor (k) of 1.645 as part of the calculation. The staff issued RAI 301-8280, Question 07.01-45, to inquire about this tolerance limit factor and the conformance to RG 1.105, Revision 3. In the December 28, 2015, response to this RAI (ML15362A593), the applicant did not demonstrate that the methodology conforms to the 95/95 probability/confidence value as described in RG 1.105, Revision 3.

At the May 2016 APR1400 I&C meeting (see ML16113A319 for the meeting notice), the applicant also notes that this methodology has been previously documented and approved by the staff in CEN-283(S)-P, “Statistical Combination of Uncertainties Part 2,” October 1984. This document is listed as a reference in the CPC Setpoint Analysis Methodology TeR. Based on the discussions during the Chapter 4 audit (ML16060A413) held on January 20 - 21, 2016, and the supplemental response to RAI 328-8422, Question 04.04-8 (ML16216A631), the axial power shape is evaluated in a process known as annealing to estimate the axial power shape on the core periphery based on the three axial measurements from each of the three ex-core detectors. Likewise, approximately 4800 pre-calculated operating conditions are evaluated for each cycle to determine the radial peaking factor (Fxy), which is largely a function of rod position. During startup testing, the value of Fxy is measured and compared to a calculation at that burnup. A penalty factor is subsequently calculated and applied for the rest of the cycle to correct the estimated Fxy and ensure that the 3-D peaking factor remains conservative. The number of cycle-specific operating cases considered and the penalty factor calculated during startup testing provides a large sample size for pre-calculated operating conditions and therefore, provides a solid basis for the data points conforming to the 95/95 probability/confidence value. However, the responses did not demonstrate using 1.645 conformance to the 95/95 probability/confidence value as described in RG 1.105, Revision 3. Additional clarification is needed in the CPC Setpoint Analysis Methodology TeR.
RAI 301-8280, Question 07.01-45, was tracked as an open item. In the supplemental response to RAI 301-8280, Question 07.01-45 (ML17214A218), the applicant stated that the CPC setpoint analysis methodology described in the CPC Setpoint Analysis Methodology TeR is identical to CEN-283(S)-P, which has been previously evaluated and approved by the staff. Additionally, the applicant stated that it has followed the methodology for determining setpoints for safety instrumentation as described in RG 1.105, Revision 3, with the exception of the 95/95 tolerance limit. As such, DCD Tier 2 is revised to denote that the setpoint calculations using the CPC Setpoint Analysis Methodology TeR does not meet RG 1.105, Revision 3. The staff finds that the RAI response to Table 1.9-1 column, “Conformance or Summary Description of Deviation,” adequately clarifies that the setpoints calculated by the CPC TeR do not meet the guidance of RG 1.105, Revision 3. The revisions to the TeR from the RAI response are evaluated in Section 4.4 of this SER and found acceptable. For these reasons, the staff finds the proposed changes to CPC Setpoint Analysis Methodology TeR and DCD Tier 2 in RAI 301-8280,

Question 07.01-45, are acceptable. The incorporation of the proposed markups into the next revision of the TeR was a confirmatory item. The staff verified that the proposed markups have been incorporated into Revision 2 of DCD Tier 2 and Revision 2 of the CPC Setpoint Methodology TeR. As such, this confirmatory item has been satisfied. In supplemental responses to RAI 301-8280, Question 07.01-45 (ML18145A081) and (ML18184A365), the applicant added CEN-308-P-A, "CPC/CEAC Software Modifications for the CPC Improvement Program" to the CPC TeR as a reference, added a note to Table 15.0-2 that clarifies that the setpoints calculated by the CPC TeR do not meet the guidance of RG 1.105, Revision 3, and revised Table 1.9-1 column, "DCD Tier 2 Section," to delete 15.0.0.9 and add Table 15.0-12. The staff verified that the proposed markups have been incorporated into Revision 3 of DCD Tier 2, and Revision 3 of the CPC Setpoint Methodology TeR. As such, this confirmatory item has been satisfied.

The staff reviewed the information submitted by the applicant and concluded with reasonable assurance, that the applicant provided sufficient information in the APR1400 CPC Setpoint Analysis Methodology TeR to demonstrate that the requirements in 10 CFR Part 50, Appendix A, GDC 13 and 20, of 10 CFR Part 50, Appendix B, Criterion XI, of 10 CFR 50.36(c)(1)(ii)(A) and 10 CFR 50.36 (c)(3), and of 10 CFR 50.55a(h)(3), which requires compliance with IEEE Std 603-1991, are met.

7.1.4.25.4 Setpoint Methodology TeR

The objectives of the staff's review of the Setpoint Methodology TeR are to (1) verify that setpoint calculation methods are adequate to assure that protective actions are initiated before the associated plant process parameters exceed their analytical limits, (2) verify that setpoint calculation methods are adequate to assure that control and monitoring setpoints are consistent with their requirements, and (3) confirm that the established calibration intervals and methods are consistent with safety analysis assumptions. The staff evaluated the setpoint methodology using SRP BTP 7-12 to verify conformance with the previously cited regulatory bases and standards for instrument setpoints with emphasis on the following:

1. Relationships between the safety limit, the analytical limit, the limiting trip setpoint, the allowable value, the setpoint, the acceptable as-found band, the acceptable as-left band, and the setting tolerance.

2. Setpoint technical specifications meeting the requirements of 10 CFR 50.36. Additional information related to setpoint technical specifications is provided in RIS 2006-17.

3. Basis for selection of the trip setpoint.

4. Uncertainty terms that are addressed.

5. Method used to combine uncertainty terms.

6. Justification of statistical combination.

7. Relationship between instrument and process measurement units.

8. Data used to select the trip setpoint, including the source of the data.

9. Assumptions used to select the trip setpoint (e.g., ambient temperature limits for equipment calibration and operation, potential for harsh accident environment).

10. Instrument installation details and bias values that could affect the setpoint.

11. Correction factors used to determine the setpoint (e.g., pressure compensation to account for elevation difference between the trip measurement point and the sensor physical location).

Instrument test, calibration, or vendor data, as-found and as-left; for each instrument should be demonstrated to have random drift by empirical and field data. Evaluation results should be reflected appropriately in the uncertainty terms, including the setpoint methodology.

Evaluation

The applicant's setpoint methodology describes the establishment of setpoints and the relationships between draft trip setpoint (DTSP), trip setpoint (TSP), allowable value, analytical limit, and safety limit.

The safety limits are chosen to protect the integrity of physical barriers that guard against the uncontrolled release of radioactivity. The safety limits are typically provided in the plant safety analyses.

The analytical limit is established to ensure that the safety limit is not exceeded. The analytical limits are developed from event analyses models that consider parameters such as process delays, rod insertion times, reactivity changes, analysis margin, transient response, modeling error, instrument response times, etc. and are provided in Chapter 15, "Transient and Accident Analysis," of the FSAR of this application. A properly established setpoint initiates a plant protective action before the process parameter exceeds its analytical limit. This, in turn, assures that the transient will be, avoided and/or terminated before the process parameters exceed the established safety limits. IEEE Std 603-1991, Clause 4.4 is evaluated in Section 7.1.4.4 of this SER.

The Setpoint Methodology TeR is based on following the requirements of RG 1.105, Revision 3, which describes a method acceptable to the NRC for complying with the applicable regulations. The Setpoint Methodology TeR follows ISA-S67.04-1994, Part I as endorsed by RG 1.105, Revision 3. The Setpoint Methodology TeR also follows the recommended practices of ISA-S67.04-1994, Part II, which is provided in the Uncertainty Methodology TeR, as referenced in Section 4.7 of this Setpoint Methodology TeR. Although not endorsed by the NRC, these recommended practices are well understood by the staff and are considered a reasonable approach to implement the guidance of ISA-S67.04-1994, Part I, to establish safety setpoint calculations.

The Uncertainty Methodology TeR, as referenced in Section 4.7 of the Setpoint Methodology TeR, Response Time Analysis TeR, as referenced in Section 4.8 of the Setpoint Methodology TeR, and the CPC Setpoint Analysis Methodology TeR, Revision 1, as referenced in Section 4.9 of the Setpoint Methodology TeR may be reviewed as part of the safety evaluation of the Setpoint Methodology TeR. However, no safety finding is made on these references in this section of the SER.

The relationships among DTSP, TSP, allowable value, and analytical limit were not clear to the staff as described in Section 2.1 of the Setpoint Methodology TeR. In addition, there were

inconsistencies between the figures and descriptions in the Setpoint Methodology TeR and a clear understanding of allowable value and the margin that separates allowable value and TSP. The staff issued RAI 34-7870, Question 07.01-1, to request the applicant to clarify relationships among these variables. In the July 14, 2015, response to this RAI (ML15195A451), the applicant proposed to update the Setpoint Methodology TeR to correct an error in a reference to the DTSP and stating, "the allowable value is less conservative than the TSP by an offset which is greater than the PPS cabinet periodic test error." However, the response did not satisfactorily resolve all of the staff's concerns and therefore, instead of a supplemental question to this RAI, the staff closed this RAI and created a new RAI. The staff issued a follow up RAI 301-8280, Question 07.01-41, stating why the previous RAI was closed as discussed above, and to propose performing an audit of setpoint methodology related documents, implementation procedures, and example actual setpoint calculation documentation, along with holding discussions with an instrumentation setpoint methodology specialist representative from the applicant, as a means to expedite obtaining needed clarification of the Setpoint Methodology. In the April 22, 2016, response to RAI 301-8280, Question 07.01-41 (ML16113A458), the applicant stated, in part,

> The final TSP is offset in a conservative direction from the calculated [allowable value] by approximately 0.5% of the channel span, which is sufficiently greater than the PPS cabinet periodic test error. This approach can reduce the possibility of a licensee event report being required when a periodic test result exceeds the [allowable value].

At the May 2016 APR1400 I&C meeting, the staff provided feedback and requested the applicant to justify using 0.5 percent of channel span as the margin between the DTSP and the TSP to ensure the analytical limit is not exceeded and to justify why the other devices in the loop are not considered when evaluating allowable value. Also, the staff requested the applicant to remove any mention of event reports or reportable events from the FSAR. In the June 24, 2016, supplemental response to RAI 301-8280, Question 07.01-41 (ML16176A382), the applicant stated, in part, "reference to reducing the possibility of 'a licensee event report' will be changed to reducing the possibility that a periodic test result exceeds the allowable value to focus on the setpoint methodology rather than the administrative result." The proposed markups address the staff's concern regarding removing event reporting language. However, the applicant has not fully addressed the staff's concern regarding the 0.5 percent of the channel span as the margin to ensure analytical limit is not exceeded. Staff will be requesting that the applicant better document the basis for choosing the value of the "Offset" from the allowable value (according to the APR1400 setpoint methodology, for digital channels, this has the same value as the DTSP [i.e., the limiting trip setpoint (LTSP)]) to establish the TSP (i.e., the nominal trip setpoint (NTSP)). For example, it was not clear if the offset takes into consideration the as-found tolerance (AFT) bands of the transmitter and the APC-S.

Based on the example calculation, it appears to the staff that the Offset (0.5 percent of the span) does not include or account for the transmitter Periodic Test Error and the APC-S Periodic Test Error (i.e., the AFT). The applicant's response did not satisfactorily resolve all of the staff's concerns. Therefore, RAI 301-8280, Question 07.01-41, was tracked as an open item. In the supplemental response to RAI 301-8280, Question 07.01-41 (ML17261A455), the applicant provided a revised Setpoint Methodology TeR to demonstrate conformance to the guidance of RG 1.105, Revision 3. The evaluation of this TeR is provided below. Additionally, this Setpoint Methodology TeR closes the following RAIs; RAI 34-7870, Question 07.01-6; RAI 301-8280, Question 07.01-48; RAI 301-8280, Question 07.01-49; RAI 301-8280, Question 07.01-50; and RAI 301-8280, Question 07.01-51. The staff finds the proposed

changes to the Setpoint Methodology TeR in RAI 301-8280, Question 07.01-41, are acceptable. The incorporation of the proposed markups into the next revision of the TeR was a confirmatory item. The staff verified that the proposed markups have been incorporated into Revision 2 of the Setpoint Methodology TeR. As such, this confirmatory item has been satisfied.

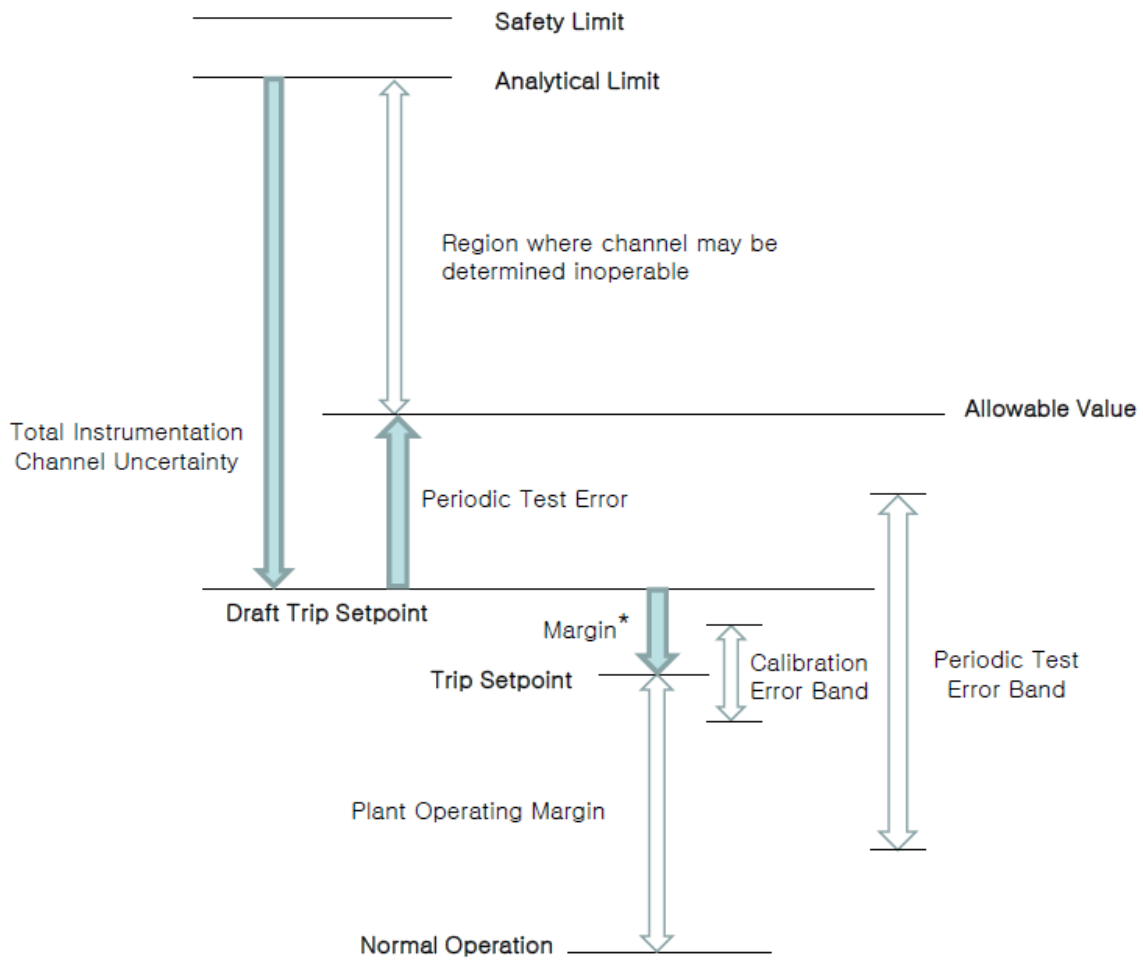

Figure 1. Nuclear safety setpoint relationships for rising trip

Note: The evaluation below shows equations with plus or minus (+/-) to reflect setpoint in both directions. Plus values for lowering setpoints and minus values used for rising setpoints. Equations are shown in Appendix A of the Setpoint Methodology TeR.

Section 2.4.2 of the Setpoint Methodology TeR defines DTSP as the LSSS and also defines TSP as the desired value of the measured variable at which an actuation occurs. The calculation of the DTSP = analytical limit+/- total instrumentation channel uncertainty (TLU), where TLU is the total channel uncertainty.

The TSP includes additional margin such that it is more conservative than the DTSP. TSP = DTSP +/- Margin. Margin is determined by engineering judgement.

Sections 2.3.2.1 and 2.3.2.2 of the Setpoint Methodology TeR describe how the channel calibration error (i.e., as-left tolerance (ALT)) and channel periodic test error (AFT) are derived

for use in the setpoint calculation for the transmitter and signal conditioning device for each loop. Sections 2.3.2.5 and 2.3.2.6 of Setpoint Methodology TeR describe how the safety-related system cabinet calibration error (ALT) and safety-related system cabinet periodic test error (AFT) is derived for the safety-related system cabinet.

Section 2.4.3 of Setpoint Methodology TeR describes allowable value as less conservative than DTSP, by the amount of the total +/- AFT of the loop (transmitter, signal conditioning device, and safety-related system cabinet) which is shown as periodic test error on Figure 1. Allowable value = DTSP (most conservative SP) +/- AFT Total (Appendix A). Allowable value is defined as a limiting value that the trip setpoint may have when tested periodically, beyond which appropriate action shall be taken. Total +/- ALT and total +/- AFT for the loop is shown as Calibration Error Band and Periodic Test Error Band around the Trip Setpoint as shown on Figure 1. These values are used as part of the steps listed in Section 2.1 of Setpoint Methodology TeR to verify instrument operability as provided in the guidance of RIS 2006-17.

The staff finds that this approach is consistent with the guidance in RG 1.105, Revision 3, ISA-S67.04, Part 1-1994, and RIS 2006-17.

Based on the discussion in Section 2.4.3 of the Setpoint Methodology TeR, sample calculation in Appendix A, and Figure 1 presented in the Setpoint Methodology TeR, the staff finds that the applicant setpoint methodology demonstrates that the correct relationships between the safety limit, analytical limit, periodic test error (i.e., allowable value)), DTSP, TSP, calibration error band (ALT), and periodic test error band (AFT) will be ensured, that the basis for the trip setpoint is correct, and that the requirements of GDC 13 and 20 are met.

The applicant's setpoint methodology allows for a minimum set of assumptions to be used as referenced in Appendix B of the Setpoint Methodology TeR. This minimum set of assumptions will yield conservative uncertainties used in the calculations and less chance of error during calibration of instrument channels, which the staff finds reasonable and acceptable.

As described in Section 2.5.1 of the Setpoint Methodology TeR, the results of the calculation are documented in accordance with controlled plant procedures and programs (such as the Setpoint Control Program) with adequate detail so that all bases, equations, and conclusions are fully understood and documented.

The surveillance and calibration intervals are established in accordance with the reference technical specifications contained in Chapter 16 of DCD Tier 2 as documented in Section 3.2 of the Setpoint Methodology TeR. Surveillance and calibration intervals takes into account the uncertainty due to instrument drift as described in this report such that there is reasonable assurance that the PPS instrumentation is functioning as expected between the surveillance intervals. Plant-specific procedures will include the required methods to evaluate the historical performance of the drift for each instrument channel and confirm that the surveillance and calibration intervals do not exceed the assumptions in the plant safety analysis. For these reasons the staff finds that the setpoint methodology conforms to ISA-S67.04, Part 1-1994 and RG 1.105, Revision 3 with respect the assumptions and data used to determine the uncertainties and select the trip setpoint.

The setpoint methodology combines the uncertainty of the instrument loop components to determine the TLU for the functions for any safety instrument channel that requires a setpoint calculation (e.g., reactor trip functions and the ESFAS setpoints). All appropriate and applicable uncertainties are to be considered for components that support the setpoint function. As stated

in Section 2.1 of the Setpoint Methodology TeR and Appendix A, include a list of uncertainties for calculating the TLU, that are considered typical, but not inclusive, and the list is consistent with ISA-S67.04-1994, Part 1. Other considerations that contribute to the uncertainty, such as environmental conditions and installation details of the components are also factored into the TLU are described in the Setpoint Methodology TeR, with additional clarifications described in Sections 4 and 5 of the Uncertainty Methodology TeR. For these reasons, the staff finds that the setpoint methodology conforms to ISA-S67.04-1994, Part 1 and RG 1.105, Revision 3 with respect to uncertainty terms, bias values, and correction factors used to select the trip setpoint.

The TLU values are established at a 95 percent probability and a 95 percent confidence level, using a 2 sigma Gaussian distribution which is consistent with RG 1.105, Revision 3. The TLU value is based on the following:

- Characteristics of uncertainties and how they are combined are described in described in Sections 3, 6 and 7 of the Uncertainty Methodology TeR and are generally shown below:

- Random, independent uncertainties are eligible for the square-root-sum-of-squares method (SRSS) combination propagated from the process measurement module through the signal conditioning module of the instrument channel to the device that initiates the actuation.

- Dependent uncertainties are combined algebraically to create a larger independent uncertainty that is eligible for SRSS combination.

- Non-random, bias and abnormally distributed uncertainties are those that consistently have the same algebraic sign. If they are predictable for a given set of conditions because of a known positive or negative direction, they are classified as bias with a known sign. If they do not have a known sign, they are treated conservatively by algebraically adding the bias to the TLU of interest (negative bias for increasing setpoints and positive bias for decreasing setpoint). These are classified as bias with an unknown sign.

The staff finds that the described method of statistical combination of uncertainties conforms to ISA-S67.04-1994, Part 1, Section 4 and to RG 1.105, Revision 3.

The equations shown Appendix A of the Setpoint Methodology TeR for determining module and channel uncertainty, and trip setpoint conform to ISA-S67.04-1994, Part 1 and to RG 1.105, Revision 3.

Based on the discussion above, the staff finds that Setpoint Methodology TeR follows the guidance of RG 1.105, Revision 3, RIS 2006-17, and ISA-S67.04-1994, Part 1 with respect to setpoint methodology and therefore complies with IEEE Std 603-1991, Clause 6.8.1 for ensuring that setpoints for safety instruments are initially within and remain within the technical specification limits.

In RAI 34-7870, Question 07.01-4, the staff asked the applicant to describe how the offset between the TSP and the allowable value is determined, and to clarify the relationship between the terms margin and offset. In the July 14, 2015, response to this RAI (ML15195A451), the applicant responded by stating,

> In order to reduce the possibility of a license event report, the final TSP would be offset from the [allowable value] by about 0.5 percent of span that applied for the Korean nuclear power plants in service. The offset used...is based on engineering judgement...the offset is greater than the PPS cabinet periodic test error...this approach does not affect the safety aspect since the final TSP is moved in the conservative direction by reducing the plant operating margin.

Although the applicant's response provided new information, the applicant did not propose to update the DCD Tier 2 or the Setpoint Methodology TeR with this information. Regarding the new information, the applicant was requested to provide a technical basis as to why a 0.5 percent of span provides adequate margin between the TSP and the allowable value for all specified automatic reactor trip and safety-related system actuation instrumentation functions. Instead of a supplemental question to this RAI, the staff closed this RAI and created a new RAI. RAI 34-7870, Question 07.01-4, is closed. The staff issued a follow up RAI 301-8280, Question 07.01-50, to request the applicant to add the new information to Setpoint Methodology TeR, and to add a description of the basis or rationale for the stated offset value to DCD Tier 2 or to the Setpoint Methodology TeR. In the April 22, 2016 response to RAI 301-8280, Question 07.01-50 (ML16113A458), the applicant stated, in part,

> To describe the basis for the stated offset, Section 2.5.4, “Drift Allowance” of [the Setpoint Methodology TeR] will be revised as follows: To prevent a licensee event report, the TSP is offset in a conservative direction from the calculated [allowable value] by a drift allowance of about 0.5% of the channel span, which is sufficiently greater than the PPS cabinet periodic test error. Since the PPS cabinet periodic test error is used in determining the [allowable value] from the DTSP, the drift allowance does not consider the sensor and the APC-S periodic test errors, which are individually verified to be within their respective periodic test error bands. Historically, the 0.5% of channel span value is larger than the value of the PPS cabinet periodic test error. Because the PPS cabinet periodic test error is the difference of the DTSP and the [allowable value], the approach results in a TSP which is reasonable. This approach does not negatively affect safety since the TSP is moved in the conservative direction by reducing the plant operating margin.

At the May 2016 APR1400 I&C public meeting, the applicant agreed to remove any mention event reports or reportable events from the FSAR, and to justify using 0.5 percent of channel span as the margin between the DTSP and the TSP and provide justification to ensure the analytical limit was not exceeded during fuel cycle resulting from the surveillance of sensor and APC-S. The June 24, 2016, supplemental response to RAI 301-8280, Question 07.01-50 (ML16176A382), along with the response outlined in RAI 301-8280, Question 07.01-41 evaluated above, did not satisfactorily resolve all of the staff’s concerns. Therefore, RAI 301-8280, Question 07.01-50, was tracked as an open item. All outstanding issues are addressed in the final draft TeR for the APR1400’s setpoint methodology and the staff’s evaluation of the response to RAI 301-8280, Question 07.01-41. As such, RAI 301-8280, Question 07.01-50, is closed.

The TSP is derived from the analytical limit by subtracting or adding the safety margin and the TLU, depending on the direction of process variable change when approaching the analytical limit. The TLU is the combined uncertainties of all instruments within the loop. The safety margin is established in order to assure that TSP are always smaller than or equal to the allowable value. As discussed in RIS 2006-17, if the as-found value is conservative with

respect to the as-found tolerance from TSP, then the channel is operable. If the as-found value is conservative with respect to the allowable value, and outside the predefined as-found tolerance band, then the instrument channel is operable as required to protect the analytical limit but degraded and corrective action is required to restore the channel to within the as-found tolerance. If the as-found value is less conservative with respect to the allowable value, then the channel is inoperable and corrective action is required.

The staff issued RAI 34-7870, Question 07.01-3, to ask the applicant to describe how the change in measured TSP will be verified to be within predefined limits (double-sided acceptance criteria band) and the appropriate actions to be taken if the change is outside these limits per RIS 2006-17. In the July 14, 2015, response to this RAI (ML15195A451), the applicant responded by quoting Section 2.1 of Setpoint Methodology TeR, "The calibration error band serves as an error limit during a periodic test...If the reading is outside of the periodic test error band, the instrumentation is not behaving as expected. The source of anomaly and the possibility of exceeding the allowable value should be investigated...."

The applicant explained that in the Setpoint Methodology, the scenario where the as-found TSP is not conservative with respect to the allowable value as described in RIS 2006-17. However, it was not clear to the staff what appropriate actions are to be taken in case the measured TSP value is measured to be outside the predefined limits (as-found tolerance band of the trip setting value) but is conservative with respect to the allowable value, or is conservative with respect to the as-left value of the trip setting at the beginning of a Channel Calibration surveillance interval, as described in RIS 2006-17. Instead of a supplemental question to this RAI, the staff closed this RAI and created a new RAI. The staff issued a follow up RAI 301-8280, Question 07.01-49, for the applicant to describe what appropriate actions are to be taken in case the measured TSP value is outside the predefined limits, that is, the double-sided (as-found) acceptance criteria band as described in RIS 2006-17. In the April 22, 2016 response to RAI 301-8280, Question 07.01-49 (ML16113A458), the applicant stated,

> to describe appropriate actions to be taken in the event that the TSP value is outside the periodic test error band, or that the TSP value has exceeded the allowable value, the last paragraph of Section 2.1, "Basic Description," of the Setpoint Methodology TeR, will be revised, as indicated in the response to RAI 301-8280, Question 7.1-41.

The applicant's response did not satisfactorily resolve all of the staff's concerns. Therefore, RAI 301-8280, Question 07.01-49 was tracked as an open item. All outstanding issues are addressed in the final draft TeR for the APR1400's setpoint methodology and the staff's evaluation of the response to RAI 301-8280, Question 07.01-41. As such, RAI 301-8280, Question 07.01-49, is closed.

Figure 1 of Setpoint Methodology TeR depicts the relationship among the Calibration Error Band (as-left limit), Periodic Test Error Band (as-found limit), and the Trip Setpoint. The staff issued RAI 34-7870, Question 07.01-2, to request the applicant discuss the as-left limit and as-found limit of the five-point calibration (0 percent, 25 percent, 50 percent, 75 percent, or 100 percent of the range) of the instrument transmitter, and how these limits relate to the TSP, as-left limit, and as-found limit as shown in Figure 1. In the July 15, 2016, response to RAI 34-7870, Question 07.01-2 (ML15195A451), the applicant stated, in part,

> …the as-left limits of instrument transmitters are assigned to include the reference accuracy, power supply effect, and measurement and test error… as

> described in Section 2.3.2.1 of [the Setpoint Methodology] TeR…the [SRSS] combination will describe the tolerance to the five-point calibration for as-left limits which is implemented by the utility…regarding the as-found limits, the drift, temperature effect, and radiation effect will be additionally included into the limits as described in Section 2.3.2.2 of the [Setpoint Methodology TeR]…Calibration Error Band (as-left limit) illustrated in Figure 1 is composed of individual calibration acceptance criteria for the transmitter, [APC-S], and PPS cabinet as described in Sections 2.3.2.1 and 2.3.2.4 of the [Setpoint Methodology] TeR…the as-left and as-found data of transmitter, APC-S, and PPS cabinet are required to be maintained appropriately within the corresponding Calibration Error Band and Periodic Test Error Band in order to ensure that the TSP does not exceed the [analytical limit] assumed in performing the safety analysis. The specific SRSS combination methods for the individual Calibration Error and Periodic Test Error Band for each trip parameter are described in appendices of the [Setpoint Methodology] TeR.

Therefore, there is no plan to revise Setpoint Methodology TeR, as referenced in Section 7.2.5, Item 14 of DCD Tier 2, since the individual Calibration Error Band and Periodic Test Error Band are explained in Sections 2.3.2.1, 2.3.2.2, 2.3.2.4, and 2.3.2.5 and the detailed SRSS combination methods are described in appendices of the Setpoint Methodology TeR. The staff does not agree that the Setpoint Methodology TeR adequately describes and explains the use of the individual Calibration Error Band and Periodic Test Error Band, for the transmitter, APC-S, and PPS Cabinet, and therefore, instead of a supplemental question to this RAI, the staff closed this RAI and created a new RAI. -The staff issued a follow up RAI 301-8280, Question 07.01-48, and requested the applicant to clearly describe these error bands so staff can properly understand the relationship among DTSP, allowable value, TSP, as-left limit, and as-found limit. In the April 22, 2016, response to RAI 301-8280, Question 07.01-48 (ML16113A458), the applicant stated, “To clearly describe the calibration error band and periodic error band, the last paragraph of Section 2.1, “Basic Description,” of the Setpoint Methodology TeR will be revised, as indicated in the attachment to the response to RAI 301-8280, Question 7.1-41. The applicant”s response did not satisfactorily resolve all of the staff’s concerns. Therefore, RAI 301-8280, Question 07.01-48, was tracked as an open item. All outstanding issues are addressed in the final draft TeR for the APR1400’s setpoint methodology and the staff’s evaluation of the response to RAI 301-8280, Question 07.01-41. As such, RAI 301-8280, Question 07.01-48, is closed.

10 CFR 50.36(c)(1)(ii)(A) states that the limiting safety-related system settings (LSSSs) are settings for automatic protective devices related to those variables having significant safety functions. Where an LSSS is specified for a variable on which a safety limit has been placed, the setting must be chosen so that automatic protective action will correct the abnormal situation before the safety limit is exceeded. In the applicant’s methodology, the TSP is established to ensure that an instrument channel trip signal occurs before the safety limit is reached and to minimize spurious trips close to the normal operating point of the process.

For RAI 34-7870, Question 07.01-5, the staff asked the applicant to identify the LSSS for the APR1400. In the July 14, 2015 response to this RAI (ML15195A451), the applicant responded by proposing to modify Setpoint Methodology TeR Section 2.5.1 to say, "The LSSS, which is maintained in the TS, establishes the allowable value.” Per RG 1.105, Revision 3, the allowable value is the limiting value that the trip setpoint can have when tested periodically, beyond which the instrument channel is considered inoperable and correction action must be taken in accordance with the technical specifications.” The Setpoint Methodology TeR also states that

the “[allowable value] is less conservative than the TSP by an offset which is greater than the PPS cabinet periodic test error...the PPS cabinet periodic test error is not applicable since there is no calibration associated with the PPS cabinet.”

Setpoint Methodology TeR Section 2.3.2.2 discusses measurement channel periodic test error (equipment drift) for the transmitter and APC-S. It was not clear to the staff why these two individual periodic test errors were not included in the allowable value determination/calculation. Instead of a supplemental question to this RAI, the staff closed this RAI and created a new RAI. -The staff issued a follow up RAI 301-8280, Question 07.01-51, to request the applicant to explain the concerns due to the response for RAI 34-7870, Question 07.01-5, and also to explain why the proposed offset (0.5 percent of span), as described in the applicant's response to RAI 34-7870, Question 07.01-4, provides an adequate margin to ensure that automatic protective action will correct an abnormal situation before a safety limit is exceeded per RG 1.105, Revision 3. In the April 22, 2016, response to RAI 301-8280, Question 07.01-51 (ML16113A458), the applicant stated, in part, the transmitter and the APC-S periodic test error bands are not used in determining the allowable value since the surveillance test for the PPS cabinet is performed every month but the test frequency of the transmitter and the APC-S is every refueling period. However, the transmitter and the APC-S errors are each individually verified every refueling period to be within their respective calibration error bands and periodic test error bands. The applicant’s response did not satisfactorily resolve all of the staff’s concerns. Therefore, RAI 301-8280, Question 07.01-51, was an open item. All outstanding issues are addressed in the final draft TeR for the APR1400’s setpoint methodology and the staff’s evaluation of the response to RAI 301-8280, Question 07.01-41. As such, RAI 301-8280, Question 07.01-51, is closed.

IEEE Std 603-1991, Clause 6.8.2, states that where it is necessary to provide multiple setpoints for adequate protection for a particular mode of operation or set of operating conditions, the design shall provide positive means of ensuring that the more restrictive setpoint is used when required. Where it is necessary to provide multiple setpoints as discussed in IEEE Std 603-1991, Clause 6.8, the staff’s interpretation of “positive means” is that automatic action is provided to ensure that the more restrictive setpoint is used when required. SRP BTP 7-3 provides additional guidance on multiple setpoints used to allow operation with reactor coolant pumps out of service.

Safety I&C System TeR, Appendix A, Section A.6.8, “Setpoints,” states the following.

> Manual reduction of the setpoints for low pressurizer pressure and low [SG] pressure trips is used for the controlled reduction of pressurizer pressure and SG pressure. The setpoint reductions are initiated by the [MCR], safety console’s two pushbutton switches for each division, one pushbutton switch for the pressurizer pressure and one pushbutton switch for both SG pressures within the division. This method of setpoint reduction provides positive assurance that the setpoint is never decreased below the existing pressure by more than a predetermined amount.

DCD Tier 2 Chapter 7, Section 7.2.3.4, states "Restrictive setpoints are not used for the RPS." The staff issued RAI 301-7870, Question 07.01-9, to clarify and describe the use of reset setpoints, fixed value setpoints, and setpoints in the APR1400 design and why they would not be considered more restrictive per Clause 6.8.2 of IEEE Std 603. In the July 14, 2015, response to this RAI (ML15195A451), the applicant responded by stating that “[DCD] Tier 2 Chapter 7, Section 7.2.1.4, specifies,

> The low pressurizer pressure trip is provided to trip the reactor when the measured pressurizer pressure falls to a low preset value. At pressures below the normal operating range, this setpoint can be manually decreased to a fixed increment below the existing pressurizer pressure down to a minimum value. The incremental and minimum values are given in Table 7.2-4. This provides the capability to trip the reactor when required during plant cooldown.

The section also states,

> The low SG pressure trip is provided to trip the reactor when the measured SG pressure falls below a preset value. At SG pressure below normal, the setpoint can be manually decreased to a fixed increment below the existing system pressure. This is used during plant cooldown. The fixed increment is provided in Table 7.2-4.

Regarding the "fixed value" DCD Tier 2 Chapter 7, Table 7.2-4 (2 of 2), Note (4), states,

> Setpoint can be manually decreased to a fixed increment below existing pressure as pressure is reduced during controlled plant cooldown and is automatically increased as pressure is increased maintaining a fixed increment. This fixed increment is 28 kg/cm2 (400 [pounds per square inch (psi)]) for pressurizer pressure and 14 kg/cm2 (200 psi) for steam generator pressure.

According to DCD Tier 2, Chapter 7, Section 7.2.1.4 and Table 7.2-4, low pressurizer pressure and low steam generator pressure reactor trip parameters have the function of manually resetting setpoints that should be used to shut down the nuclear power plant without the initiation of any unnecessary protective actions during plant cooldown for refueling or urgent maintenance. The purpose of the manual reset setpoints is not to provide multiple setpoints for adequate protection for a particular mode of operation or set of operating conditions but to shut down the plant without any unnecessary protective actions when plant cooldown is necessary.

In the APR1400 design, when a plant operator manually resets the predetermined reset setpoint in service, the new reset setpoint is determined as a setpoint that is lower than the existing pressurizer pressure or steam generator pressure by its own fixed value. Therefore, there is no plan to revise the Setpoint Methodology TeR, as referenced in Section 7.2.5, Item 14 of the applicant's response did not satisfactorily resolve all of the staff's concerns concerning the topic of restrictive setpoints as required per Clause 6.8.2 of IEEE Std 603-1991. As such, instead of a supplemental question to this RAI, the staff closed this RAI and created a new RAI. -The staff issued RAI 301-8280, Question 07.01-52, as a follow on RAI to RAI 34-7870, Question 07.01-9, to request that the applicant clarify whether one setpoint reset switch on the safety console applies to both low pressurizer pressure and low SG pressure trips or if there are two switches, one for each manual reduction. In the April 22, 2016 response (ML16113A458), the applicant committed to modifications to the FSAR to clarify the setpoint reset switches: one is for low pressurizer pressure and the other for low steam generator pressure on the MCR Safety Console and Remote Shutdown Console. The staff finds the proposed changes to the FSAR in RAI 34-7870, Question 07.01-52, are acceptable, however, the topic on the use of restrictive setpoints as required per Clause 6.8.2 of IEEE Std 603-1991 had not satisfactorily resolve all of the staff's concerns. Therefore, RAI 301-8280, Question 07.01-52, was an open item. In the supplemental responses to RAI 301-8280, Question 07.01-52 (ML17262A336 and ML17319A341), the applicant revised DCD Tier 2, Sections 7.2.3.4 and 7.4.3.3.5, and the Safety I&C System TeR, Appendix A to address multiple setpoints in the APR1400 design and

their compliance to IEEE Std 603-1991. In addition, the supplemental response corrected the title for the Setpoint TeR in Response Time Analysis TeR and various sections throughout the FSAR as noted in the response. It also deleted DCD Tier 2 Section 15.0.0.9 because the topic is discussed in the setpoint TeR and evaluated above in this SER. The response has satisfactorily resolved all of the staff's concerns. The incorporation of the proposed markups into the next revision of FSAR and TeR was a confirmatory item. The staff verified that the proposed markups have been incorporated into Revision 2 of DCD Tier 2, Sections 7.1.5, 7.2.3.5, 7.4.3.3.5, 15.0.0.9, and 15.0.5, Revision 2 of the Safety I&C TeR, Section 9 and Appendix A.6.8, and Revision 2 of the Response Time Analysis TeR, Section 8.- As such, this confirmatory item has been satisfied.

The staff issued RAI 34-7870, Question 07.01-6, to request that the applicant provide consistent use of setpoint terminology. The Setpoint Methodology TeR describes the setpoint methodology applied to the PPS and DPS for the APR1400 and states conformance to RG 1.105, Revision 3, SRP BTP 7-12, and RIS 2006-17. Section 5 of the Setpoint Methodology TeR defines the setpoint-related terminology used. For clarity, staff requested applicant to cite the source, if relevant, for the definitions. For example, "[analytical limit], limit of a measured or calculated variable established by the safety analysis to ensure that a safety limit is not exceeded. Appendix A of the Setpoint Methodology TeR, "Pressurizer Pressure – High Trip Setpoint Calculation," Section VI, "TRIP SETPOINT, ALLOWABLE VALUE, PRETRIP SETPOINT," uses the terms Trip Setpoint, Allowable Value, and Final Trip Setpoint. It was not clear if "Trip Setpoint" is referring to the "Draft Setpoint" in Figure 1 of the technical report. The staff requested the applicant to use consistent terminology between the technical report and its appendices. Also, the staff requested the applicant to unambiguously state how the terms (e.g., allowable value, NTSP, ALT, AFT) used in Tier 2, Chapter 16, Section 5.5.19, "Setpoint Control Program," correspond to the terms used in the setpoint methodology technical report (e.g., allowable value, TSP, Calibration Error Band [as-left limit], Periodic Test Error Band [as-found limit]).

In the July 14, 2015, response to RAI 34-7870, Question 07.01-6 (ML15195A451), the applicant responded by stating the following.

> …the setpoint-related terminologies defined in Section 5 of the [Setpoint Methodology] TeR are synonymous with those of RG 1.105, [Revision 3], ISA-S67.04-1994, Part 1, and RIS 2006-17 and also unique to APR1400 documentation. The term of "Trip Setpoint" described in Section VI of Appendix A of the [Setpoint Methodology] TeR means the "Draft Trip Setpoint" in Figure 1 of the technical report. To use consistent terminology between the technical report and its appendices "Draft" will be added to corresponding wordings in all Appendices of the [Setpoint Methodology] TeR as shown in Attachment 1. [NTSP, ALT, AFT] used in Tier 2, Chapter 16, Section 5.5.19 correspond, respectively, to final TSP, Calibration Error Band, and Periodic Test Error Band used in the [Setpoint Methodology TeR]. The relationship between NTSP and final TSP is described in Section 2.1 of the [Setpoint Methodology] TeR. The definitions of Calibration Error and Periodic Test Error provided in Section 5 of the [Setpoint Methodology] TeR are synonymous with the "region of calibration tolerance," as shown in Figure 1 of RG 1.105, [Revision 3,] and "as-found LSSS," as used in RIS 2006-17, respectively.

The staff finds the proposed changes to the Setpoint Methodology TeR in RAI 34-7870, Question 07.01-6, acceptable; however, topics concerning SRP BTP 7-12, RIS 2006-17, and

the setpoint control program has not satisfactorily resolve all of the staff's concerns Therefore, RAI 34-7870, Question 07.01-6, was an open item. All outstanding issues are addressed in the final draft TeR for the APR1400's setpoint methodology and the staff's evaluation of the response to RAI 301-8280, Question 07.01-41. As such, RAI 34-7870, Question 07.01-6, is closed.

The staff issued RAI 34-7870, Question 07.01-7, to request the applicant to clarify what is meant by "previous errors" as used in the Setpoint Methodology. In the July 14, 2015, response to this RAI (ML15195A451), the applicant responded, and stated the following.

> In the draft version of the Setpoint Methodology TeR, Sections 2.3.2.5 thru 2.3.2.7 regarding the PPS cabinet errors were initially located in front of the Sections 2.3.2.1 thru 2.3.2.4 covering measurement channel errors. The wording of "previous errors" described in Section 2.3.2.1 was used to indicate the PPS cabinet calibration error and PPS cabinet periodic test error. However, the wording is not necessary to be used in the Setpoint Methodology TeR, Revision 0. Therefore, "As with the previous errors" described in Section 2.3.2.1 will be deleted as shown in Attachment 1.

The staff finds the proposed changes to the Setpoint Methodology TeR in RAI 34-7870, Question 07.01-7, are acceptable. The incorporation of the proposed markups into the next revision of the TeR was a confirmatory item. The staff verified that the proposed markups have been incorporated into Revision 2 of the Setpoint Methodology TeR. As such, this confirmatory item has been satisfied.

The staff issued RAI 34-7870, Question 07.01-8, to request the applicant to describe how surveillance testing and maintenance are used to determine setpoints. In the July 14, 2015, response to this RAI (ML15195A451), the applicant responded by stating the following.

> Section 2.1 of the [Setpoint Methodology TeR], states "The calibration error band serves as an error limit during a periodic test. If the instrument reading is within this tolerance band, no recalibration is necessary. If the instrument reading is outside the calibration error band, but within the periodic test error band, the channel segment is functioning as intended although recalibration is required." Surveillance testing is a periodic test required by the TS, and is to be performed at an appropriate test interval to ensure that an instrument channel is functioning in compliance with the safety analysis and to verify that trip setpoints remain within their established limits during operation. If as-found data from surveillance testing indicates that the calibration error band was exceeded, appropriate maintenance, such as calibration, will be performed. Therefore, DCD Tier 1, Section 2.5.1.1, Item 10 will be revised, as shown in Attachment 1, to state that surveillance testing and maintenance are used to determine if setpoints for variables of [reactor trip] and ESF initiation are within acceptable limits.

The response has satisfactorily resolved all of the staff's concerns. Therefore, RAI 34-7870, Question 07.01-8, was a confirmatory item. The staff verified that the proposed markups have been incorporated into Revision 1 of DCD Tier 1 Section 2.5.1.1, Item 10. As such, this confirmatory item has been satisfied.

Setpoint Methodology TeR Conclusions

The staff reviewed the information submitted by the applicant and concluded with reasonable assurance, that the applicant provided sufficient information in the APR1400 Setpoint Methodology Technical Report to demonstrate that the requirements in 10 CFR Part 50, Appendix A, GDC 13 and 20, of 10 CFR Part 50, Appendix B, CriterionXI, of 10 CFR 50.36(c)(1)(ii)(A) and 10 CFR 50.36 (c)(3), and of 10 CFR 50.55a(h)(3), which requires compliance with IEEE Std 603-1991 are met.

Under 10 CFR Part 52, the application must include ITAAC for the plant-specific setpoint analysis, which details the procedures for establishing the setpoints including the margins and their location. Prior to initial fuel load, a reconciliation of the setpoint analysis and setpoint program against the final design for each plant must be performed, as required by the ITAAC. The staff's review of the proposed ITAAC is documented in Section 14.3.5 of this SER.

7.1.4.26 Three-Mile Island Action Plan (TMI) Items

7.1.4.26.1 TMI Action Plan Item I.D.3: Bypass and Inoperable Status Indication

10 CFR 50.34(f)(2)(v) requires that the design provide for automatic indication of the bypassed and operable status of safety-related systems.

Tier 2 Section 7.1.2.5 of the FSAR states that display instrumentation provides accurate, complete, and timely information to safety-related system status by compliance to Clause 5.8.2 (system status indication) and Clause 5.8.3 (indication of bypasses) of IEEE Std 603. Conformance with IEEE Std 603 is described in the Safety I&C System TeR. Information regarding bypassed and inoperable status is provided in Section 7.5.1.3.

The staff's evaluation on APR1400 compliance to the 10 CFR 50.34(f)(2)(v) is discussed in Section 7.5 of this SER.

7.1.4.26.2 TMI Action Plan Item II.D.3: Direct Indication of Relief and Safety Valve Position

10 CFR 50.34(f)(2)(xi) requires that the design provide direct indication of relief and safety valve position (open or closed) in the control room.

The staff's evaluation on APR1400 compliance to the 10 CFR 50.34(f)(2)(xi) is discussed in Section 7.5 of this SER.

7.1.4.26.3 TMI Action Plan Item II.E.1.2: Auxiliary Feedwater System Automatic Initiation and Flow Indication

10 CFR 50.34(f)(2)(xi) requires that the design provide automatic and manual (AFWS) initiation, and provide auxiliary feedwater system flow indication in the control room.

The staff's evaluation on APR1400 compliance to the 10 CFR 50.34(f)(2)(xii) is discussed in Section 7.3 and 7.5 of this SER.

7.1.4.26.4 TMI Action Plan Item II.E.4.2: Containment Isolation Systems

10 CFR 50.34(f)(2)(xiv) requires that the design provide containment isolation systems that (1) ensure all non-essential systems are isolated automatically by the containment isolation

system; (2) for each non-essential penetration (except instrument lines) have two isolation barriers in series; (3) do not result in reopening of the containment isolation valves on resetting of the isolation signal; (4) utilize a containment set point pressure for initiating containment isolation as low as is compatible with normal operation; and (5) include automatic closing on a high radiation signal for all systems that provide a path to the environs.

The staff's evaluation on APR1400 compliance to the 10 CFR 50.34(f)(2)(xiv) is discussed in Section 7.3 of this SER.

7.1.4.26.5 TMI Action Plan Item II.F.1: Accident Monitoring Instrumentation

10 CFR 50.34(f)(2)(xvii) requires that the design provide instrumentation to measure, record and readout in the control room: (1) containment pressure, (2) containment water level, (3) containment hydrogen concentration, (4) containment radiation intensity (high level), and (5) noble gas effluents at all potential, accident release points. The design must also provide for continuous sampling of radioactive iodines and particulates in gaseous effluents from all potential accident release points, and for onsite capability to analyze and measure these samples.

The staff's evaluation on APR1400 compliance to the 10 CFR 50.34(f)(2)(xvii) is discussed in Section 7.5 of this SER.

7.1.4.26.6 TMI Action Plan Item II.F.2: Instrumentation for the Detection of Inadequate Core Cooling

10 CFR 50.34(f)(2)(xviii) requires that the design provide instruments that provide in the control room an unambiguous indication of inadequate core cooling, such as primary coolant saturation meters in PWRs, and a suitable combination of signals from indicators of coolant level in the reactor vessel and in-core thermocouples in PWRs and BWRs.

The staff's evaluation on APR1400 compliance to the 10 CFR 50.34(f)(2)(xviii) is discussed in Section 7.5 of this SER.

7.1.4.26.7 TMI Action Plan Item II.F.3: Instruments for Monitoring Plant Conditions Following Core Damage

10 CFR 50.34(f)(2)(xix) requires that the design provide instrumentation adequate for monitoring plant conditions following an accident that includes core damage.

The staff's evaluation on APR1400 compliance to the 10 CFR 50.34(f)(2)(xix) is discussed in Section 7.5 of this SER.

7.1.4.26.8 TMI Action Plan Item II.G.1: Power for Pressurizer Level Indication and Controls for Pressurizer Relief and Block Valves

10 CFR 50.34(f)(2)(xx) requires that the design provide power supplies for pressurizer relief valves, block valves, and level indicators such that: (1) level indicators are powered from vital buses; (2) motive and control power connections to the emergency power sources are through devices qualified in accordance with requirements applicable to systems important to safety; and (3) electric power is provided from emergency power sources.

The staff's evaluation on APR1400 compliance to the 10 CFR 50.34(f)(2)(xx) is discussed in Section 7.5 of this SER. The review of emergency power sources and electrical power for these sources is discussed in Chapter 8 of this SER.

7.1.5 Combined License Information Items

No applicable items were identified in the FSAR. No additional COL information items need to be included in DCD Tier 2 Table 1.8 2, "APR1400 Combined License Information Items," for I&C Systems - Introduction.

7.1.6 Findings and Conclusions

The staff review identified areas that the applicant still has not provided sufficient information to allow the staff to make its safety finding. The applicant identified the I&C systems that are important to safety in accordance with RG 1.206, "Combined License Applications for Nuclear Power Plants," Revision 0, and identified the NRC regulations that are applicable to these systems. The applicant has also identified guidelines consisting of the RGs and the industry codes and standards that are applicable to the systems.

10 CFR 50.55a(h)(3) states, in part, that application filed on or after May 13, 1999, for design certifications must meet the requirements for safety-related systems in IEEE Std 603-1991 and the correction sheet dated January 30, 1995. The staff reviewed the application against the requirements of IEEE Std 603-1991. The clauses within IEEE Std 603-1991 address, among other requirements, single failure protection, independence, quality, design bases, information displays, automatic and manual controls, operating and maintenance bypasses, and capability for test and calibration. Based on the information provided in the FSAR and IBR technical reports, the staff determined that the I&C design meets the requirements of IEEE Std 603-1991.

The staff reviewed the APR1400 I&C design to verify its compliance with GDC 1. The staff finds that the applicant meets the requirements of GDC 1.

In conjunction of the staff's review of IEEE Std 603-1991, the staff reviewed compliance of the design to GDC 2, 4, 13, 20, 21, 22, 23, 24, and 29. Based on the information provided in the FSAR and IBR technical reports, staff determined the APR1400 design meets the requirements of GDC 2, 4, 13, 20, 21, 22, 23, 24, and 29.

The staff reviewed the ITAAC in regards to compliance to 10 CFR 52.47(b)(1). Additional discussion on the staff's review of compliance to 10 CFR 52.47(b)(1) is found in Section 14.3.5 of this SER. Based on the staff's conclusions in Section 14.3.5 of this SER, the staff finds the APR1400 design meets the requirements of 10 CFR 52.47(b)(1).

7.2 Reactor Trip System

The APR1400 provides safety-related I&C to sense conditions requiring protective action and to automatically initiate a reactor trip. Manual initiation of a reactor trip at the division-level is provided in the MCR.

7.2.1 Introduction

The PPS is a safety-related system that actuates reactor control rod scrams (i.e., reactor trips) and ESFAS. The portion of the PPS that is responsible for initiating a reactor trip is the RPS.

The complete RTS (i.e., sensor to final actuation device) that initiates reactor trips is referred to as the RTS. The RTS is classified as a safety-related system. DCD Tier 1 Section 2.5.1.1, "Design Description," states that the RTS consists of:

- Four channels of sensors,
- APC-S cabinets,
- ENFMS cabinets,
- Four divisions of CPCS cabinets,
- RPS portion of the PPS cabinets,
- RTSS cabinets.

DCD Tier 2, Revision 0, Figure 7.2-1, "PPS Basic Block Diagram," provides a single line, block diagram of the four channel RTS reactor trip actuation signal path from the RTS sensor measurement inputs to the RTSS. As shown in Figure 7.2-1, reactor plant parameters are sensed and measured and the resultant plant parameter process value (i.e., signal) is sent to the RPS portion of the PPS via the APC-S and the ENFMS. The ENFMS includes neutron detectors located around the reactor core which provide neutron flux information from near startup neutron flux levels to 200 percent (10 decades) of rated power. The ENFMS sends variable overpower and high log power reactor trip actuation signals to the PPS. The CPCS contains the CEAC, the CPP, and the CPC. The CPCS monitors reactor core conditions and generates and sends a low DNBR and a high LPD reactor trip signal to the PPS. The CPCS transmits digital reactor trip actuation signals to the PPS versus sensor measurement values.

Each PPS channel contains two redundant bistable processors, one per rack, that contain the reactor trip logic to compare the incoming process values to a safety setpoint value. If the measured plant process value exceeds the safety setpoint, both bistable processors will generate a reactor trip actuation signal and send this reactor trip actuation signal to the LCL processors. An individual PPS channel single line diagram is shown in DCD Tier 2, Revision 0, Figure 7.2-10, "PPS Channel A Trip Path Diagram." However, since Figure 7.2-10 was titled for "Channel A" only, staff was not clear if Figure 7.2-10 was representative for all PPS safety divisions or just Channel A of the PPS. Therefore, staff issued RAI 50-7911, Question 07.02-1, requesting the applicant to insert a caption on the figures explaining whether the schematic or diagram shown is identical for all divisions/channels or whether there are differences between the divisions/channels. In the September 22, 2015 response to RAI 50-7911, Question 07.02-1 (ML15265A594), the applicant stated that the trip path shown in Figure 7.2-10 of DCD Tier 2 is identical for all PPS channels and that the applicant would add the following phrase to the DCD Tier 2 Section 7.1, "All figures provided in Chapter 7 are identical for all channels or divisions. If a figure provided is not identical for all channels or divisions, a note is provided to indicate the difference."

The staff finds this response provides clarity and therefore is acceptable. Similar phrases were added to Section 4.1 of the Safety I&C System TeR, Revision 0 and Section 1.2 of the CPCS TeR. The staff finds this response provides clarity and therefore is acceptable. In addition, during the staff's evaluation of other design documents, the staff noticed differences between the LCL processor schematic boxes in Figure 4-5, "PPS Division A Trip Path Diagram," of the Safety I&C System TeR, Revision 0 and Figure 7.2-10 of DCD Tier 2 Revision 0. The staff

issued RAI 50-7911, Question 07.02-5, requesting the applicant to discuss the differences between the two figures and update the APR1400 application as necessary. In the September 22, 2015, response to RAI 50-7911, Question 07.02-5 (ML15265A594), the applicant stated that Figure 4-5 of the Safety I&C System TeR will be revised to be identical to Figure 7.2-10 of DCD Tier 2. The staff finds this response acceptable. Therefore, the incorporation of the proposed markups within RAI 50-7911, Question 07.02-1 and RAI 50-7911, Question 07.02-5, were tracked as confirmatory items. In a March 2, 2017, revised response to RAI 50-7911, Question 07.02-1 (ML17061A729), the applicant proposed to move the phrase "All figures provided in this document are identical for all channels or division. If a figure provided is not identical for all channels or divisions, a note is provided to indicate the difference," from Section 1.2 to Section 3 of the CPCS TeR because the phrase is not relevant to that particular section's scope, but rather to Section 3 where the general description of system requirements is contained. In addition, the applicant provided a markup which included a note on DCD Tier 2 Figure 7.2-28, "Functional Logic Diagram for Reactor Trip Signal Generation," that clarified that the manual reactor trip switches in the RSR are provided only for divisions A and B. The staff has reviewed the markups and agrees with these changes and the added figure note which is consistent with the design, and finds this revised response is acceptable. The staff verified that the RAI 50-7911, Question 07.02-1, phrase has been incorporated into Revision 1 of DCD Section 7.1, and Revision 1 of the Safety I&C System TeR, Section 4.1, and Revision 1 of the Functional Design Requirement for a CPCS TeR, Section 3. The staff verified that the proposed note from the response to RAI 50-7911, Question 07.02-1, has been added to Revision 1 of the FSAR, Figure 7.2-28. The staff verified that the proposed markups of Figure 4-5 provided in the response to RAI 50-7911, Question 07.02-5, has been inserted into Revision 1 of the Safety I&C System TeR. As such, these confirmatory items have been satisfied.

All of the other PPS safety divisions' bistable processors will send their respective divisions' reactor trip actuation signals to all other RTS safety divisions' LCL processors. Per RTS safety channel, there are four RTS LCL processors, two per rack, which are redundant to each other within the safety channel. Each LCL processor will receive all safety divisions' bistable processor reactor trip actuation signals and will generate two redundant trip signals (two LCL output signals per rack) if at least 2oo4 safety channel's bistable processors send a reactor trip actuation signal. The LCL processors, per safety channel, will generate four reactor trip actuation signals and send these actuation signals to the selective 2oo4 initiation circuit. This reactor trip actuation logic is illustrated in DCD Tier 2, Revision 0, Figure 7.2-15, "Reactor Trip Initiation Diagram." The four LCL reactor trip actuation signals are combined in the "Selective 2/4" initiation circuit logic, into two reactor trip output signals, which are sent to two reactor trip circuit breaker (RTCB) undervoltage trip devices contained in the RTSS. This reactor trip actuation signal path from the selective 2oo4 initiation circuits to the RTSS is illustrated in DCD Tier 2, Revision 0, Figure 7.2-10, "PPS Channel A Trip path Diagram." The reactor trip actuation signals de-energize the undervoltage trip devices resulting in opening the RTCB which interrupts power to the CEDM coils allowing the CEAs (i.e., control rods) to drop into the core by gravity. The RTSS interface diagram is shown in Figure 7.2-9, "Reactor Trip Switchgear System Interface Diagram."

DCD Tier 2 Section 3.9.4.1, "Descriptive Information of Control Element Drive Mechanism," states that the CEDM is a magnetic jack-type driving apparatus that is used to position the CEAs (i.e., control rods). Each CEDM is capable of withdrawing, inserting, holding, or tripping the applicable CEAs. DCD Tier 2 Section 4.2.2.4.1, "Control Element Assembly," states that CEAs consist of either 4 or 12 neutron absorber elements. The 4-element CEAs are used for control of power distribution and core reactivity in the power operating range. The 12-element CEAs provide the core with shutdown rod worth. During normal power operation, all of the

12-element CEAs are in the fully withdrawn position. The 4-element CEAs are provided for reactivity and axial power control during power operations, including load maneuvering. DCD Tier 2 Table 4.2-1, states that there are 33 (thirty-three) 4-element CEAs and 48 (forty-eight) 12-element CEAs in the core. DCD Tier 2, Revision 0, Section 15.4.2.3.2, "Input Parameters and Initial Conditions," and DCD Tier 2, Revision 0, Table 15.4.2-2, "Assumptions and Initial Conditions for the Sequential CEA Withdrawal Analysis at Power," state that the maximum CEA withdrawal rate of the CEA drive system is 30 inches/minute (76.2 cm/min).

7.2.2 Summary of Application

DCD Tier 1: The DCD Tier 1 information associated with this section is found in DCD Tier 1 Section 2.5.1, "Reactor Trip System and Engineered Safety Features Initiation," In DCD Tier 1 Section 2.5.1.1., "Design Description," Item 4.a, the applicant states that the PPS provides an automatic reactor trip if plant process signals reach predetermined setpoints.

DCD Tier 2: The applicant provided an RTS system description in DCD Tier 2 Section 7.2, "Reactor Trip System," summarized here, in part, as follows:

The RTS is a safety-related system that initiates reactor trips. The RTS functions protect the core fuel design limits and the RCS pressure boundary following AOOs and provide assistance in mitigating the consequences of PAs. The PPS consists of four divisions. Each PPS division is located in a divisionalized I&C equipment room. Two pairs of manual trip switches are provided in the MCR, and one pair of manual trip switches is provided in the RSR for reactor trip. These manual reactor trip switch signals are connected directly to the undervoltage trip device of the TCB in each RTSG. The RPS initiation relays in each division interface with the undervoltage devices to trip the control rod (i.e., CEAs) circuit breakers allowing the CEAs to fall into the core.

ITAAC: The ITAAC associated with DCD Tier 2 Section 7.2, are specified in DCD Tier 1 Table 2.5.1-5, "Reactor Trip System and Engineered Safety Features Initiation ITAAC."
Technical Specifications: The Technical Specifications associated with DCD Tier 2 Section 7.2 are specified in DCD Tier 2 Chapter 16, "Technical Specifications." Chapter 16 of this SER provides the staff's evaluation of the technical specifications related to the RTS.

7.2.3 Regulatory Basis

The relevant requirements of the NRC regulations for this area of review, and the associated acceptance criteria, are specified in SRP Section 7.2 and are summarized below. Review interfaces with other SRP Sections also can be found in SRP Section 7.2.

1. 10 CFR 50.55a(h)(3), "Safety Systems," requires compliance with IEEE Std 603 1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," and the correction sheet dated January 30, 1995.

2. 10 CFR 50.34(f), "Additional TMI-related Requirements," or equivalent TMI action requirements imposed by Generic Letters:

    a. (2)(v), "Bypass and Inoperable Status Indication."

    b. (2)(xxiii), "Anticipatory Trip on Loss of Main Feedwater or Turbine Trip."

3. GDC 1, 2, 4, 10, 13, 15, 19, 20, 21, 22, 23, 24, 25, 29.

4. 10 CFR 50.55a(z), “Alternatives to codes and standards requirements,” requires that alternatives to the requirements of 10 CFR 50.55a(h)(3) must demonstrate that the proposed alternative would provide an acceptable level of quality and safety.

5. 10 CFR 52.47(b)(1), “Contents of Applications; Technical Information,” requires that a design certification contain the proposed ITAAC that are necessary and sufficient to provide reasonable assurance that, if the inspections, tests, and analyses are performed and the acceptance criteria met, a facility that incorporates the design certification has been constructed and will be operated in conformity with the design certification, the provisions of the Act, and the Commission's rules and regulations.

Acceptance criteria adequate to meet the above requirements include SRP Section 7.2 and SRP Table 7-1, “Regulatory Requirements, Acceptance Criteria, And Guidelines for Instrumentation and Control Systems Important to Safety,” Revision 5. Table 7-1 lists the SRP acceptance criteria applicable to the RTS.

7.2.4 Technical Evaluation

The objective of the staff’s evaluation is to confirm that the reactor trip design satisfies NRC regulations through a set of acceptance criteria and that it can perform its safety functions for all plant conditions. SRP Section 7.2 lists regulatory acceptance criteria for design considerations that should be emphasized for the review of reactor trip functions.

10 CFR 50.55a(z), “Alternatives to Codes and Standards Requirements,” allows an applicant under 10 CFR Part 52 to propose alternatives to the requirements of 10 CFR 50.55a(h)(3). The APR1400 design certification applicant proposes to share the CEA position sensor signals between redundant safety divisions, as an alternative to the independent safety division sensor requirement by IEEE Std 603-1991, Clause 5.6.1, “Independence Between Redundant Potions of a Safety System.” Section 7.1.4.2 of this SER discusses the staff’s evaluation and approval of this alternative.

7.2.4.1 Design Basis Evaluation for the APR1400 RTS

Clause 4 of IEEE Std 603-1991, “Safety System Designation,” requires that a specific basis be established for the design of each safety-related system of the nuclear power generating station. SRP Appendix 7.1-C, Guidance for Evaluation of Conformance to IEEE Std 603 Review Responsibilities,” Section 4, “Safety System Designation,” discuss the requirements of IEEE Std 603-1991 and how the requirements are used in the review of the RTS. The staff used the guidance of SRP Section 7.2, and SRP Appendix 7.1-C, “Guidance for Evaluation of Conformance to IEEE Std 603 Review Responsibilities,” Revision 5, to evaluate the APR1400 application against the regulations.

7.2.4.1.1 RTS Design Basis Evaluation Overview

DCD Tier 2, Revision 0, Section 7.2.1, “System Description,” states that the RPS functions to protect the core fuel design limits and the RCS pressure boundary following AOOs and to provide assistance in mitigating the consequences of PAs. DCD Tier 2, Revision 0, Section 16, B 2.1.1, “Reactor Core Safety Limits,” states that the RPS, in combination with the limiting conditions for operations, is designed to prevent any anticipated combination of transient

conditions for RCS temperature, pressure, and thermal power level that would result in a violation of the reactor core safety limits. DCD Tier 2 Section 15.0.0.1.1, "Normal Operation and Anticipated Operational Occurrences," states that the fuel design and reactor coolant pressure boundary limits used in the RPS design for the AOOs are:

- The DNBR in the limiting coolant channel in the core is not less than the DNBR safety limit of 1.29.

- The hot fuel pellet in the core does not undergo centerline melting. Maintaining the peak linear heat rate (LHR) less than 656 W/cm (20 kW/ft) provides reasonable assurance that fuel centerline melt will not occur during an AOO.

- The RCS pressure does not exceed the established pressure boundary limits (110 percent of design pressure).

DCD Tier 2 Section 15.0.0.1.2, "Postulated Accidents," states that the basic criteria for PAs are:

- Pressures in the reactor coolant and main steam systems are maintained below the acceptable design limits.

- Fuel cladding integrity is maintained by providing reasonable assurance that the minimum DNBR remains above the 95/95 DNBR limit. If the minimum DNBR does not meet this limit, the fuel is assumed to have failed.

- The release of radioactive material does not result in offsite doses in excess of the guidelines in 10 CFR 50.34. Any event-specific accident limits for allowable radiological releases are described in the appropriate sections.

- The postulated accident does not by itself result in a consequential loss of required functions of systems needed to cope with the fault, including those of the RCS and the reactor containment system.

The staff reviewed the RTS system design descriptions, system operation characteristics, postulated DBE analyses, and other design certification application information to determine whether the RTS design basis meet NRC design basis requirements. The staff's evaluation of the RTS design basis for conformance to regulatory requirements is documented in the following sections.

7.2.4.1.2 Identification of RTS Design Basis Parameters

The staff utilized the guidance of SRP Appendix 7.1-C, "Guidance for Evaluation of Conformance to IEEE Std 603 Review Responsibilities," Revision 5, dated March 2007, Section 4, "Safety System Designation," which provides guidance for IEEE Std 603-1991, Clause 4, to perform the safety evaluation.

Clause 4.1 of IEEE Std 603-1991 requires, in part, the identification of the DBE applicable to each mode of operation. DCD Tier 2 Section 16, "APR1400 Technical Specifications," Item 1.1, "Definitions," states that a MODE shall correspond to any one inclusive combination of core reactivity condition, power level, reactor coolant cold leg temperature, and reactor vessel

head closure bolt tensioning. DCD Tier 2 Section 16, Table 1.1-1, "MODES," list the plant MODES as:

Table 7.2-1: Plant MODES[1]

MODE	Title
1	Power Operation
2	Startup
3	Hot Standby
4	Hot Shutdown
5	Cold Shutdown
6	Refueling

DCD Tier 2 Section 15.0.0.2.1, "Design Plant Conditions," states that the AOOs and PAs are considered to occur over a safety analyses range of initial plant operating conditions, and Section 15.0.0.2.2, "Initial Conditions," states that the ranges were chosen to encompass all steady-state operational configurations. DCD Tier 2, Revision 0, Section 7.4, "Systems Required for Safe Shutdown," does not list the RPS as a system that is required to achieve and maintain a safe shutdown of the reactor. Therefore, staff finds that all listed DBEs for the RTS are analyzed during steady-state operational configurations, which would be MODE 1, as listed in Table 7.2-1 above.

Clause 4.1 of IEEE Std 603-1991, also requires the identification of initial conditions for each DBE. The staff's review found that DCD Tier 2 Section 15, Table 15.0-6, "Summary of Computer Codes and Initial Conditions," contains the major initial conditions for the DBE analyses. DCD Tier 2 Section 15, Table 15.0-9, "Time for Release Termination of Design Basis Accidents," list the release termination times for different events. The release times represent the amount of time when the release path is isolated or the plant is cooled down to the cold shutdown entry conditions. Therefore, staff finds that the applicant has identified the RPS initial conditions for each DBE and has identified the allowable release time limits for applicable DBEs and thus meet the requirements of IEEE Std 603-1991, Clause 4.1.

Clause 4.2 of IEEE Std 603-1991, requires the safety functions and corresponding protective actions of the execute features for each DBE to be documented. The staff's review found that DCD Tier 2 Section 15, Table 15.0-2, "Reactor Protection System Trips Used in the Safety Analysis," list the RPS safety function trips used in the accident analysis and Table 15.0-7, "Plant Systems Used in the Accident Analysis," list the RTS safety functions and corresponding protective actions for each DBE. Therefore, staff finds that the applicant has identified the RPS safety functions and corresponding protective actions of the execute features for each DBE to meet the requirements of IEEE Std 603-1991, Clause 4.2.

Clause 4.4 of IEEE Std 603-1991, in part, requires the identification of variables that are monitored in order to provide protective action. Clause 4.6 of IEEE Std 603-1991, requires in part, the identification of the minimum number and location of sensors for those variables in Clause 4.4 of IEEE Std 603-1991 that have a spatial dependence. The staff's review found that DCD Tier 1 Table 2.5.1-2, "Reactor Trip System Variables," and DCD Tier 2, Revision 0, Table 7.2-2, "Reactor Protection System Monitored Plant Variable Ranges," identify the plant variables that are monitored for reactor trips and the monitored plant variable ranges. Clause 4.4 of IEEE Std 603-1991 also requires in part, the identification of RTS system

[1] Generated from DCD Tier 2 Section 16, "Technical Specifications," Table 1.1-1, "MODES."

accuracies, and plant variable monitored ranges. The staff's review identified that DCD Tier 2, Revision 0, Table 7.2-2, "Reactor Protection System Monitored Plant Variable Ranges," lists the ranges and nominal values for the RTS measured plant process parameters and that Table 7.2-4, "Reactor Protection System Design Inputs," identifies the RTS sensed process parameter's full power nominal values, nominal trip setpoint values, and margin to trip values. Therefore, the staff's review of the above finds that the applicant has identified the RPS design basis monitored variables and ranges to meet the requirements of IEEE Std 603-1991, Clause 4.4. Section A.4, "Safety System Designation," of the Safety I&C System TeR, states that for variables in Clause 4.4 that have a spatial dependence, the number and location of the sensors provided to monitor these variables in Clause 4.4 are provided in DCD Tier 2 Table 7.2-3, "Reactor Protection System Sensors." Therefore, the staff finds that variables required for protective purposes that have a spatial dependence, have been identified in the APR1400 application, and thus the RPS design meets the requirements of IEEE Std 603-1991, Clause 4.6. The staff also found a design description in the Safety I&C System TeR, Section 4.1.1.3, "Core Protection Calculator System," that stated that a trip signal is transmitted to the PPS from the CPCS after the DNBR and LPD values exceed a safety limit. The staff issued RAI 50-7911, Question 07.02-6, to inform the applicant that initiating a protective action after a safety limit is exceeded does not comply with the safety limit requirements of 10 CFR 50.36(c)(ii)(A), "Technical Specifications," and to request the applicant to address this issue. 10 CFR 50.36(c)(ii)(A) states that a limiting safety-related system setting are settings for automatic protective devices related to those variables having significant safety functions. Where a limiting safety-related system setting is specified for a variable on which a safety limit has been placed, the setting must be so chosen that automatic protective action will correct the abnormal situation before a safety limit is exceeded. Pending the resolution of this issue, RAI 50-7911, Question 07.02-6, was tracked as an open item. In the September 22, 2016 response to RAI 50-7911, Question 07.02-6 (ML15265A594), the applicant provided a markup that revised the Safety I&C System TeR to state that when the CPCS's DNBR and LPD values exceed setpoints, a trip signal is transmitted to the PPS. The staff finds that the applicant's RAI response markup revision conforms to the safety limit requirements of 10 CFR 50.36(c)(ii)(A) and that the issues identified in RAI 50-7911, Question 07.02-6, is closed and resolved. The incorporation of the proposed markups into the next revision of the Safety I&C System TeR was a confirmatory item. The staff verified that the proposed markups have been incorporated into the Safety I&C System TeR, Revision 1. As such, this confirmatory item has been satisfied.

Clauses 4.10.1 and 4.10.2 of IEEE Std 603-1991, in part, requires the identification of the critical points in time after the onset of a DBE, for which the protective actions of the safety-related system shall be initiated and the point in time that define the proper completion of the safety function. DCD Tier 2 Section 15 analyzed DBEs that utilize and credit RPS reactor trip safety functions and provides a "sequence of event" description of the protective actions that should actuate and execute to mitigate an analyzed DBE as well as a "sequence of event" table that provides the time, in seconds (and the setpoint value exceeded to initiate the trip), of when the initiated protective actions should actuate, after the sensed plant variable has exceeded the safety-related system setpoint. In addition, DCD Tier 2 Section 15.0.0.3, "Reactor Trip System and Engineered Safety Feature Systems Analytical Limit and Delay Times," provides the time allotted when the magnetic flux of the CEDM control rod (i.e., CEA) holding coils has decayed enough to allow the control rods to start to fall into the core. DCD Tier 2 Section 15.0.0.2.4, "CEA Insertion Characteristics," defines the CEA "drop time" as the interval between the time the power is removed from the CEDM coils and the time the CEA has reached 90 percent of its fully inserted (i.e., tripped) position. The staff's review finds that these DBE critical times have been provided. As an example, the staff's review of DCD Tier 2, Section 15, Table 15.4.8-1 (Sheet 3 of 3), "Sequence of Events for the CEA Ejection," which lists: (1) the time after the

DBE occurred that the corresponding trip setpoint value was exceeded, (2) the setpoint value exceeded, (3) the time that the reactor trip signal was initiated, (4) the time when the reactor trip circuit breakers open, and (5) the time when the CEAs begin to drop into the core. From this example, all critical points of time for the reactor trip safety function have been provided. Therefore, the staff finds that the applicant has provided the critical points in time after a DBE when the reactor trip protective action will be initiated and the point in time for proper RPS completion of the reactor trip safety function, and thus the RPS design meets the requirements of IEEE Std 603-1991, Clauses 4.10.1 and 4.10.2.

7.2.4.1.2.1 Derivation of System Inputs

Clause 6.4 of IEEE Std 603-1991 states that to the extent feasible and practical, sense and command feature inputs shall be derived from signals that are direct measures of the desired variables as specified in the design basis. Table 7.2-2 below provides the list of the RTS reactor trips based on direct measurement of plant variables.

Table 7.2-2. RTS Reactor Trips Based on Direct Measurements of Plant Variables[2]

Reactor Trip Function	Sensed Plant Variable	Reason for Reactor Trip
Variable overpower	Neutron flux power from the ENFMS	Trip for uncontrolled rod withdrawal
High logarithmic power level	Neutron flux power from the ENFMS	Assurance of the integrity of the fuel cladding and RCS boundary in the event of unplanned criticality from a shutdown condition
High pressurizer pressure	Reactor coolant pressure from narrow range	Assurance of the integrity of the RCS boundary
High steam generator water level	Level of water in each SG down-comer region from narrow range differential pressure measurements	Coincident with the initiation of the main steam isolation, To assist the ESF systems
High containment pressure	Pressure inside containment	Coincident with the initiation of safety injection, to assist the ESF systems
Low pressurizer pressure	Reactor coolant pressure from wide range pressurizer pressure measurements	To assist the ESF systems in the event of reduction in system pressure
Low steam generator water level	Level of water in each SG down-comer region from wide range	To provide sufficient time for actuating the auxiliary feedwater pumps

[2]Generated from DCD Tier 1, Table 2.5.1-2, "Reactor Trip System Variables."

Reactor Trip Function	Sensed Plant Variable	Reason for Reactor Trip
	differential pressure measurements	
Low steam generator pressure	Steam pressure in each SG	To assist the ESF systems in the event of a steam line break accident
Reactor Coolant Pump Speed	The shaft speed sensor's voltage pulse signal's pulse train frequency	To provide a CPCS auxiliary trip with fewer than two RCPs running

The RCS flow is calculated and derived from indirect measures of the desired parameter. DCD Tier 2 Section 7.2.1.4, "Reactor Trip Initiation Signals," states that the RPS low reactor coolant flow reactor trip is provided to trip the reactor when the differential pressure across the primary side of either SG decreases below a rate-limited variable setpoint or below a preset value. This function is used to provide a reactor trip in an RCP-sheared shaft event. Another indirectly calculated measurement is the CPCS core mass flow rate. The CPCS core mass flow rate calculation, utilized as an input to the CPC DNBR reactor trip, is derived from reactor coolant pump speed and reactor coolant cold leg and hot leg temperatures. SRP Appendix 7.1-C, Section 6.4, "Derivation of System Inputs," states, in part, that variables should be reviewed and its response to postulated events compared with the credit taken for the parameter in the events for which it provides protection. DCD Tier 2 Section 15.3.3, "Reactor Coolant Pump Rotor Seizure," states that following seizure of an RCP rotor, the core flow rapidly decreases and a low coolant flow reactor trip is generated by the RPS. This RPS trip accident analysis conservatively assumes the largest possible delay time for sensor delay, calculation period, CEDM dead time, and CEDM coil decay time. Staff's review of DCD Tier 2 Table 15.3.3-1, "Sequence of Events for the Reactor Coolant Pump Rotor Seizure," show that the low reactor coolant flow trip condition is reached 0.3 seconds after the RCP seizure and that the CEAs would begin to drop 1.5 seconds after RCP seizure. Therefore, the staff finds that, with the exception of reactor coolant flow, the sense and command feature inputs are derived from signals that are direct measures of the desired variables. In addition, RCS flow is derived from indirect measures of the desired variables and the staff has reviewed the indirect measured variable and its response to postulated events where credit is taken for the parameter in the events for which it provides protection and finds it acceptable. As such, the staff finds that the RPS design meets the listed requirements of IEEE Std 603-1991, Clause 6.4.

DCD Tier 1 Table 2.5.1-5, "Reactor Trip System and Engineered Safety Features Initiation ITAAC," Item 15, provides an ITAAC to verify the above listed design basis requirements.

7.2.4.1.3 RPS Design Basis Performance

The guidance of SRP Appendix 7.1-C, states that Clause 4.4 of IEEE Std 603-1991 requires in part the identification of RTS system response times. SRP BTP 7-21 provides guidance for reviewing digital system real-time performance and system architectures in I&C systems and addressing the system response time requirements of IEEE Std 603-1991, Clause 4.4. The staff used the guidance of SRP BTP 7-21 to verify that the RTS timing requirements calculated from the DBEs and other criteria have been allocated to the safety-related I&C system as

appropriate, and have been satisfied in the reactor trip portion of the PPS architectural design and conform to the system response time criteria of Clause 4.4. SRP BTP 7-21 states that the reviewer verifies that system timing requirements calculated from the DBEs and other criteria have been allocated to the digital computer portion of the system as appropriate, and have been satisfied in the digital system architectural design.

The staff reviewed the applicant's system response time technical document, "Response Time Analysis TeR," to determine if the design addressed the listed SRP BTP 7-21 guidance for demonstration of conformance to IEEE Std 603-1991, Clause 4.4, performance requirements. The purpose of the Response Time Analysis TeR is to demonstrate that the sum of individual response time allocated to each component on the instrumentation circuit signal path of safety-related I&C system functions does not exceed the response time assumed in the APR1400 safety analysis. Appendix A, "Conformance to [SRP] BTP 7-21," of the applicant's Response Time Analysis TeR, states how the PPS safety-related I&C system addresses the response time guidance SRP BTP 7-21. The allocation of individual response times to each component on the reactor trip critical signal path of the safety-related I&C system, as well as the reactor trip safety function response time requirement listed in accident analysis Section 15 of the DCD Tier 2, are listed in Section 6, "Response Time Allocation," and Section 7, "Response Time Analysis," of the Response Time Analysis TeR. The applicant list, in Table 15.0-2, "Reactor Protection System Trips Used in the Safety Analysis," and Table 7.2-5, "Reactor Protective Instrumentation Response Time," of DCD Tier 2, the RPS trips which utilized and required in the analyses of the DBE mitigation strategy of the APR1400 safety-related system to postulated plant accidents that are described in Chapter 15, including the setpoint and response times associated with each trip. The analyses take into consideration the response times of actuated devices after the value of the monitored parameter at the sensor has equaled or exceeded the trip setpoint. The staff verified that the above listed reactor trip response time tables in the FSAR and the reactor trip response times as listed in Table 4.1, "Response Time Requirements for Reactor Trip Functions," of the Response Time Analysis TeR, were consistent.

The guidance of SRP BTP 7-21 states that the timing analysis should consider the entire digital instrumentation loop - sensor, transmitter, analog-to-digital converter, multiplexer, data communication equipment, computers, etc., and the like, should be considered.
Section 15.0.0.3, "Reactor Trip System and Engineered Safety Feature Systems Analytical Limit and Delay Times," of DCD Tier 2, defines:

- *Sensor Response Time* - The difference of the value of the monitored parameter when the sensor equals or exceeds the reactor protection system trip setpoint and when the sensor output equals or exceeds the trip setpoint.

- *Reactor Trip Delay Time* - The difference of the sensor output when it equals or exceeds the trip setpoint and when the reactor trip breakers are fully open.

Section 4.1, "Response Time Requirements for Reactor Trip Functions," of the Response Time Analysis TeR, states that response time is measured from the output of the sensor. Section 3.2, "Assumptions," of the Response Time Analysis TeR, states that the response times for the CEDM release time (when the magnetic flux of the CEA holding coils has decayed enough to allow control rod motion) and rod drop time that are assumed in the DCD Tier 2 Section 15, safety analysis, are not included as part of the allocated response times. The PPS reactor trip critical instrumentation circuit signal paths are listed in Table 5.1-1, "Signal Path for Reactor Trip Functions," of the Response Time Analysis TeR. The staff finds that these listed response time

analysis reactor trip circuit path components can be considered the complete reactor trip digital instrumentation loop. The staff's review of the timing analysis analyzed in Section 6, "Response Time Allocation," and Section 7, "Response Time Analysis," of the Response Time Analysis TeR, finds that the analysis considered the entire reactor trip digital instrumentation loop. Therefore, the staff finds that reactor trip timing analysis in the Response Time Analysis TeR addresses the entire digital instrumentation loop design guidance of SRP BTP 7-21.

As an example of staff's response time review, in DCD Tier 2 Section 7.2.1.1, "Reactor Protection System Variables," Item d, it states that the RCPs contain proximity sensors that scan the speed of the RCP. These RCP scanning devices produce a voltage pulse train signal that is input to the CPCS. The frequency of this pulse train is proportional to pump speed. Part of the digital instrumentation loop circuit path includes the RCP pulse speed sensors providing an input into the CPCS. The RCP speed sensor circuit path input into the CPCS is shown in DCD Tier 2, Figure 7.2-14, "Plant Protection System Interface Logic Diagram for Division D." The CPCS will use the RCP speed pulse signal inputs to calculate the mass flow rate. This RCP flow rate is then used in the CPCS for DNBR reactor trip algorithms. The RCP speed input, flow calculation, and calculation of DNBR reactor trip is graphically demonstrated in DCD Tier 2, Figure 7.2-7, "Core Protection Calculator System Functional Block Diagram." As shown in DCD Tier 2 Figure 7.2-13, "PPS Channel Contact Bistable Interface Diagram," the output of the CPCS DNBR trip is a "contact" output signal transmitted to the PPS. DCD Tier 2, Figure 7.2-10, "PPS Channel A Trip Path Diagram," shows the complete digital instrumentation circuit loop from the CPCS to the RTSS. The DBE analysis time requirement for the CPCS low RCP speed reactor trip is shown as 450ms in DCD Tier 2 Table 15.0-2, "Reactor Protection System Trips Used in the Safety Analysis." This 450 millisecond (ms) accident analysis time requirement is carried over and listed in Table 6.11-5, "Response Time Allocation for Primary Coolant Pump Shaft Speed (LDNBR)," and Figure 7.11-13, "Response Time Analysis for Primary Coolant Pump Shaft Speed," of the Response Time Analysis TeR. Staff has verified that the RCP reactor trip speed system timing requirement calculated from the DBEs has been allocated to the digital computer portion of the RTS.

Figure 7.11-13, "Response Time Analysis for Primary Coolant Pump Shaft Speed," Figure 7.11-14, "Response Time Analysis for CPCS," and Figure 7.11-15, "Response Time Analysis for PPS," of the Response Time Analysis TeR, show the allocated timing requirements for the reactor trip digital instrumentation loop safety-related I&C system components. The staff has verified that the RTS timing requirements for Low RCP reactor trip have been calculated from DCD Tier 2 Section 15, DBE accident analysis timing requirement and that this timing requirement feasibility has been demonstrated by the allocation of the timing budget to each component of the digital instrumentation loop of the RTS as appropriate. Staff also notes that the listed "worst case" Response Time Analysis TeR response times do not exceed the listed allocated response times listed in the accident analysis. Staff finds that the allocated response times did not exceed the accident analysis timing requirements, and staff also found that the "worst case" response times did not exceed the allocated response times for the reactor trip portion of the APR1400 safety-related system. Therefore, staff concludes that the applicant's Response Time Analysis TeR, adequately addresses the above listed guidance of SRP BTP 7-21 for the APR1400 RTS. Thus, the staff finds that the APR1400 RPS system response times meet the performance requirements of Clause 4.4 of IEEE Std 603-1991.

In order to maintain the system response times that are sufficient to meet the performance requirements, the CPCS requires additional calculations. In RAI 50-7911, Question 07.02-4, the staff requested the applicant to explain how the validity of the execution interval and dynamic changes of CPCS programs is determined and the actions performed if the execution interval of

the programs or dynamic changes were found to be invalid. In the September 22, 2015, response to this RAI (ML15265A591), the applicant submitted a proprietary response and proprietary markup to the Safety I&C System TeR. The staff's review of the proprietary response and markup found that response addressed the staff's requests in RAI 50-7911, Question 07.02-4. The incorporation of the proposed markups into the next revision of the Safety I&C System TeR was a confirmatory item. The staff verified that the proposed markups have been incorporated into the Safety I&C System TeR, Revision 1. As such, this confirmatory item has been satisfied.

DCD Tier 1 Table 2.5.1-5, "Reactor Trip System and Engineered Safety Features Initiation ITAAC," Item 10, provides an ITAAC to verify the above listed performance design basis requirements.

7.2.4.1.4 RPS Permissive Conditions

Clause 4.3 of IEEE Std 603-1991 requires that the identification of the permissive conditions for each operating bypass capability that is provided. DCD Tier 1 Table 2.5.1-4, "Reactor Trip System and Engineered Safety Features Initiation Bypasses," and DCD Tier 2 Table 7.2-1, "Reactor Protection System Operating Bypass Permissive," list the operating bypasses. The operating bypasses are listed as (1) DNBR Trip and LPD Trip Operating Bypass, (2) High Logarithmic Power Trip Operating Bypass, (3) Low Pressurizer Pressure Trip Operating Bypass. Staff's review found that the permissive conditions are identified in DCD Tier 2 Table 7.2-1, "Reactor Protection System Operating Bypass Permissive." Therefore, the staff finds that the RTS meets the permissive identification requirements of Clause 4.3 of IEEE Std 603-1991.

DCD Tier 1 Table 2.5.1-5, "Reactor Trip System and Engineered Safety Features Initiation ITAAC," Item 7.b, provides an ITAAC to verify the above listed design basis permissive requirements.

7.2.4.1.5 RPS Manual Operator Action Evaluation

Clauses 4.5.1 and 4.5.2 of IEEE Std 603-1991, states that the minimum criteria, such as, (1) points in time and plant conditions during which manual control is allowed and (2) justification for permitting initiation or control subsequent to initiation solely by manual means, for the safety functions and corresponding protective actions of the execute features for each DBE, whose operation may be controlled by manual means initially, to initiation, shall be identified. DCD Tier 2 Section 15.0.0.6, "Operator Action," states that for postulated events where operator action is credited for the mitigation of postulated events, the operator action is not credited until 30 minutes after event initiation. The staff reviewed the APR1400 application for accident analysis mitigation that called for operators to manually initiate the reactor trip safety function. A review of the DCD Tier 2 Section 15 accident analysis provided for two DBEs that listed a manual reactor trip initiation as an accident mitigation strategy. DCD Tier 2 Table 15.1.4-1, "Sequence of Events of Full-Power Inadvertent Opening of a Steam Generator Atmospheric Dump Valve with a Loss of Offsite Power," show that an operator manually initiated reactor trip is a required mitigation. The manual reactor trip is initiated 1800 seconds (30 minutes) after one atmospheric dump valve inadvertently opens. DCD Tier 2 Section 15.1.4.2, "Sequence of Events and Systems Operation," states that for this event, the FWCS, which is assumed to be in the automatic mode, supplies feedwater to the steam generators so that the steam generator water levels are maintained and that reactor power will increase and will stabilize at a higher value. Therefore, the plant will remain in this new, higher power stabilized condition for at least 30 minutes without tripping any automatic protective functions. The

operator will observe and act on the large power mismatch between the reactor and turbine and the audible indication of steam blowdown, recognize that the plant is in an abnormal state, and will then manually trip the reactor. Indications such as steam generator pressure and level, reactor power, reactor temperature (cold and hot leg), at a minimum, should be provided to the operator in the MCR. DCD Tier 2 Table 7.5-1, "Accident Monitoring Instrumentation Variables," show that plant variables are provided to the operator in the MCR which would allow the operator to recognize an inadvertent atmospheric dump valve is fully opened and manually initiate a reactor trip 30 minutes after this recognition. Clause 6.2.2 of IEEE Std 603-1991 states that means shall be provided in the control room to implement manual initiation and control of the protective actions identified in Clause 4.5 that have not been selected for automatic control. SRP Appendix 7.1-C, Section 6.2, "Manual Control," states that features for manual initiation of protective action should conform with RG 1.62, "Manual Initiation of Protection Action," Revision 1. RG 1.62, Revision 1, includes regulatory positions which provide an acceptable method for complying with IEEE Std 603-1991 in regard to the manual initiation of protective actions. One of the RG 1.62, Revision 1, positions states that an acceptable method is a system-level manual initiation of protective actions that results in the actuation of all divisions at once. DCD Tier 2 Figure 7.2-10, "PPS Channel A Trip Path Diagram," shows that the manual reactor trip initiation switch located in the MCR completely bypasses the automatic digital trip logic of the PPS (i.e., bistable processor and LCL voting logic) and is a system-level actuation. In addition, DCD Tier 2 Section 7.2.1.5, "Manual Reactor Trip and Actuated Devices," states that two pairs of manual reactor trip switches are located in the MCR and that both manual trip switches in a pair must be actuated to initiate a reactor trip. Manually actuating a pair of reactor trip switches will result in interruption of the alternating current power to the CEDMs allowing control rods to fall into the core via gravity. DCD Tier 2 Figure 7.2-16, "Manual Reactor Trip Initiation Diagram," show a pair of manual reactor switches, for a division, bypassing the digital voting logic of the PPS. In addition, DCD Tier 2 Table 7.1-1, "Regulatory Requirements Applicability Matrix," Item 40, show that the RTS is designed in accordance with the design guidance of RG 1.62, Revision 1. Therefore, the staff finds that the listed manual reactor switch design addresses the RG 1.62, Revision 1, guidance position for system-level actuation, and thus addresses the listed guidance of SRP Appendix 7.1-C, Section 6.2. The staff also finds the design meets the guidance in SRP Appendix 7.1-C, Section 6.2 and RG 1.62, Revision 1. Specifically, the credited manual reactor trip actuation after 30 minutes of event initiation is acceptable for mitigating an inadvertent opening of an atmospheric dump valve. Therefore, the design meets the requirements of IEEE Std 603-1991, Clause 6.2.2. In addition, the staff finds the design meets the requirements of IEEE Std 603-1991, Clause 4.5 because the applicant identified and documented the minimum criteria to perform the credited manual reactor trip safety function whose operation is controlled by manual means initially.

DCD Tier 1 Table 2.5.1-5, "Reactor Trip System and Engineered Safety Features Initiation ITAAC," Item 4.c, provides an ITAAC to verify the above listed design basis requirements.

7.2.4.2 RPS Independence / Alternative Request Evaluation

The independence of the safety PPS system is evaluated in Section 7.1.4.10 of this SER. An alternative design has been proposed, in lieu of conforming to the regulatory independence requirements, for part of the RTS.

By letter dated December 23, 2014 (ML14357A449), the applicant submitted its request for NRC approval to use an alternative to the independence requirements of IEEE Std 603-1991, Clause 5.6.1, "Between Redundant Portions of a Safety System," to satisfy the requirement of 10 CFR 50.55a(h)(3), for the APR1400 design certification. The applicant's alternative request

proposes to utilize shared CEA position sensors as an alternative to the independent safety division sensor requirement by IEEE Std 603-1991, Clause 5.6.1, “Independence Between Redundant Potions of a Safety System.” The applicant’s letter states that the basis and technical justification for this alternative is provided in Appendix D of the Safety I&C System TeR. The applicant requests approval of this alternative request as part of the staff's SER for their application for design certification of the APR1400.

Background

The independence requirements of IEEE Std 603-1991, Clause 5.6.1, states that redundant portions of a safety-related system provided for a safety function shall be independent of and physically separated from each other to the degree necessary to retain the capability to accomplish the safety function during and following any DBE requiring that safety function. The guidance of SRP Appendix 7.1-C, “Guidance for Evaluation of Conformance to IEEE Std 603,” Clause 5.6, “Independence,” states, in part, that the applicant should confirm that the safety-related system design precludes the use of components that are common to redundant portions of the safety-related system, such as common sensing lines or any other features which could compromise the independence of redundant portions of the safety-related system. The applicant requests the use of shared, redundant, CEA position sensors among all CPCS safety channels as an alternative to separate and independent sensors for each redundant safety-related system channel design requirement. Appendix D, “Alternative to Independence Requirements of IEEE Std 603-1991,” of the Safety I&C System TeR, states that the implementation of the CPCS safety-related system sharing CEA position sensor signals among all CPCS safety channels does not conform to the independence requirements of IEEE Std 603, Clause 5.6.1.

DCD Tier 2 Section 4.2.1.6.1, “Control Element Assembly,” and Section 7.7.1.1, “Control Systems,” state that the CEAs provide core reactivity control and reactivity adjustments for all normal and adverse conditions during reactor startup, operation, shutdown, and accidents. The CEAs can be referred to as control rods. The CEAs are arranged in groups (i.e., shutdown, regulating) and move (i.e., withdrawal and insertion) to control reactivity via sequential group movement. A sequential group movement is a process where one group of CEAs completes its movement in the core before another group of CEAs start to move. It is important that each individual CEA remains aligned with its group’s sequential movement, as well as each CEA group remain aligned within its sequential movement pattern, to prevent the rate of reactivity addition and the worth of individual CEAs from exceeding limiting values.

The CPCS monitors for individual and group CEA position deviation. Each CEA position is measured by two independent reed switch position transmitters (RSPTs) sensors. The RSPT CEA position measurements are raw, analog, electrical signals. The RSPTs transmits these raw CEA analog position signals to the CPCS. The RSPTs do not initiate, actuate, or perform any DBE safety mitigation functions or protective actions. The CPCS will monitor for individual and group CEA position deviations and will calculate CEA deviation “penalty factors” for CEAs that are out of group alignment and/or not following correct group sequential movement. The CPCS will determine the magnitude of CEA deviation penalty factors based upon the raw analog CEA position sensor signal inputs obtained from the RSPTs. The CPCS will utilize the CEA deviation penalty factors as one of several plant variable inputs to its reactor trip initiation logic to calculate and generate low DNBR and high LPD trip actuation signals.

The independence requirements of IEEE Std 603-1991, Clause 5.6.1 require each safety channel of the CPCS (total of four CPCS safety channels) to acquire CEA position

measurements from within its own safety channel (requiring a total of four independent RSPTs). Therefore, adhering to the regulatory independence requirement, failure of one of the required four RSPTs (only affecting one CPCS safety channel) would not affect the other three CPCS safety channels DNBR or LPD reactor trip calculations or rector trip safety function actuations. However, the APR1400 is designed with only two RSPTs and these two RSPT CEA position signals are shared among all CPCS channels.

Appendix D of the Safety I&C System TeR states that to design and implement each CPCS safety channel with an individual, independent, RSPT sensor, would result in a total of four independent and separate RSPT measurement assemblies (one for each CPCS safety channel). However, the applicant states that this is not possible due to the physical constraints of the CEA and reactor head geometry. Therefore, the applicant request to use two RSPTs and share the two RSPT sensor measurements among all CPCS channels.

As stated in the Safety I&C System TeR, Section C.5.1.3.2, "Divisional Independence," and the DCD Tier 2 Section 7.2.1.1, "Reactor Protection System Variables," the RSPTs transmit the raw CEA analog position signals to all four CPCS channels. Reactor trip initiation logic is contained in the CPCS and performed within the CPCS safety divisions. The RSPTs do not contain reactor trip logic, do not perform reactor trip setpoint comparison, or reactor trip initiation mitigation protective actions.

Regulatory Requirements for Evaluation of Proposed Alternative

10 CFR 52.48, "Standards for Review of Applications," states in part, that applications filed under 10 CFR Part 52, Subpart B, "Standard Design Certifications," will be reviewed for compliance with the standards set out in 10 CFR Part 50 and its appendices. 10 CFR 50.55a, "Codes and Standards," paragraph (h)(3), "Safety Systems," states, in part, that applications filed on or after May 13, 1999, for design approvals and design certifications, under Part 52, must meet the requirements for safety-related systems in IEEE Std 603-1991 and the correction sheet dated January 30, 1995. Specifically, the design certification application must demonstrate conformance to the safety-related system independence requirements of IEEE Std 603-1991, Clause 5.6.1, "Between Redundant Portions of a Safety System," which states:

> Redundant portions of a [safety-related] system provided for a safety function shall be independent of and physically separated from each other to the degree necessary to retain the capability to accomplish the safety function during and following any design basis event requiring that safety function.

However, 10 CFR 50.55a, paragraph (z), "Alternatives to codes and standards requirements," Criterion Item (1), states that for proposed alternatives to the requirements of paragraph (h), an applicant must demonstrate that the proposed alternative would provide an acceptable level of quality and safety. Therefore, the applicant's request to implement the proposed alternative to the independence requirements of IEEE Std 603-1991, Clause 5.6.1, must demonstrate an acceptable level of quality and safety for NRC approval in order to implement the proposed alternative. The staff has evaluated the proposed alternative design for requisite quality and safety by evaluating the request's conformance to the following regulatory requirements:

- 10 CFR 50.55a(h)(3), "Safety Systems," states that applications filed on or after May 13, 1999, for design approvals, design certifications, and combined licenses under part 52 of this chapter, must meet the requirements for safety-related systems in IEEE Std 603 -1991 and the correction sheet dated January 30, 1995. Staff will evaluate the

alternative proposal to the quality requirements of IEEE Std 603-1991, Clause 5.3, "Quality," which requires, in part, that safety-related system equipment shall be designed, manufactured, inspected, installed, tested, operated, and maintained in accordance with a prescribed quality assurance program.

- 10 CFR Part 50, Appendix A, GDC 13, "Instrumentation and Control," requires that instrumentation shall be provided to monitor variables and systems over their anticipated ranges for normal operation, for AOOs, and for accident conditions as appropriate to assure adequate safety, including those variables and systems that can affect the fission process, the integrity of the reactor core, the reactor coolant pressure boundary, and the containment and its associated systems. Appropriate controls shall be provided to maintain these variables and systems within prescribed operating ranges.

- 10 CFR Part 50, Appendix A, GDC 21, "Protection System Reliability and Testability," requires that the protection system be designed for high functional reliability and in-service testability commensurate with the safety functions to be performed. Redundancy and independence designed into the protection system shall be sufficient to assure 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 testing of its functioning when the reactor is in operation, including a capability to test channels independently to determine failures and losses of redundancy that may have occurred.

- 10 CFR Part 50, Appendix A, GDC 23, "Protection System Failure Modes," requires that the protection system be designed to fail into a safe state or into a state demonstrated to be acceptable on some other defined basis if conditions such as disconnection of the system, loss of energy (e.g., electric power, instrument air), or postulated adverse environments (e.g., extreme heat or cold, fire, pressure, steam, water, and radiation) are experienced.

Regulatory Guidance for Evaluation of Proposed Alternative

The staff will utilize the following guidance to evaluate the proposed alternative's request conformance to the above listed regulatory requirements:

- NUREG-0800, SRP Revision 5, March 2007.

- RG 1.53, Revision 2, which endorses, IEEE Std 379-2000, provides methods acceptable to the staff for satisfying the NRC's regulations with respect to the application of the single failure criterion to the electrical power, instrumentation, and control portions of nuclear power plant safety-related systems.

- RG 1.75, Revision 3, which endorses IEEE Std 384-1992, provides a method that the staff considers acceptable for satisfying the agency's regulatory requirements concerning physical independence of the circuits and electrical equipment that comprise or are associated with safety-related systems, subject to the listed provisions.

- RG 1.151, Revision 1, provides an approach that the staff considers acceptable for satisfying the agency's regulatory requirements with respect to designing and installing safety instrument sensing lines in nuclear power plants.

Alternative Proposal Technical Evaluation

The proposed alternative design consists of sharing sensor inputs (RSPTs) among redundant safety-related system divisions and then sharing the RSPT incoming analog signals (CEA position signals) among all safety-related system divisions. The applicant's non-conformance to regulatory independence is graphically displayed in DCD Tier 2 Figure 7.2-4, "CEA Position Signal Flow for CPCS." As shown:

- RSPT1's CEA analog signal inputs are connected to both safety divisions A and B.
- RSPT2's CEA analog signal inputs are connected both to safety divisions C and D.
- Each safety division's CPP output signals are transmitted to all redundant and independent safety divisions.

The Safety I&C System TeR provides several different terms to describe the center CEA (i.e., CEA 1, CEA01). In addition, the Safety I&C System TeR, Section C.5.1.3.2, "Divisional Independence," that the center CEA is assigned to Channel B. However, Table C.5.1-1, "RSPT1 and RSPT2 Channel Assignment," and Figure 4-8, "CPCS Block Diagram," of the Safety I&C System TeR, show the center CEA is going to CPCS safety channels B and C. The staff requested the applicant in RAI 50-7911, Question 07.02-7, to provide a consistent definition and acronym for the center CEA and to clarify the assignment of the center CEA to the CPCS channels. In the September 22, 2016, response to RAI 50-7911, Question 07.02-7 (ML15265A594), the applicant provided a markup that revised the Safety I&C System TeR to define the acronym for the center CEA to be "CEA01" and also changed the design descriptions to state that the center CEA is assigned to both CPCS safety channels B and C. The staff finds that these revised design descriptions address staff's RAI request by defining the acronym and clarifying in the proposed markups that the center CEA is assigned to both CPCS safety channels B and C. The incorporation of the proposed markups into the next revision of the Safety I&C System TeR was a confirmatory item. The staff verified that the proposed markups have been incorporated into the Safety I&C System TeR, Revision 1. As such, this confirmatory item has been satisfied.

Alternative Request Evaluation for Acceptable Level of Safety

The staff evaluated the RSPT alternative request for requisite electrical and physical independence. The guidance of SRP Appendix 7.1-C, Section 5.6, states, in part, that electrical independence should include the utilization of separate power sources and that physical independence is attained by physical separation and physical barriers. The guidance of IEEE Std 384-1992, Section 5.1, "Required Independence," states that physical separation and electrical isolation shall be provided to maintain the independence of Class 1E circuits and equipment so that the safety functions required during and following any DBE can be accomplished. The Safety I&C System TeR states in Section 4.2.2.1, "General," that the safety-related system is configured with redundant internal power supplies in each cabinet and that the direct current output is auctioneered. The staff was not able to verify how the RSPT's are powered and therefore could not review them for requisite electrical independence.

The staff issued RAI 50-7911, Question 07.02-3, to request the applicant to provide diagrams and figures to demonstrate CEA functional design in accordance with CPCS safety-related system operation and FMEA and to update the APR1400 application accordingly. On September 22, 2015, the applicant responded to RAI 50-7911, Question 07.02-3 (ML15265A594). In Item "e)" of the response, the applicant provided proprietary Figure 4, "CPCS Block Diagram for FMEA." This figure shows that the electrical power supply for the RSPT analog inputs are supplied per independent and separate CPCS safety divisions via auctioneered power of that division. The single failure of auctioneered power of one independent CPCS safety division does not affect the RSPT power supply of the other three CPCS safety divisions. The failure of CPCS safety division A's RSPT power supply will not affect the other three independent CPCS safety division's RSPT power supplies. Item "e)" of RAI 50-7911, Question 07.02-3, addressed the staff's RAI request for RSPT power supply design.

As shown in DCD Tier 2, Revision 0, Figure 7.2-4, "CEA Position Signal Flow for CPCS," the RSPT's analog sensor inputs are separated (23 CEA inputs and 70 CEA inputs) and connected to separate and independent CPCS safety channels. As stated in DCD Tier 2, Revision 0, Section 7.2.1.1, "Reactor Protection System Variables," Item b, "CEA Position Measurements," the two RSPT assemblies and wiring (e.g., RSPT1 and RSPT2) are physically and electrically separated from each other. Section C.5.1.3.2, "Divisional Independence," of the Safety I&C System TeR, states that the RSPT is a Class 1E measurement device. DCD Tier 2 Section 7.1.2.42, states that the instrumentation for the safety electric systems complies with the requirements of IEEE Std 384-1992 as endorsed by RG 1.75, Revision 3. DCD Tier 2 Table 7.1-1, "Regulatory Requirements Applicability Matrix." Item 41, show that the RTS will be designed in accordance with the design guidance of RG 1.75, Revision 3.

Based on the applicant statements that: (1) the RSPT design requirement of the RSPT sensor analog inputs will be connected to separate and independent CPCS safety channels, (2) power will be supplied to the separate RSPT sensor analog input connections from independent and separate CPCS safety channels, and (3) the design commitment to conform to the RG 1.75, Revision 3, physical independence and separation implementation requirements for Class 1E equipment, the staff finds that the RPST alternative request addresses the applicable electrical independence and physical separation guidance of IEEE Std 384-1992 as endorsed by RG 1.75, Revision 3, and SRP Appendix 7.1-C, Section 5.6.

There are four CPCS safety divisions. Each CPCS safety division is independent from the others. The CPCS safety divisions do not share power between divisions. The safety-related I&C system cabinets for each division are geographically distributed into four separate, divisionalized I&C equipment rooms. Equipment and circuits of the CPCS and PPS safety divisions are implemented with four-division, physical separation and electrical isolation that are designed and implemented in accordance with the guidance of IEEE Std 384-1992, as endorsed by RG 1.75, Revision 3. This design commitment is also shown in DCD Tier 2 Table 7.1-1, "Regulatory Requirements Applicability Matrix," Item 41. Section C.5.1.3.7, "DI&C-ISG-04 Staff Positions," of the Safety I&C System TeR, states that the SDL among CPCS channels are fiber-optically isolated between channels to meet the separation criteria of IEEE Std 384-1992 and RG 1.75, Revision 3. Based on the above-listed CPP design requirements for electrical independence and physical separation, and the design commitment to conform to the RG 1.75, Revision 3, physical independence and separation implementation guidance for Class 1E equipment, the staff finds that the CPCS signal sharing between safety divisions, as proposed in the alternative request, addresses the applicable electrical

independence and physical separation guidance of RG 1.75, Revision 3, and SRP Appendix 7.1-C, Section 5.6.

In order to determine if the sharing of the RSPT's CEA analog position input signals among all CPCS safety channels is acceptable, the staff evaluated for conformance to the design criterion of GDC 21, "Protection System Reliability and Testability." GDC 21 requires, in part, that the protection system shall be designed for high functional reliability and that redundancy and independence are designed into the protection system sufficient to assure 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 guidance of SRP Appendix 7.1-A, "Acceptance Criteria and Guidelines for Instrumentation and Control Systems Important to Safety," Item 2(j), states that the review of compliance with GDC 21 should address the guidance of SRP Appendix 7.1-C, Section 5.5, "System integrity." SRP Appendix 7.1-C, Section 5.5, guidance states that the review of system integrity should confirm that the design provides for safety-related systems to fail in a safe state or into a state that has been demonstrated to be acceptable on some other defined basis, if conditions such as disconnection of the system, are experienced, and that this system integrity failure analysis aspect is typically evaluated through evaluation of the applicant's FMEA. The analysis should justify the acceptability of each postulated failure.

The APR1400 FMEA applicable for this RSPT evaluation is located in DCD Tier 2, Revision 0, Table 7.2-7, "Failure Mode and Effects Analysis for the Plant Protection System" (herein after referred to as FMEA Table 7.2-7). However, the staff's review of several of the APR1400 application documents found inconsistencies between several of the terms used in FMEA Table 7.2-7. The staff issued RAI 328-8422, Question 04.04-08, Subpart No. 11, to request the applicant to review the design descriptions of the CPCS in the FSAR and its referenced technical documents to ensure consistency of the terminology used in FMEA Table 7.2-7 and to provide definitions for the terms used, such as "pre-assigned" and "pre-determined" penalty factor. In addition, the staff issued RAI 488-8617, Question 07.02-17, requesting the applicant to provide a consistent and unambiguous definition for the CPCS maximum penalty factor value when two CPCS CEACs become inoperable.

On July 16, 2016, the applicant responded to the staff's request in RAI 488-8617, Question 07.02-17 (ML16198A008), and on August 3, 2016, the applicant responded to the staff's request in RAI 328-8422, Question 04.04-08, Subpart No. 11 (ML16216A636). In order to address the staff's request to provide consistency and clarity of terms used in the APR1400 application, the applicant's responses provided the following revisions and definitions:

- The term of "Last Valid" penalty factor will be replaced with "<u>Last Good</u>" penalty factor.
- "Pre-assigned penalty factor" and "Pre-determined penalty factor" will be replaced with "<u>Pre-selected</u> penalty factor."

The RAI responses also provided terminology definitions of:

- "<u>Last Good</u>" penalty factor position is a value which is received from the sending processor when the quality is good.

- "Pre-selected penalty factor" is the CPCS DNBR and LPD penalty factors selected when both CEACs become inoperable due to CEACs failure.

The applicant proposed to revise the FSAR to include the proposed terminology changes and definitions. The staff finds that this information provided the clarity and consistency in design descriptions as requested by the staff, and therefore, the staff considers the responses to RAI 488-8617, Question 07.02-17 and RAI 328-8422, Question 04.04-08, Subpart No. 11 acceptable. The incorporation of the response's proposed FSAR markups into the next revision of the FSAR was a confirmatory item. The staff verified that the markups to RAI 328-8422, Question 04.04-08, Subpart No. 11, and RAI 488-8617, Question 07.02-17, have been incorporated into Revision 1 of the FSAR. As such, these confirmatory items have been satisfied.

The staff did not understand several phrases used in the FMEA Table 7.2-7, with respect to the description of the resultant CPCS reactor trip logic. The staff issued RAI 50-7911, Question 07.02-9 to request the applicant to describe what is meant when stating in FMEA Table 7.2-7 that the coincidence logic is "changed" or "converted," as listed in FMEA Table 7.2-7 column titled "Effect on PPS." In the December 3, 2015, response to RAI 50-7911, Question 07.02-9 (ML15337A379), the applicant clarified that where the resultant logic currently states "converts to," that this term will be changed to "resulting logic becomes," and where the resultant logic states "changes to," this terminology will be changed to "becomes." The staff finds this information provided in the response to RAI 50-7911, Question 07.02-9 provides clarity and is acceptable. The incorporation of the proposed FSAR markups into the next revision to the FSAR was a confirmatory item. The staff verified that the proposed markups have been incorporated into the applicable sections of Revision 1 of the FSAR and Revision 1 of the Safety I&C System TeR. As such, these confirmatory items have been satisfied. In addition, the staff could not identify definitions for several other terms used in FMEA Table 7.2-7. The staff issued RAI 50-7911, Question 07.02-11 requesting the applicant to define and explain the meaning of the term "quality margin" as it relates to DCD Tier 2, Revision 0, FMEA Table 7.2-7. In the September 22, 2015, response to RAI 50-7911, Question 07.02-11 (ML15265A594), the applicant explained that quality margin is the difference between the quality limit and the calculated value of quality as discussed in Section 4.2.7, "Update of DNBR and Quality Margin," in the CPCS TeR. The response provided FSAR markups that would add the definitions for quality and quality margin in FMEA Table 7.2-7. The staff finds that the RAI response is acceptable because the applicant provided adequate definitions for the term, "quality margin." The incorporation of the proposed FSAR markups into the next revision to the FSAR was a confirmatory item. The staff verified that the proposed markups have been incorporated into the applicable section of Revision 1 of the FSAR. As such, these confirmatory items have been satisfied.

DCD Tier 2, Revision 0, Section 3.9.4.1.1.4, "RSPT Assembly," states that the RSPTs consist of reed switches and voltage divider networks that are used to provide two independent output voltages. As stated in DCD Tier 2, Revision 0, Section 7.2.1.1, "Reactor Protection System Variables," Item b, "CEA Position Measurements," when the CEAs move, a permanent magnet at the top of the CEA extension shaft actuates the RSPT reed switches as it passes them. The actuation of the RSPT's voltage divider networks, as the CEA moves, produces voltages that are proportional to the position of the CEA. DCD Tier 2, Figure 7.2-3, "Reed Switch Position Transmitter Assembly Schematic," provides a graphical representation of the RSPT voltage divider network. Proprietary Figure 4, "CPCS Block Diagram for FMEA," of Item "e)" of the RAI response to RAI 50-7911, Question 07.02-3, shows that the electrical power supply for the RSPT voltage divider network is supplied per independent and separate CPCS safety division

via auctioneered power. As shown in DCD Tier 2, Figure 7.2-4, "CEA Position Signal Flow for CPCS," the RSPT electrical voltage divider network analog sensor inputs are separate and individually connected to each CPCS safety channel.

The FMEA Table 7.2-7, provides a system analysis for postulated RSPT single failures. There are several types of RSPT failures that are analyzed: (1) "In-range" and "out-of-range" RSPT failures, as well as (2) detected and un-detected RSPT failures. FMEA Table 7.2-7, entry item Nos 2-4 and 2-5, provide the safety-related system single failure analysis for RSPT loss of power, power malfunctions, as well as RSPT voltage divider network malfunctions. In all RSPT single failure FMEA entry items, the postulated RSPT single failures do not affect or disable the ability of the CPCS or the RTS to accomplish its safety function. FMEA Table 7.2-7 states that a cause for failure of an excessive number of RSPT CEA analog position inputs can be an RSPT loss of power. The staff needed further clarification for several listed FMEA Table 7.2-7 failure terms. The staff issued RAI 274-8277, Question 07.01-40 to request the applicant to clarify the terms used in DCD Tier 2 Table 7.2-7, "Failure Mode and Effects Analysis for the Plant Protection System." The staff requested the applicant to clarify why an improper CEA position renders a CPC inoperable and changes the voting logic, and to explain what the terms, "Unrecognized software malfunctions," "Erroneous CEA position transmission and indication," and "Improper CEA position," mean with respect to the failure analysis. In the October 26, 2016, supplemental response (ML15363A343), the applicant provided a new proprietary figure, Figure 4-9a, "CEA Position and penalty factor Movement," that will be added to the Safety I&C System TeR, to address the staff's request in RAI 274-8277, Question 07.01-40. The response provided additional descriptions of requested terms related to the failure analysis. The response's FSAR markups include the following definitions in the DCD Tier 2, FMEA Table 7.2-7:

- *Unrecognized software malfunctions*: Software failures which cannot be detected by system and application diagnostics.

- *Improper CEA positions*: Erroneous CEA positions which cannot generate the DNBR/LPD trip.

- *Erroneous CEA position transmitted:* When CEA values are different from reading values transmitted from the analog input modules to the CPP/CEAC/CPC processors.

The response's proprietary Figure 4-9a provides a graphical representation of the CPP and CEAC RSPT CEA position signal processing selection strategy of sensed CEA position signals. Upon the staff's review of RAI 274-8277, Question 07.01-40 proprietary Figure 4-9a, the staff found several errors upon comparison with other figures. The staff informed the applicant of these errors and requested the applicant to provide a supplemental response that corrects the errors. RAI 274-8277, Question 07.01-40 was tracked as an open item. The applicant provided a response on February 10, 2017 (ML17041A188), to RAI 274-8277, Question 07.01-40, and then supplemental response (ML17214A240) on August 2, 2017, to RAI 274-8277, Question 07.01-40. These revised responses include markups that provide corrections to FSAR and Safety I&C System TeR figures and corrected errors in the FMEA Table 7.2-7. The markups included requested definitions for terms and terminology that had not been defined within the application, corrections to FMEA Table 7.2-7 single failure entry topics, as well as corrections to CPCS figures in the FSAR and Safety I&C System TeR. The staff finds that these corrections address the issues that staff raised in the request and finds them acceptable. The staff verified that the proposed markups have been incorporated into Revision 1 of the

FSAR and Revision 1 of the Safety I&C System TeR, and thus, the RAI 274-8277, Question 07.01-40 confirmatory items have been satisfied. The staff utilized the RAI response's clarifications and proprietary design information, in its evaluation for RSPT failures.

[

]. IEEE Std 603-1991 defines "channel" as "An arrangement of components and modules as required to generate a single protective action signal when required by a generating station condition." The staff considers the arrangement of CPP1/CEAC1 and CPP2/CEAC2 to be two "safety channels," in accordance with IEEE Std 603-1991, within a CPCS safety division, which utilize the inputs from two separate RSPT instrument sensors to generate the protective action signal.

DCD Tier 2 Chapter 16, "Technical Specifications," Subpart B 3.3.3, "CEACs," states that each CPCS CPC directly monitors one "target CEA" from each subgroup and uses this information to account for excessive radial peaking factors for events involving CEA groups out of sequence and subgroup deviations within a group, without the need for CEACs. [

]. Upon reviewing the technical report, "Functional Design Requirement for a CPCS for APR1400," staff was not able to understand the functional design and relationship between CEA groups, CEA subgroups, and CEA control groups. The staff issued RAI 50-7911, Question 07.02-3, requesting the applicant to demonstrate CEA functional design in accordance with CPCS safety-related system operation and failure mode analysis and update the application accordingly.

In the September 22, 2015, response to RAI 50-7911, Question 07.02-3 (ML15265A594), the applicant provided two figures and additional design descriptions to explain the relationship between groups, subgroups, and CEAs. The RAI response states that the CEAs are divided into four quadrant symmetric sets that are symmetrical about the center of the reactor core and that a subgroup is composed of four CEAs, one from each quadrant set. These subgroups are the "target CEAs" whose position within a quadrant is sent directly to the corresponding CPCS safety division for direct monitoring by the CPC of a CPCS safety division. [

]:

- [

  ].
- [

  ].

[

]:

- [

  ].
- [

  ].
- [

  ].

The staff finds that the RAI 50-7911, Question 07.02-3 response addressed the staff's request because the applicant identified the FSAR sections that included the staff's requested design information regarding the CEA and RAI 50-7911, Question 07.02-3 is closed and resolved.

The guidance of SRP Appendix 7.1-C, Section 5.5, states, "that computer-based safety-related systems should, upon detection of inoperable input instruments, automatically place the protective functions associated with the failed instrument(s) into a safe state (e.g., automatically place the affected channel(s) in trip), unless the operator has already placed the affected channel in a bypass mode." However, the staff could not identify design descriptions that would fully describe and explain what happens when a CPCS processor(s) declares itself to be "failed" or inoperable, or when a CPCS processors senses that another processor is failed or inoperable. Therefore, the staff issued RAI 274-8277, Question 07.01-39 to request the applicant to describe what happens to the output of safety-related I&C system processors when the processor is declared inoperable. In the December 29, 2015, response to RAI 274-8277, Question 07.01-39 (ML15363A343), the applicant stated that the output of the safety-related I&C system processors stay in a "non-trip" state when the processor is declared inoperable. The response also provided FSAR markups to include (1) the definition of an inoperable safety-related I&C processor to FMEA Table 7.2-7, and that (2) the output of the safety-related I&C system processors stay in a "non-trip" state when the processor is declared inoperable. The staff finds this response is acceptable because the applicant provided design commitments

in the FSAR to specify what the outputs of the safety-related I&C system processors will be when the processor is declared inoperable. The incorporation of the proposed markups into the next revision of the FSAR was a confirmatory item. The staff verified that the proposed markups have been incorporated into Revision 1 of DCD Tier 2 Table 7.2-7. As such, this confirmatory item has been satisfied.

The staff reviewed the RSPT FMEA results to verify that the design addresses the above listed guidance. However, the staff was not able to find FMEA results information that describe what system, component, and/or processor senses and makes the determination that CEA position data is unavailable. In RAI 50-7911, Question 07.02-8, the staff requested the applicant to explain and describe the complete safety-related system actions performed to detect and mitigate against the unavailability of preferred CEA position data. In the September 22, 2015, response to RAI 50-7911, Question 07.02-8 (ML15265A591), [ ]:

- [ ].
- [ ].
- [ ].
- [ ].

[ ]:

- [ ].
- [ ].

The response to RAI 50-7911, Question 07.02-8, also provided several new FMEA Table 7.2-7 failure entries markups. The staff reviewed the new FMEA Table 7.2-7 FSAR markups and found these new entries to be acceptable. The staff finds that the RAI response adequately addressed the staff's request and is acceptable because the applicant adequately described the safety-related system actions performed to detect and mitigate against the unavailability of preferred CEA position data. The incorporation of the proposed FMEA Table 7.2-7 FSAR markups into the next revision of the FSAR was a confirmatory item. The staff verified that the proposed markups have been incorporated into the Revision 1 of FSAR, FMEA Table 7.2-7. As such, this confirmatory item has been satisfied.

FMEA Table 7.2-7 provides several resultant failure mode outcomes for postulated RSPT single failures, as described, below.

- [ ]:
  - [ ].
  - [ ].
  - [ ].
- [ ].
- [ ].
- [ ].

]

However, upon further review, it was not clear to the staff how the CPCS system would respond to a complete failure of both RSPT instrument signals or both CEACs within a CPCS safety division failing (due to single safety division's power supply failure). GDC 23 requires the protection system to be designed to fail into a safe state or into a state demonstrated to be acceptable on some other defined basis if conditions such as disconnection of the system, loss of energy (e.g., electric power, instrument air), or postulated adverse environments (e.g., extreme heat or cold, fire, pressure, steam, water, and radiation) are experienced. The staff requested the applicant, in RAI 274-8277, Question 07.01-37, to discuss how the system would respond if both the RSPT instruments were failed or if both CEACs within a CPCS safety division have failed. In the December 29, 2015, response to this RAI 274-8277, Question 07.01-37 (ML15363A343), the applicant stated that upon the CPC sensing that both RSPTs have failed, which also means the CPC has lost its target CEA position input signals, the CPC will automatically generate the DNBR and LPD reactor trip signals. The response also stated that if the CPC senses that both CEACs of its safety division have failed (inoperable) without subsequent changes in status (i.e., remain inoperable), the CPC will revert to utilize a "pre-determined penalty factor" whose value is large enough to initiate the DNBR and LPD trips. In the August 3, 2016 response to RAI 328-8422, Question 04.04-8, Subpart No. 11 (ML16242A432), the applicant stated that the penalty factor term used for the v will be large enough to initiate a plant trip is "Pre-selected penalty factor." Therefore, upon sensing that both CEACs have failed within its same safety division, the CPC, after a time delay, will revert to a "Pre-selected penalty factor" value which will be a value large enough to result in a reactor trip at any level. The staff finds that the failure design for both RSPTs failed or both CEACs within a CPCS division failed addresses the listed guidance of SRP Appendix 7.1-C, Section 5.5. The staff also finds that the CPCS failure design, based on FMEA Table 7.2-7 FMEA results and design strategy when sensing either both RSPTs or both CEACs within a CPCS safety division have failed, meets the above listed requirements of GDC 23.

[

].

RG 1.53, Revision 2 provides guidance on the application of the single failure criterion to the electrical power, instrumentation, and control portions of nuclear power plant safety-related systems. DCD Tier 2 Section 7.1.2.40 states that applicable I&C systems comply with the requirements of IEEE Std 379-2000, as endorsed by RG 1.53, Revision 2. DCD Tier 2 Table 7.1-1, "Regulatory Requirements Applicability Matrix," shows that the RTS is required to be designed in accordance with RG 1.53, Revision 2.

Based upon the resolution of the open items discussed above and demonstration that the CPCS RSPT sharing meets the single failure criterion, the staff determined that the proposed alternative request to share RSPT analog input signals among all CPCS safety divisions provides an acceptable level of safety in accordance with the alternative request criterion of 10 CFR 50.55a(z)(1).

Alternative Request Evaluation for Acceptable Level of Quality

Clause 5.3 of IEEE Std 603-1991, "Quality," states, in part, that safety-related system equipment shall be designed, manufactured, inspected, installed, tested, operated, and maintained in accordance with a prescribed quality assurance program. Section D.3, "Reason for Alternative Request," of the Safety I&C System TeR states the CEA position measurements for the positions of the CEAs within the reactor core is performed with the Class 1E RSPTs. The guidance of SRP Appendix 7.1-C, Section 5.4, "Equipment Qualification," states that mild environment qualification should conform with the guidance of IEEE Std 323, "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations." DCD Tier 2 Section 3.9.4.2, "Applicable CEDM Design Specifications," states that the RSPT assemblies are designed to conform with IEEE Std 323-2003 and IEEE Std 344-2004 and that the RSPT electrical components are external to the pressure boundary and are non-pressurized. DCD Tier 2 Table 3.11-3, "Equipment Qualification Equipment List," states that the RSPT Type I and II cable assemblies are qualified and implemented for harsh environmental conditions and harsh radiation conditions. The guidance of SRP Appendix 7.1-A, Section 2, "10 CFR Part 50 Appendix A, General Design Criteria," Item (e), states in part that the review of compliance with GDC 13 should include consideration of the protection of instrument sensing lines from environmental extremes. RG 1.151, Revision 1, describes a method that the staff considers acceptable for use in complying with the agency's regulations with respect to the design and installation of safety instrument sensing lines in nuclear power plants. Section 7.1.2.46, "Conformance with RG 1.151," Revision 1, of DCD Tier 2, states that instrument sensing lines comply with RG 1.151, Revision 1. DCD Tier 2 Table 7.1-1, "Regulatory Requirements Applicability Matrix," shows that the RTS, which is composed of the CPCS, will comply with the design and implementation guidance GDC 13 and the guidance of RG 1.151, Revision 1. Based on the listed RSPT quality design and implementation commitments, the staff finds that the RSPT alternative request provides an acceptable level of quality which conforms with the listed quality criterion of GDC 13 and the acceptable level of quality required by 10 CFR 50.55a(z)(1). Staff also finds that based on the acceptable quality design and implementation guidance, as listed above, that the APR1400 RSPTs are committed to be design to, as well as meeting the listed quality criterion of GDC 13, staff concludes that the RSPT design and implementation meets the listed quality criterion of Clause 5.3 of IEEE Std 603-1991.

Conclusion for Alternative Request

Based on the resolution of the open item associated with RAI 274-8277, Question 07.01-40, and the safety findings listed above, the staff finds that the alternative design request to share RSPT analog sensor signals among all CPCS safety channels provides an acceptable level of quality and safety and the staff finds that the alternative design request conforms to the regulatory criterion of 10 CFR 50.55a(z)(1), "Alternatives to codes and standards requirements." The staff also finds that applicant's request to use an alternative (i.e., to utilize shared RSPT CEA position sensors as an alternative to the independent safety division sensor requirement by IEEE Std 603-1991, Clause 5.6.1) to the independence requirements of IEEE Std 603-1991, Clause 5.6.1 is acceptable and approved.

7.2.4.3 RPS Single Failure Criterion Evaluation

10 CFR Part 50, Appendix A, GDC 21, requires that the protection system be designed for high functional reliability and in-service testability commensurate with the safety functions to be performed. Redundancy and independence designed into the protection system shall be sufficient to assure 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. In addition, IEEE 603-1991, Clause 5.1, "Single Failure Criterion," states that the safety-related systems shall perform all safety functions required for a DBE in the presence of: (1) any single detectable failure within the safety-related systems concurrent with all identifiable but non-detectable failures; (2) all failures caused by the single failure; and (3) all failures and spurious system actions that cause or are caused by the DBE requiring the safety functions. The guidance of SRP Appendix 7.1-C, "Guidance for Evaluation of Conformance to IEEE Std 603 Review Responsibilities," Section 5.1, "Single Failure Criterion," states that guidance for the application of the single failure criterion is provided in RG 1.53, Revision 2.

The APR1400 RTS is a safety-related system. The safety function of the RTS is to initiate a reactor trip to rapidly insert the control rods into the core. A successful APR1400 reactor trip safety function will interrupt power to the CEDM coils and allow all CEAs to drop into the core by gravity. CEA's are control rods that insert negative reactivity into the core, which reduces power. As stated in DCD Tier 2 Section 7.2.1, "System Description," the RTS safety function protects the core fuel design limits and the RCS pressure boundary following AOOs and provides assistance in mitigating the consequences of PAs. Therefore, postulated single failures should not prevent the RTS from initiating a reactor trip safety function.

The staff utilized the guidance of IEEE Std 379-2000, in accordance with the provisions stated in RG 1.53, Revision 2, to evaluate the RTS design for conformance to the single failure criterion. The following sections document the staff's evaluation of the RTS design conformance to the above listed single failure criterion.

The staff's evaluation of GDC 21 and IEEE Std 603-1991, Clause 5.1 with respect to the data communication system is discussed in Section 7.9.4.4 of this SER. The staff's evaluation of GDC 21 and IEEE Std 603-1991, Clause 5.1 with respect to independence is discussed in Section 7.1.4.10 of this SER. The staff's evaluation of GDC 21 with respect to capability for test (including self-test diagnostics) and calibration is discussed in Section 7.1.4.11 of this SER.

RTS Performance Assumptions for Evaluating the Single Failure Criterion Conformance

DCD Tier 1, Section 2.5.1.1, "Design Description," states that each LCL receives trip signals from four channels of bistable processors and utilizes 2oo4 coincidence logic to actuate RTS safety functions. The RTS coincidence logic is changed to 2oo3 coincidence actuation logic whenever a safety channel is placed in the trip channel bypass condition. DCD Tier 2 Section 7.2.1.5, "Manual Reactor Trip and Actuated Devices," states that a minimum of two divisions of RPS trips are required for a reactor trip. Therefore, two independent safety divisions or two independent safety channels are considered the minimum redundancy necessary to prevent loss of the RTS safety function. Thus, postulated single failures should not result in less than two operable independent RTS safety divisions or safety channels.

RTS Shared and Interconnected Systems Evaluation for Single Failure Criterion Conformance

SRP Appendix 7.1-C, Section 5.1, "Single Failure Criterion," states that any single failure within the safety-related system shall not prevent proper protective action at the system level when required. IEEE Std 379-2000, Clause 6.2, "Systems Portion Analysis," states that when performing the single failure analysis, certain portions of the safety-related systems require considerations that may be unique. As stated in DCD Tier 2 Section 7.2.1.1, "Reactor Protection System Variables," Item b, states that the CPCS's RSPT signals are transmitted to the CEACs through the CPPs in all four CPCS channels. The sharing consists of sharing the inputs of RSPT-1 to CPCS safety channels A and B, and sharing RSPT-2 inputs to CPCS safety channels C and D. Then, the CPPs of all channels, via inter-channel communication, will share (transmit) their respective channel's RSPT input signals with all other CPCS safety channels. This RSPT incoming CEA signals (i.e., 23 and 70) connection to the CPCS safety divisions is shown in DCD Tier 2, Figure 7.2-4, "CEA Position Signal Flow for CPCS." This design of sharing signals among all safety channels does not conform to the safety-related system independence requirements of Clause 5.6, "Independence," of IEEE Std 603-1991. The applicant has submitted a request for NRC approval of an alternative design proposal for the independence requirements of Clause 5.6 for the CPCS. The staff's evaluation of this CPCS alternative proposal is discussed in Section 7.1.4.1 of this SER.

The staff reviewed the results of the system-level FMEA as shown in DCD Tier 2 Table 7.2-7, "Failure Mode and Effects Analysis for the Plant Protection System." The FMEA was performed with one of the four safety channels in a bypassed status. Therefore, the FMEA was performed with only three operable and functional safety channels to actuate the reactor trip safety function and the resultant reactor scram trip logic for actuation is 2oo3, which retains the voting coincidence logic of two for reactor trip initiation. The causes of the postulated single failures for the shared RSPT instrumentation signals vary from shorted resistors to power supply failures. DCD Tier 2, FMEA Table 7.2-7, Item No. 2-4 and No. 2-5, provide the results of postulated RSPT single failures on the safety-related system. As stated in the "Safety I&C System," technical report, Section 4.3.1.1, "Trip Functions," and Section C.5.1.3.7, "DI&C-ISG-04 Staff Positions," the CPCS has "out of range" auxiliary trip functions such that if the input values or certain calculated variables exceed the pre-defined ranges, the range reactor trip signal is generated. The staff requested, in RAI 488-8617, Question 07.02-17, the applicant to provide design details, design descriptions, functional, and logic diagrams that explain and describe the actuation, execution, and operation of the CPCS auxiliary trips. On July 16, 2016, the applicant responded to the staff's request in RAI 488-8617, Question 07.02-17 (ML16198A008), by identifying the APR1400 application FSAR and technical report sections and figures that

addressed the staff request. In addition, the response provided FSAR markups adding an operational design description that stated that the CPC auxiliary trip sets both the DNBR and LPD trip contact outputs. The staff finds that the response resolved issues that were identified in RAI 488-8617, Question 07.02-17. The incorporation of the proposed markups into the next revision of the FSAR was a confirmatory item. The staff verified that the proposed markup has been incorporated into the Revision 1 of DCD Tier 2, Tables 7.2-4 and 7.2-7. As such, this confirmatory item has been satisfied.

[

].

[

].

- [ ].

- [ ].
- [ ].
- [ ].
- [ ].

In the September 22, 2015, response to RAI 50-7911, Question 07.02-8 (ML15265A591), the applicant submitted Figure 1, “Redundancy in CPCS,” which provided additional design details [ ]. This additional CPCS single failure FMEA design information provided in the response addresses the staff’s RAI 50-7911, Question 07.02-8, request. The incorporation of the proposed markups into the next revision of the FSAR was a confirmatory item. The staff verified the proposed markups have been incorporated into the FSAR. As such, this confirmatory item has been satisfied.

The staff’s review of the FMEA table CPP single failures found that transmission failures (i.e., erroneous CEA positions transmitted, failure to receive or transmit) were considered, as well as software and hardware malfunctions. For the postulated CPP single failures, the FMEA Table results demonstrate that the operation of the RTS with a postulated single failure of one CPP: (1) does not affect the ability of the CPCS system to monitor CEA positions in the core due to CEA RSPT measurement redundancy and CPCS safety division CPP redundancy; and (2) does not prevent the CPCS from initiating a DNBR or LPD reactor trip safety function. The FMEA results also show that CPCS self-diagnostics would detect failed CPP CEA position signal transmissions and provide alarms that would inform of the postulated CPP single failures. The staff finds that the CPCS design of utilizing redundant CPPs to transmit CEA signals to all CPCS safety channels address the guidance for interconnected redundant channels of IEEE Std 379-2000, Clause 6.2.1, in that with a single CPP failure, provisions have been made to ensure that the CPCS is capable of initiating a DNBR or LPD reactor trip safety function with a single failed CPP assumed during CPCS operation.

Another portion of the RTS that the staff evaluated to the interconnection guidance of IEEE Std 379-2000, Clause 6.2.1, are the redundant safety division connections to the coincidence voting logic of the LCL processors. DCD Tier 2, Figure 7.2-1, “PPS Basic Block Diagram,”

displays the interdivisional communications between redundant RTS interdivisional communications connected to the LCLs. These interdivisional communications connect the reactor trip output signal from each safety division's bistable processors to the LCL of all RTS safety divisions for reactor trip actuation voting purposes. IEEE Std 379-2000, Clause 6.2.1, guidance states that these interconnections shall be analyzed to assure that no single failure can cause the loss of a safety function. DCD Tier 2, FMEA Table 7.2-7, Item No. 10, Item No. 12, and Item No. 13, provide the postulated single failure results for the LCL operation. In addition, FMEA Table 7.2-7, Item No. 5, provides the results of postulated failures of the transmission of data from the bistable processor to the LCLs. As shown in DCD Tier 2, Figure 7.2-10, "PPS Channel A Trip Path Diagram," there are two sets of two redundant reactor trip LCL processors, per division, that receive all safety division's bistable processor outputs through interdivisional communications. Therefore, the 2oo4 coincidence voting of the four LCL processors per division, will produce four reactor trip output signals, per division. The LCL reactor trip information received from other division's bistable processors is validated through CRC checks. The trip signal information received from the bistable processors is used only for voting purposes in LCLs. A communications fault in which the bistable processor information is delayed, incorrect, or missing, will be input into the LCL, however, the LCL will not use the faulty information from the affected bistable processor and will perform coincidence logic using the signal from the redundant bistable processor. This is demonstrated in the FMEA table for postulated LCL single failures where the FMEA results show that there is no loss of the reactor trip safety function and that the coincidence logic to initiate a reactor trip remains the same. For postulated single LCL processor failures, the FMEA results demonstrate that the LCL WDT contacts will open and trip one-half of the safety division's reactor trip initiation circuit and will not affect the safety function or the minimum required reactor trip safety function redundancy. The reactor trip initiation circuit is identified in Note 2 on Tier 2, Figure 7.2-10, "PPS Channel A Trip Path Diagram." The FMEA results of a postulated single LCL processor failure is shown in DCD Tier 2, FMEA Table 7.2-7, Item 10a. Therefore, the staff has analyzed and verified, via the above listed FMEA results, that postulated single failures of the interconnected coincidence voting logic of the LCL reactor trip initiation logic will not cause the loss of the reactor trip safety function. Thus, staff's finds that the interconnected coincidence logic design and provisions addresses the guidance of IEEE Std 379-2000, Clause 6.2.1.

RTS Single Failure Evaluation for Non-detectable Failures and System Logic Failures

IEEE Std 379-2000, Clause 5.2, "Non-detectable Failure," states that a failure that cannot be detected through periodic testing, or revealed by alarm or anomalous indication, is non-detectable and that when non-detectable failures are identified, one of the following courses of action shall be taken:

- Preferred course: The system or the test scheme shall be redesigned to make the failure detectable.

- Alternative course: When analyzing the effect of each single failure, all identified non-detectable failures shall be assumed to have occurred.

Based on the staff's review of DCD Tier 2 Table 7.2-7, "Failure Mode and Effects Analysis for the Plant Protection System," the staff requested clarity on several terms used in the table to determine if these particular FMEA results were candidates for evaluation under the IEEE Std 379-2000, Clause 5.2, non-detectable failure guidance. The staff issued RAI 274-8277, Question 07.01-40 to request the applicant to clarify the terms used in DCD Tier 2 Table 7.2-7

of: (1) unrecognized software malfunctions; (2) erroneous CEA position transmission and indication; and (3) improper CEA positions. In the October 26, 2016, supplemental response to this RAI (ML15363A340), the applicant provided a proprietary response and proprietary markups to Figure 4-9a, "CEA Position and penalty factor movement." Upon review of proprietary Figure 4-9a provided in the response, the staff found several labeling errors within the proprietary figure and requested the applicant to provide a supplemental response to RAI 274-8277, Question 07.01-40 with the correct labeling on the figure. Therefore, RAI 274-8277, Question 07.01-40 was being tracked as an open item. The applicant provided a response on February 10, 2017 (ML17041A188), to RAI 274-8277, Question 07.01-40, and then a supplemental response (ML17214A240) on August 2, 2017. These revised responses include markups that provide corrections to the FSAR and the Safety I&C System TeR figures and corrected errors in the FMEA, Table 7.2-7. The staff finds that these corrections address the issues that staff raised in the request and finds them acceptable. Therefore, the verification that the proposed markups are incorporated into the next revision of the FSAR and the Safety I&C System TeR was a confirmatory item. The staff verified that the proposed markups have been incorporated into Revision 1 of the FSAR and Revision 1 of the Safety I&C System TeR. As such, this confirmatory item have been satisfied. Based on the clarifications provided in the proprietary response, the staff determined that for the "unrecognized software malfunctions" and "improper CEA positions" (as listed in FMEA Table 7.2-7) that cannot be detected by self-diagnostics, these failures are considered non-detectable failures. Therefore, the staff analyzed these failures utilizing the single failure guidance of IEEE Std 379-2000, Clause 5.2.

DCD Tier 2 Table 7.2-7, Items 2-10, 2-12, 2-13, 2-14, 2-14a, 2-14b (FMEA Table 7.2-7, Items 2-14a/b were provided as FSAR markups to the response to RAI 50-7911, Question 07.02-8), and 2-15, are considered single failure results for reactor trip safety functions that provide non-detectable failure results. All of these postulated single failures are postulated upon the CPCS operation. [

].

[

]

[

].

[

].

IEEE Std 379-2000, Clause 6.2.2, “System Logic,” states that the analysis shall verify that no single failure in the system logic will cause failure in the channels or actuation circuits, that would then cause loss of the safety function. The guidance of SRP Appendix 7.1-D, “Guidance for Evaluation of the Application of IEEE Std 7-4.3.2,” Section 5.7, “Capability for Test and Calibration,” states that Clause 5.5.3 of IEEE Std 7-4.3.2-2003, recommends that fault detection and self-diagnostics are one means that can be used to assist in detecting partial system failures that could degrade the capabilities of the computer system, but may not be immediately detectable by the system. This section also states the reviewer should carefully examine the capability of the software to test itself. SRP BTP 7-17 describes additional considerations in the evaluation of test provisions in digital computer-based systems. Section 3, “Acceptance Criteria,” of SRP BTP 7-17 states, in part, that digital computer based I&C system self-test features should accomplish the following.

- Include monitoring memory and memory reference integrity, using WDTs or processors, monitoring communication channels, monitoring central processing unit status, and checking data integrity.

- Checks for intermediate results, evaluation using different methods, ranges of variables, array bound checking, well-defined outputs for detected failures, reporting of errors for which error recovery techniques are used, use of counters and reasonableness traps, and correctness verification of transferred parameters.

The staff reviewed for adequate and appropriate RTS self-testing and self-diagnostic features that would address the above listed SRP BTP 7-17 guidance, and to address the guidance of IEEE Std 379-2000, Clause 6.2.2, “System Logic,” that the analysis shall verify that no single failure in the system logic will cause failure by utilizing automatic self-test and self-diagnostics as a means to assist in detecting partial system failures that could degrade the capabilities of the RTS. DCD Tier 2 Section 7.2.2.5, “System Testing and Inoperable Surveillance,” states that the RTS integrity is confirmed through self-diagnostics and surveillance testing and that testing features are provided for RPS testing during power operation. As stated by Safety I&C System TeR, Section 4.2.2.1, “General,” the PPS is designed to detect any error condition of the PPS through the self-diagnostic and supervisory functions such as input/output module diagnostics, processor module diagnostics, application program CRC, and communication error CRC. For the SDL communications, the SDL diagnostics are executed to detect physical layer failures and failures of the communication link to other processor modules (i.e., bistable processor to LCL SDL communication link to another redundant, independent safety division). Diagnostic functions monitor system operation and report any faults detected. The monitoring functions include an internal watchdog, bus supervision, and memory checking. The internal diagnostics check for process, system, and device errors. DCD Tier 2, FMEA Table 7.2-7, lists several types of safety-related system diagnostics: input/output diagnostics, on-line diagnostics, SDL diagnostics, receiving processor diagnostics, analog input diagnostics, live signal handshaking diagnostics, bistable processor diagnostics, LCL processor diagnostics, and ITP diagnostics. These diagnostics are defined in Common Q Topical Report, Revision 3:

- The self-contained diagnostics of the input/output modules and communication modules are executed by interrogating all modules for errors and reports the errors to the processor module.

- The SDL diagnostics are executed to detect physical layer failures and failures of the communication link to the recipient processor module (i.e., redundant division’s LCLs, CPPs, CEACs, CPCs).

- The physical layer of the data link control is secured through a CRC. If three bad CRCs occur consecutively, the SDL communication link will be marked as failed.

- A keep-alive (i.e., live signal) signal is transmitted over the SDL every 25 milliseconds if an application has requested no transmission. When a processor module has not received data for 250 milliseconds, the SDL is considered failed. All detected errors are reported.

- The SDN continuously monitors the status of the nodes on the bus. The SDN will monitors the validity of the data sets it is supposed to receive. If no data has been received for four cycles of the data set or when the communication interface has failed, the database element for the data set will be flagged as failed.

- The communications interface module provides on-line surveillance to ensure that it is in operational condition. The communications interface module contains self-diagnostics, and reports any errors to the application in the PM646A.

- Each CPC and CEAC processor module contains an external hardware WDT module. If the CPC or CEAC processor fails to refresh this module, the WDT module will open its respective trips and generate a reactor trip signal, and annunciation outputs.

- Each PPS LCL reactor trip processor is supervised by the built-in WDT. The contact outputs of the WDT are hardwired in series to the RPS initiation circuit to ensure appropriate trip signals are generated for the reactor trip function.

The RTS performs range checking on all sensor inputs such that a trouble alarm is generated upon detection of an input failure such as an out-of-range low or out-of-range high input condition. The staff finds that these RTS self-diagnostic and self-test features addresses the above listed SRP BTP 7-17 guidance for self-testing features, and finds that the RTS self-testing features are adequate, appropriate, and are used to assist in detecting partial system failures that could degrade the capabilities of the computer system.

NUREG/CR-6303 provides guidance for analyzing computer-based nuclear reactor protection systems for common mode failures where software design errors (i.e., logic errors) are a credible source of common mode failures. Several assumptions about postulating and analyzing these types of failures are stated in NUREG/CR-6303:

- In general, logical faults can propagate by the transmission of data for which the recipient is unprepared, or by failure to transmit data for which a recipient is waiting.

- In blocks containing software, it is credible that outputs shall assume values irrespective of inputs because the only logic connecting inputs to outputs is software, and the effects of software failures on outputs are unpredictable.

- …[S]ignals entering failed blocks (i.e., components, devices, systems) assume the most adverse credible values on output, essentially losing their protective function at that point.

- …[S]ignals from failed blocks (i.e., components, devices, systems) are propagated to downstream blocks (i.e., components, devices, systems), which react to the possibly erroneous signals.

The staff used the above listed logic failure assumptions to analyze the RTS FMEA to verify that no single failure in the system logic would cause failure in the channels or actuation circuits that would then cause loss of the safety function. The staff analyzed the possible logic failures utilizing the guidance described above. This guidance for postulating logic failures was applied to all CPCS processors. A detected logic failure would have a CPP, CEAC, CPC, or analog input module fail “in place” (i.e., no outputs transmitted, no processing of inputs) or transmit faulty, erroneous, improper, and/or intermittent output signals. The staff finds that these postulated logic errors would be detected by the system diagnostics described in the application. Therefore, the staff finds that the diagnostics provided in the design would address the single failure guidance of IEEE Std 379-2000, Clause 6.2.2, “System Logic.”

The staff finds that the RTS single failure design addresses the guidance of IEEE Std 379-2000, and thus, addresses the guidance in RG 1.53, Revision 2. Based on the conformance of the RTS single failure design to RG 1.53, Revision 2, the staff finds that the RTS single failure

design meets the listed single failure criterion requirements of GDC 21 and IEEE Std 603-1991, Clause 5.1.

7.2.5 Combined License Information Items

No applicable items were identified in the FSAR. No additional COL information items need to be included in DCD Tier 2 Table 1.8-2, "Combined License Information Items," for RTS consideration.

7.2.6 Findings and Conclusions

The staff reviewed the RTS to verify their compliance to applicable regulations. The staff concludes that the design of the RTS meets the listed requirements of 10 CFR 50.55a(h)(3), and 10 CFR Part 50, Appendix A, GDC 10, 13, 15, 20, 21, 23, 24, and 25. This does not include the alternative request associated with independence for the sharing of RSPT signals among CPCS channels. The staff, as documented in the above SER sections, has reviewed the applicant's responses to RAI 274-8277, Question 07.01-40 and found the response acceptable, and has verified that the response's proposed markups have been incorporated into Revision 1 of the FSAR and Revision 1 of the Safety I&C System TeR. As such, RAI 274-8277, Question 07.01-40 has been satisfied. Thus, based on the safety findings listed above, the staff concludes that the alternative request design to share RSPT analog sensor signals among all CPCS safety channels provides an acceptable level of quality and safety, and thus, the staff finds that the alternative request conforms to the criterion of 10 CFR 50.55a(z)(1), "Alternatives to codes and standards requirements." Therefore, the staff approves the applicant's request to use the alternative design as an alternative to the independence requirements of IEEE Std 603-1991, Clause 5.6.1. GDC 2 and 4 are evaluated in Section 7.1.4.8 of this SER. GDC 19 is evaluated in Sections 7.1.4.12, 7.5, 7.9 of this SER.

The staff conducted a review of the RTS for conformance to the guidelines in the RGs and industry codes and standards applicable to the RTS. The staff concluded that the applicant identified the guidelines applicable to the RTS adequately. Based upon the review of the system design for conformance to the guidelines, the staff finds that there is reasonable assurance that the systems fully conform to the guidelines applicable to these systems. Therefore the staff finds that the requirements GDC 1 have been met.

Based upon this review and coordination with those having primary review responsibility for the accident analysis, the staff concludes that the RTS includes the provision to sense accident conditions and AOOs in order to initiate reactor shutdown in conformance with the accident analysis presented in DCD Tier 2 Chapter 15, and evaluated by the staff in Chapter 15 of this SER. Therefore, the staff finds that the RTS satisfies the requirements of GDC 10, 15, 20 and 29.

Based on the review of the RTS, the staff concludes that the system satisfies the protection system requirements for malfunctions of the reactivity control system such as accidental withdrawal of control rods. Chapter 15 of this SER address the capability of the system to ensure that fuel design limits are not exceeded for such events. Therefore, the staff finds that the RTS satisfies the requirements of GDC 25.

The staff's review for compliance with 10 CFR 50.34(f)(2)(v) and 10 CFR 50.34(f)(2)(xxiii) are in Section 7.5 of this SER.

The staff reviewed the ITAAC in regards to compliance to 10 CFR 52.47(b)(1). Additional discussion on the staff's review of compliance to 10 CFR 52.47(b)(1) is found in Section 14.3.5 of this SER. Therefore, the staff concludes that the RTS design meets the ITAAC requirements of 10 CFR 52.47(b)(1).

7.3 Engineered Safety Features Systems

7.3.1 Introduction

The APR1400 design provides safety-related I&C to sense accident conditions and automatically actuate the ESF systems when selected variables exceed associated setpoints. The setpoints are established for indication of conditions that require protective and mitigating action. The I&C of the ESF systems includes components from sensors to actuation device input terminals that are involved in generating signals to actuate the required ESF systems. Additionally, the ability to manually initiate ESF systems is provided in the MCR. System-level manual actuation of ESF systems initiates all actions performed by the corresponding automatic actuation, including starting auxiliary or supporting systems and performing required sequencing functions. Component-level manual control of ESF system actuators is also provided in the MCR. The manual control for the main steam isolation system is provided as well in the RSR to assist in achieving cool-down when the condenser is not available. Minimum inventory switches at both system-level and component-level, and ESCM on the safety console provide manual control means to maintain plan safe shutdown under transient and accident conditions. The minimum inventory indications and alarms are used to support the required actions by operators under the accident conditions.

7.3.2 Summary of Application

DCD Tier 1: The Tier 1 information associated with this section is found in DCD Tier 1, Section 2.5.1 for RTS and ESF Initiation and Section 2.5.4 for ESF-CCS. DCD Tier 1, Section 2.5.1 includes essential design information on the bistable trip logic, LCL, ESF system initiation, and testing function for the ESFAS portion of the PPS. DCD Tier 1, Section 2.5.4 includes similar information for the ESF-CCS, which provides automatic actuation of ESF systems.

DCD Tier 2: The applicant provided a description for the design of the ESF systems in DCD Tier 2 Section 7.3, "Engineered Safety Features Systems," which is summarized, in part, as follows:

Automatic actuation of ESF systems and auxiliary supporting systems is performed by the sensors, APC-S, ESFAS portion of the PPS, the safety portion of RMS, and the ESF-CCS combined when selected plant parameters reach their corresponding trip setpoints.

The safety ESF I&C system consists of four channels of sensors, APC-S, and four divisions of the ESFAS portion of the PPS, the ESF-CCS, and CIM. The ESF I&C system also includes the safety portion of RMS. APC-S functions include signal conditioning/splitting for the safety field sensor signals shared by the PPS, CPCS, ESF-CCS, and other safety-related systems or non-safety systems. Isolation is provided when signals are split in the APC-S to a non-safety system.

The ESF initiation is performed in the combined sensors, APC-S cabinets, and ESFAS portion of the PPS cabinets. ESF initiation equipment is located in the auxiliary building and reactor

containment building. The ESF-CCS provides automatic actuation of ESF systems through the CIM for each ESF component. The ESF-CCS performs the NSSS ESFAS function, BOP ESFAS function, and EDG loading sequencer function. The ESF-CCS generates the NSSS ESF actuation signals upon receipt of ESFAS initiation signals from the PPS. The ESF-CCS generates the BOP ESF actuation signals upon receipt of initiation signals from the process and effluent RMS. The ESF-CCS also generates the EDG loading sequencer signals upon receipt of loss of power to Class 1E train buses, SIAS, CSAS, and AFAS. The ESF-CCS provides the capability for manual actuation of ESF systems and manual control of ESF components.

ITAAC: The ITAAC items associated with DCD Tier 2 Section 7.3 are given in Tier 1, Table 2.5.1-5 for ESF initiation and Table 2.5.4-4 for ESF-CCS. The evaluation of ITAAC items for the ESF systems focuses on the design basis requirements only, and is addressed in Section 14.3.5 of this SER.

Technical Specifications: The Technical Specifications associated with DCD Tier 2 Section 7.3 is given in DCD Tier 2 Chapter 16, Sections 3.3 and B 3.3, and its evaluation is addressed in Chapter 16 of this SER.

Technical Reports: More detailed information associated with DCD Tier 2 Section 7.3 is provided in the following technical reports:

- Safety I&C System TeR
- CIM TeR
- D3 TeR
- SPM TeR
- Uncertainty Methodology TeR
- Setpoint Methodology TeR
- Response Time Analysis TeR

7.3.3 Regulatory Basis

The relevant NRC regulations for review of ESF systems and associated acceptance criteria are given in SRP Section 7.3, “Engineered Safety Features Systems,” and are summarized below. Review interfaces with other SRP sections can also be found in SRP Section 7.3.

1. 10 CFR 50.55a(h)(3), “Safety Systems,” requires compliance with IEEE Std 603-1991, “IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations,” and the correction sheet dated January 30, 1995.

2. 10 CFR 50.34(f), “Additional TMI-related Requirements,” or equivalent TMI action requirements imposed by Generic Letters:

    a. (2)(v), “Bypass and Inoperable Status Indication.”

    b. (2)(xii), “Auxiliary Feedwater System Automatic Initiation and Flow Indication.”

c. (2)(xiv), “Containment Isolation Systems.”

3. GDC 1, 2, 4, 10, 13, 15, 16, 19, 20, 21, 22, 23, 24, and 29.

Additional requirements which are applicable to ESF systems include:

1. GDC 33, 34, 35, 38, 41, and 44.

2. 10 CFR 52.47(b)(1), “Contents of Applications; Technical Information.”

Additional acceptance criteria adequate to meet the above requirements also include SRP Table 7-1, Section 3 (SRMs), Section 4 (RGs), and Section 5 (RGs), which list specific SRP acceptance criteria applicable to ESF systems.

7.3.4 Technical Evaluation

7.3.4.1 Introduction

The objective of the staff’s technical evaluation is to confirm that the control system of the ESFAS design satisfies NRC regulations through a set of acceptance criteria and that it can perform its safety functions for all plant conditions. SRP Section 7.3 lists regulatory acceptance criteria for design considerations that should be emphasized for the review of ESFAS. The RTS portion of the PPS and HSI system, which are mentioned in DCD Tier 2 Section 7.3 as well, are evaluated in detail in Sections 7.1, 7.2, 7.5, and Chapter 18 of this SER. The DAS and data communications for the APR1400 design are also mentioned in DCD Tier 2 Section 7.3, but are evaluated in Sections 7.8 and 7.9, respectively, of this SER.

7.3.4.2 System Description

An ESF system is safety-related system that includes the actuation functions of ESF and its components that perform protective and mitigating actions after receiving a signal from the ESFAS or the operator. The ESFAS consists of the sensors, APC-S cabinets, ESFAS initiation portion of the PPS, safety portion of RMS, the ESF-CCS, and CIM. The description for each subsystem of the ESFAS is summarized below. The detailed design features of the APC-S, ESFAS initiation portion of the PPS, and ESF-CCS are described in the Safety I&C System TeR.

7.3.4.2.1 Auxiliary Process Cabinets - Safety

The APC-S consists of four Class 1E, redundant channels. It receives safety sensor signals and distributes them to the PPS, CPCS, ESF-CCS group controller and loop controller, QIAS-P, DIS via hardwired interfaces or other safety-related systems and non-safety systems. The APC-S includes signal conditioning and splitting equipment and associated power supplies for sensor inputs. Qualified isolation devices are provided within the APC-S to interface safety signals to the non-safety systems.

7.3.4.2.2 Engineered Safety Features Actuation System Portion of the Plant Protection System

The PPS consists of four redundant divisions that perform the necessary bistable, coincidence, initiation logic, maintenance, and test functions. The PPS comprises two portions: the RPS and ESFAS. The ESFAS portion of the PPS initiates system-level ESF actuation functions

automatically whenever a safety setpoint of variables for the ESF systems is exceeded by the plant conditions.

The ESFAS portion consists of NSSS ESFAS and BOP ESFAS. NSSS ESFAS signals include:

- SIAS;
- CSAS;
- CIAS;
- MSIS; and
- AFAS-1 and AFAS-2.

BOP ESFAS signals are as follows:

- FHEVAS;
- Containment purge isolation actuation signal; and
- Control room emergency ventilation actuation signal (CREVAS).

The ESFAS portion of the PPS is also equipped with means for manual initiation of each protective action. The ESFAS portion of the PPS provides outputs for operator monitoring of the status of the PPS and receives manually entered inputs for limited operator intervention in the automatic ESF actuation such as an operating bypass and setpoint reset. It also provides alarms and, in some cases, limiting signals to control systems, whenever the selected plant process parameters approach the predetermined levels where plant protection would be required. The ESFAS portion of the PPS has test capability for determining system operability and hardware diagnostic testing, and actuates system-level ESF functions that transmit signals to ESF components necessary to mitigate the consequences of the design basis accidents. This includes minimizing fuel damage and subsequent release of fission products to the environment. There is an actuation signal for each ESFAS function. Each actuation function is similar except that specific inputs (and bypasses where provided) and the actuated devices are different.

The ESFAS portion of the PPS includes its bistable trip logic and LCL processing sections. Each bistable trip logic processing station includes a single bistable processor which receives input signals from process instrumentation sensors, ENFMS, and CPC. Each bistable processor station transmits bistable data to the LCL processors via the SDL. The bistable processor software determines the partial trip state by comparing the process variable measurement with the setpoints. The LCL processors perform 2oo4 coincidence voting logic which generates the RPS and ESFAS initiation signals.

7.3.4.2.3 Safety Portion of RMS

The RMS monitors normal and potential paths for release of radioactive materials to provide continuous indication and recording of radioactivity levels of the gaseous and liquid waste leaving the plant. The safety portion of the RMS is implemented on a separate platform and

provides ESFAS initiation signals to the ESF-CCS. Detailed design features of the RMS are described in DCD Tier 2, Sections 11.5 and 12.3.4.

7.3.4.2.4 ESF-CCS

The ESF-CCS consists of four divisions that perform additional 2oo4 voting logic, component control logic, and priority logic function. The ESF-CCS design consists of processors arranged in primary and standby processor configurations within each ESF-CCS division. ESFAS functions are divided into the ESF-CCS distributed segments which receive the ESF initiation signals from the PPS through the fiber optic cable. Separation is provided between protective ESFAS processing function and auxiliary functions of human-system interfaces, data communication, and automatic testing. The SDL supports the transmission of protection data on a continuous cyclical basis independent of plant transients.
The ESF-CCS consists of two subsystems: the ESF-CCS group controller and ESF-CCS loop controller. The group controller of each ESF-CCS division receives four division ESFAS initiation signals derived from the ESFAS portion of the PPS and performs additional selective 2oo4 coincidence voting logic to generate the ESF actuation signal. The group controller also receives two division ESFAS initiation signals derived from the SRDC in the RMS and performs 1oo2 voting logic to generate the ESF actuation signal. The ESF actuation signals are transmitted to the loop controller of the ESF-CCS. The loop controller executes the component control logic and outputs the component control signal to its associated CIM. The component control logic includes the priority logic for the operator's manual control signal and ESF actuation signal. The ESCM on the operator console generates a component control signal of safety components by manual operator actions.

The ESF-CCS loop controller receives ESF actuation signals from the group controller and the component-level minimum inventory switches to control safety components. The ESF-CCS loop controller performs the prioritization logic between group controller outputs (ESF actuation signals and minimum inventory switches) and manual ESF component-level control signals (from the ESCM). The ESF actuation signal from group controllers has priority over ESF component-level control signals from the ESCM. The ESF actuation signals from the ESF-CCS group controller can override the control signals from the ESCM at any time.

The output of the ESF-CCS is hardwired to the CIM which performs prioritization of system signals associated with a particular ESF component. The ESF-CCS also receives an initiation signal for the EDG load sequencer from the electrical panel. The signal is generated by under-voltage relays (one division per 4.16 kilovolt (kV) power bus) consisting of 2oo4 voting logic under loss of offsite power (LOOP) event.

The ESF-CCS provides the control of other safety components as well as the actuation of ESF components. Such components include breaker and relay operated components (e.g., pumps, fans, heaters, and motor operated valves), and solenoid operated components (e.g., pneumatic, electro-pneumatic, and direct operated valves). The output of the CIM is hardwired to the electrical equipment that supplies electrical power to the ESF components. The electrical equipment interfaces directly with the ESF components.

7.3.4.2.5 Component Interface Modules

The CIM is a safety module that is used to send the actuation command to each field ESF component. The CIM receives component actuation signals from the ESF-CCS, DPS, DMA

switches, and its front panel control (FPC) switch and then prioritize them according to pre-established priority logic configuration.

The CIM combines the control signals received through conventional hardware priority logic and then sends the resulting commanding signal to the ESF component to be controlled, such as a motor-operated valve (MOV), pump motor, or solenoid-operated valve. The priority logic function in the CIM is implemented by the hardware device such as transistor-transistor logic (TTL) or complementary metal-oxide semiconductor (CMOS). The CIM receives control signals (as discrete contact outputs) from the ESF-CCS as well as DPS. The control signals from DMA switches are also hardwired to the CIM directly to cope with a postulated software CCF of the digital safety-related I&C system. The FPC switch is provided on the CIM front panel.

The four control sources for the CIM are designated as Input A, B, and C and the FPC switch. The component control signal from the ESF-CCS is assigned to Input A. Input B is used for the DPS, and Input C is configured to receive the hardware control inputs from the DMA switches. In addition, the FPC switch is also connected to the priority logic section of the CIM.

The CIM provides two kinds of priority: state-based priority and system-based priority. If the CIM receives component control signals from multiple systems concurrently, the CIM prioritizes control signals to generate an output signal to the designated plant component.

The state-based priority is applicable to Input A for the ESF-CCS output signal and Input B for the DPS output signal. When the CIM receives input signals from the ESF-CCS and DPS concurrently, the CIM prioritizes control signals so that the pre-designated signal state (e.g., energize/de-energize, open/closed) has always higher priority than non-designated signal state regardless of the system generating the signal.

The system-based priority is applicable to Input C from the DMA switches and FPC switch, which both have priority over signals from the ESF-CCS and DPS. In addition, the FPC switch has priority over the DMA switches. The DMA switches, which have higher priority than initiation signals from the ESF-CCS and DPS, provide operator's actions that are required for coping with AOO or PA with a concurrent CCF in the PPS and ESF-CCS.

The detailed design features of the CIM are described in the CIM TeR.

7.3.4.3 Evaluation of Engineered Safety Feature Systems Conformance with Acceptance Criteria - Major Design Considerations

The SRP Section 7.3 lists the following major design considerations that should be emphasized in the review of the ESFAS and ESF in accordance with the SRP.

- Design basis;
- Single failure criterion;
- Quality of components and modules;
- Independence;
- Completion of protective action;

- D3;
- System testing and inoperable surveillance;
- Use of digital systems;
- Setpoint determination; and
- ESFAS and its control systems as required by GDC 34, 35, 38, and 41.

Some of design acceptance criteria and considerations are addressed in other sections of this SER, and where appropriate, the technical evaluation for SRP Section 7.3 refers to other SRP sections for additional details. Table 7.3-1 below lists the sections in this SER where each specific design acceptance criteria and consideration applicable to the review of the ESAFAS and its control systems are addressed.

Table 7.3-1. SER Section References

Design Considerations	SER Section(s)
Quality Standard, GDC 1	7.1.4.3, 7.1.4.7
Design Bases, 10 CFR 50.55a(h)(3), GDC 2	7.1.4.4, 7.3.4.3.1
Single Failure Criterion, 10 CFR 50.55a(h)(3), GDC 21	7.1.4.5, 7.3.4.3.2
Independence, 10 CFR 50.55a(h)(3), GDC 22	7.1.4.10, 7.9
Equipment Qualification, 10 CFR 50.55a(h)(3), GDC 4	7.1.4.8
System Integrity, 10 CFR 50.55a(h)(3)	7.1.4.9
Capability for Test and Calibration, 10 CFR 50.55a(h)(3), GDC 21	7.1.4.11
Information Display, 10 CFR 50.55a(h)(3), GDC 13, GDC 19	7.1.4.12, 7.5, 7.9
Control of Access, 10 CFR 50.55a(h)(3)	7.1.4.13
Repair, 10 CFR 50.55a(h)(3)	7.1.4.14
Identification, 10 CFR 50.55a(h)(3)	7.1.4.15
Auxiliary Features, 10 CFR 50.55a(h)(3)	7.1.4.16
Multi-unit Stations, 10 CFR 50.55a(h)(3)	7.1.4.18
Human Factors, 10 CFR 50.55a(h)(3), GDC 19	7.1.4.19, Chapter 18
Reliability, 10 CFR 50.55a(h)(3), GDC 21	7.1.4.20
Automatic and Manual Control, 10 CFR 50.55a(h)(3)	7.1.4.22
Derivation of System Inputs, 10 CFR 50.55a(h)(3)	7.1.4.17
Completion of Protective Action, 10 CFR 50.55a(h)(3)	7.1.4.6, 7.3.4.3.5
Bypasses (Operating and Maintenance), 10 CFR 50.55a(h)(3)	7.1.4.23, 7.1.4.24
Setpoints, 10 CFR 50.55a(h)(3)	7.1.4.25

Design Considerations	SER Section(s)
Power Sources, 10 CFR 50.55a(h)(3)	7.1.4.4
Bypass and Inoperable Status Indication, 10 CFR 50.55a(h)(3), GDC 13, GDC 19	7.1.4.12, 7.5
Power and Environmental Condition Ranges, 10 CFR 50.55a(h)(3), GDC 4	7.1.4.4, Chapter 3
Protection System Functional Degradation, 10 CFR 50.55a(h)(3), GDC 4, GDC 20	7.1.4.4, Chapter 3
TMI-Related Requirements, 10 CFR 50.34(f)	7.1.4.26, 7.5
D3, GDC 24	7.1.4.21, 7.3.4.3.6, 7.8, 7.9
GDC 33, 34, 35, 38, 41, 44	Chapter 15, Section 8.3.1
ITAAC, 10 CFR 52.47(b)(1)	14.3.5

The requirements of 10 CFR 50.55a(h)(3) specify that safety-related systems must meet the requirements of IEEE Std 603-1991 and the correction sheet dated January 30, 1995. Appendix A in the Safety I&C System TeR documents the analysis and evaluates compliance with IEEE Std 603-1991, which is noted in DCD Tier 2 Section 7.3 as well. The compliance with the GDC in 10 CFR Part 50, Appendix A is also described in the above technical report and DCD Tier 2 Section 7.1.

This section evaluates compliance with IEEE Std 603-1991 for portions of the ESF safety control systems which are not evaluated elsewhere. The staff's technical evaluation on the ESF safety control systems presented in this section is based on IEEE Std 603-1991, and the scope of the evaluation is limited to Clause 4, "Design Bases," in IEEE Std 603-1991, other applicable regulatory criteria and design considerations mentioned at the beginning of this section.

The staff's technical evaluation of the ESFAS is conducted in this section is based on the FSAR, Revision 1 and its associated technical reports.

7.3.4.3.1 Design Basis (IEEE Std 603-1991, Clause 4)

There are 12 design bases or clauses in Clause 4 of IEEE Std 603-1991. SRP Appendix 7.1-C for IEEE Std 603-1991, Clause 4, states, in part, that the design basis should be reviewed to confirm that it has the characteristics of completeness, consistency, correctness, traceability, unambiguity, and verifiability. Also, the application information provided for the design basis should address all system functions necessary to fulfill the system's safety intent. Information provided in the application for each design basis item should be sufficient to enable the detailed design of the I&C system to be carried out. In addition, all functional requirements for the I&C system and the operational environment for the I&C system should be described in the application. The application information provided to address each of the 12 design bases is evaluated below.

Clause 4.1, in IEEE Std 603-1991, requires the identification of the DBE applicable to each mode of operation along with the initial conditions and allowable limits of plant conditions for

each such event. Clause 4.2 in IEEE Std 603-1991 requires the applicant to design the safety functions and corresponding protective actions of the execute features for each DBE.

Each DBE and the allowable limit for each DBE and accident are described in DCD Tier 2 Chapter 15. DCD Tier 2 Table 7.3-3 describes the ESFAS initiating signals and Table 7.3-5 provides actuation setpoints and margins for each ESFAS initiating signal. The ESFAS mitigates the consequence of an event to within the allowable limit during a DBE. The ESFAS utilizes bistable logic and coincidence voting logic in the PPS and coincidence voting logic and component control logic in the ESF-CCS to generate actuation signals. Actuation signals are provided as input signals to the ESF systems. Upon receipt of ESFAS initiation signal from the PPS, the ESF-CCS generates the following actuation signals:

- CIAS initiated by high containment pressure trip and low pressurizer pressure trip;
- CSAS initiated by high-high containment pressure trip;
- MSIS initiated by high containment pressure trip, low SG 1 and 2 pressure trips, and high SG 1 and 2 water level trips;
- SIAS initiated by high containment pressure trip and low pressurizer pressure trip;
- AFAS-1 initiated by low SG 1 water level trip; and
- AFAS-2 initiated by low SG 2 water level trip.

Information provided in DCD Tier 2 Section 7.3 is consistent with the assumptions for the safety analysis in DCD Tier 2 Chapter 15, which the staff found acceptable to meet the requirements in Clause 4.1 of IEEE Std 603-1991.

DCD Tier 2 Table 7.3-2 shows the protective ESFAS actions for each DBE in accordance with Clause 4.2 of IEEE Std 603-1991, which the staff also found acceptable. However, the staff found that the logic diagram in Figure 7.3-5 of DCD Tier 2 shows four divisions for the CSAS safety function. There are only two containment spray pumps used for the two containment spray trains, respectively. It was not clear in DCD Tier 2 Section 7.3 how the two containment spray pumps are controlled. In addition, there is no design information in DCD Tier 2 Section 7.3 on how the two shutdown cooling pumps will be controlled. As such, the staff requested in RAI 323-8281, Question 07.03-11, that the applicant describe the control and interface of the containment spray and shutdown cooling pumps in relation to the ESFAS.

In the March 4, 2016, response to RAI 323-8281, Question 07.03-11 (ML16064A060), the applicant stated, in relevant part, that the CSAS initiation signal is generated from all four PPS divisions A, B, C, and D. The CSAS initiation signal is transmitted to the group controllers in all four ESF-CCS divisions. The group controllers in each ESF-CCS division perform a 2oo4 coincidence voting logic based on the CSAS initiation signal received from the PPS and transmit the CSAS actuation signal to the LCs. The outputs of the loop controller in ESF-CCS divisions A, B, C, and D are then transmitted via the CIM to the division A, B, C, and D components, respectively. The CSS is designed to have two independent divisions: Divisions C and D, each containing one containment spray pump. The containment spray pumps are actuated by a CSAS or an SIAS from the ESF-CCS loop controller via a dedicated CIM. Two shutdown cooling pumps which are assigned to independent divisions A and B are aligned to perform the containment spray function if the following three conditions are met simultaneously: (1) CSAS actuation or SIAS actuation; (2) the containment spray pump is in trouble or disabled; and (3)

the cross-connection valves of the containment spray/shutdown cooling pumps are not fully closed. The staff finds that the above additional design information needs to be incorporated in the DC application. In addition, in the initial RAI response above, it is unclear to the staff how interdivisional communication to support these functions is implemented. As such, the staff requested the applicant to supplement the response to address this issue. In the revised response to RAI 348-8279, Question 07.09-9, the applicant states, in relevant part, that the interdivisional communication is hardwired to support the logic functions. The cross-connected signals between electrical divisions use Class 1E qualified electrical isolation devices to achieve the required electrical isolation and physical separation. The staff found that the initial response to RAI 323-8281, Question 07.03-11, and supplemental information provided in the revised response to RAI 348-8279, Question 07.09-9, demonstrate compliance with the regulatory requirements in IEEE Std 603-1991, Clauses 4.1 and 4.2. The staff verified that all proposed changes have been incorporated into Revision 1 of DCD Tier 2, Sections 7.3.1.9, 7.6.1.6, and Section 4.4.4.13 of the Safety I&C System TeR.

Clause 4.3 in IEEE Std 603-1991, requires documentation of the permissive conditions for each operating bypass capability that is to be provided. The PPS and ESF-CCS are designed such that protective functions are initiated and accomplished during various reactor operating modes. Where operating requirements necessitate automatic or manual block of a protective function, the block is automatically removed whenever the appropriate permissive conditions are not met. Hardware and software used to achieve automatic removal of the block of a protective function are part of the PPS and ESF-CCS and are designed in accordance with the same criteria as the protective function. Block of a protective function is automatically cleared when the protective function is required to function. The ESFAS operating bypass types, permissive, and removal condition are described in Table 7.3-1 of DCD Tier 2. Based on the above discussion, the staff found that the ESFAS design satisfies requirements in Clause 4.3 of IEEE Std 603-1991 to document the permissive conditions for each operating bypass capability.

Clause 4.4, in IEEE Std 603-1991, requires the definition of protective system variables and their range and rate of changes. DCD Tier 2 Table 7.3.7 lists the variables required to be monitored for protective action and their ranges and rates of change for the ESF systems. The initiation of automatic ESF actuation and where the protection signals are derived will be verified during the implementation of the ITAAC items, as defined in DCD Tier 1 Table 2.5.1-5 for ESF initiation and Table 2.5.4-4 for ESF-CCS. The evaluation of ITAAC items for the ESF systems is addressed in Section 14.3.5 of this SER. Based on the discussion above, the evaluation in Section 14.3.5 of this SER, and the verification in the DCD Tier 1, ITAAC Table 2.5.1-5 for ESF initiation and Tier 1 ITAAC Table 2.5.4-4 for ESF-CCS, the staff found that the APR1400 design meets the requirement in Clause 4.4 of IEEE Std 603-1991 for the ESF systems.

Clause 4.5, in IEEE Std 603-1991, requires a means of initiating manual actions. The MCR provides the means for manual initiation of safety functions for ESF systems. The manual actuation of the main steam isolation system is provided as well in the RSR to help achieve cool-down when the condenser becomes unavailable. The manual controls are a backup to the automatic protection provided by the PPS and ESF-CCS. Manual control is not credited within the first 30 minutes of occurrence of an accident. The assumption, initial condition, event details, and plant state for each accident and event are described in DCD Tier 2 Chapter 15. Manual actuation relies on minimum equipment and, once initiated, proceeds to completion unless the operator deliberately intervenes. Failure in the automatic initiation portion of a system-level function does not prevent the manual initiation of the function. The HSI design includes a minimum inventory of dedicated or fixed-position displays and controls. The manual initiation is not allowed in principle prior to the actuation of ESFAS when the setpoint is

exceeded after event onset. The manual control for the ESF systems, which is conducted after ESFAS initiation, is performed in accordance with the EOP. The ESFAS is not designed to permit initiation only by manual means. MCR environmental conditions during manual operation are provided in DCD Tier 2 Section 6.4. The variable list required by Clause 4.4 of IEEE Std 603-1991 that is displayed for the operator for taking manual action is provided in DCD Tier 2 Table 7.5-1. The PPS manual actuation for the ESF will be verified during the implementation of the ITAAC items, as defined in DCD Tier 1, ITAAC Table 2.5.1-5 for ESF initiation and Table 2.5.4-4 for ESF-CCS. Based on the discussion above, evaluation in Section 14.3.5 of this SER, and the verification in the DCD Tier 1 ITAAC items, the staff found that the safety-related I&C design meets the requirement in Clause 4.5 of IEEE Std 603-1991 for the ESF systems.

Clause 4.6, in IEEE Std 603-1991, requires the identification of the minimum number and location for the spatially dependent variables required in Clause 4.4 of IEEE Std 603-1991. There are no spatially dependent variables for the ESF systems. But, the spatially dependent variables used in the PPS for the RTS are evaluated in Sections 7.1.4.4 and 7.2 of this SER. Based on this discussion, the staff found that Clause 4.6 in IEEE Std 603-1991 is not applicable for the ESF systems.

Clause 4.7, in IEEE Std 603-1991, requires, in part, that the range of transient and steady-state conditions be identified for the energy supply and the environment during normal, abnormal, and accident conditions under which the system must perform. The safety-related I&C system is qualified to meet environmental conditions as described in DCD Tier 2 Section 3.11 in accordance with IEEE Std 323-2003. In addition, the safety-related I&C system is capable of performing its intended function under the most degraded conditions of the energy supply. The ESFAS is designed and tested in accordance with the requirements of IEEE Std 323-2003 for environmental qualification and IEEE Std 344-2004 for seismic qualification. The ESFAS system is designed and tested to minimize both the emission and susceptibility of EMI and RFI in compliance with the guidance in RG 1.180, Revision 1. The safety control system is powered by Class 1E direct current and an uninterruptible power supply system.
As evaluated in Section 7.1.4.8 of this SER above, the staff found that the supplemental response to RAI 323-8281, Question 07.03-9 is acceptable. Hence, the applicant provided sufficient information in the APR1400 design certification application combined with initial and supplemental RAI responses that demonstrate compliance with regulatory requirements for environmental seismic, and EMC qualification for the safety-related I&C systems. Therefore, the issue associated with the above RAI 323-8281, Question 07.03-9, has been closed and resolved. The proposed changes in the supplemental RAI responses have not been incorporated in Revision 1 of the Safety I&C System TeR, and hence, RAI 323-8281, Question 07.03-9, was being tracked as a confirmatory item. The staff verified the proposed markups have been incorporated into Revision 2 of the Safety I&C System TeR. As such, this confirmatory item has been satisfied.

Clause 4.8, in IEEE Std 603-1991, requires, in part, the identification of conditions which have the potential to cause functional degradation of safety-related system performance and the proposed protective action. The PPS and ESF-CCS are located in plant areas that provide protection from accident related hazards such as missiles, pipe breaks, and flooding. The redundant divisions of the PPS and ESF-CCS are isolated from each other and isolated from non-safety systems. Isolation should ensure functional independence and communication independence. The redundant division arrangement should provide independent operations in case of fires or electrical faults. The ESFAS logic design takes account of functional degradation that could occur in some conditions. The ESFAS design is verified according to

IEEE Std 344-2004 to demonstrate that the ESFAS can perform the intended function for seismic conditions. The ESFAS is qualified according to an established plan for EMC that requires the equipment to function properly when subjected to electrical surges, EMI, RFI, and electrostatic discharge. Qualification is applied in equipment based on operating environment and/or inherent design characteristics. Radiated and conducted electromagnetic interference envelopes are established for qualification.
Based on the review of DCD Tier 2, Sections 3.11, 7.1, and 7.3 that describe the locations, environment, and hazards in installed locations of the PPS and ESF-CCS components, the staff issued RAI 43-7887, Questions 07.01-23, 07.01-24, and RAI 323-8281, Question 07.03-9, and evaluated the responses to those questions in Section 7.1.4.8 of this SER. Based on the evaluation in Section 7.1.4.8 of this SER regarding the resolution of issues identified in RAI 43-7887, Questions 07.01-23, 07.01-24, and RAI 323-8281, Question 07.03-9, the staff finds that the applicant provided sufficient information in the APR1400 design certification application to demonstrate the requirements in IEEE Std 603-1991, Clause 4.8, are met.

Clause 4.9, in IEEE Std 603-1991, requires the applicant to identify the methods used to determine that the reliability of the safety-related system design is appropriate. In addition, it requires that the applicant identify the qualitative or quantitative goals used to verify the reliability imposed on the system design. The equipment reliability for the safety-related I&C system is described in Section 7 of the Safety I&C System TeR. Section 7.1.4.20 of this SER provides the evaluation of the reliability for the safety-related I&C system.

Clause 4.10, in IEEE Std 603-1991, requires identification of the critical points in time or plant conditions, for which the protective actions shall be initiated. The PPS automatically initiates appropriate protective actions when a condition monitored by the PPS reaches a preset level. The critical points in time are determined by the PPS and ESF-CCS response time modeled in the accident analyses provided in DCD Tier 2 Chapter 15.

The staff found that ITAAC Item 16 in Table 2.5.1-5 of DCD Tier 1 includes one design commitment and associated inspection, tests, and analyses which ensure that the PPS provides reactor trip and ESF initiation signals to meet the required response time for reactor trip and ESF initiation conditions. The staff also found that ITAAC Item 20 in Table 2.5.4-4 of DCD Tier 1 includes one design commitment and associated inspection, tests, and analyses which ensure the ESF-CCS to provide ESF actuation within required response time for ESF functions. The Response Time Analysis TeR includes estimated response times for an integrated safety-related I&C system, which include sensors, APC-S, PPS, ESF-CCS, and field actuated components for the ESF systems. However, there is lack of design commitment and associated inspection, tests, and analyses in the design certification application to ensure that the integrated safety-related I&C system can meet the response times required in the safety analyses and proposed in the Response Time Analysis TeR. As such, the staff asked the applicant in RAI 300-8297, Question 07.03-3, to provide design commitment or clarification on how the response time for an integrated safety-related I&C system is ensured to meet the response time requirements in the safety analyses.

The staff also found that it was not clear how the response times are calculated differently in the Response Time Analysis TeR for some safety actuation signals generated from the same ESF-CCS. For example, Figure 7.12-3 in this technical report shows a few group controller racks, loop controller racks, and CIM before sending an actuation signal to the safety injection pump. However, Figure 7.12-6 in the above same technical report just shows one group controller rack and loop controller rack before sending an actuation signal to a safety valve. As such, the staff asked the applicant in RAI 300-8297, Question 07.03-4, to provide necessary

design information or clarification on how the response times are calculated differently for some ESF actuation signals, which are executed in the same safety-related I&C system.

In the March 24, 2016, response to RAI 300-8297, Question 07.03-3 (ML16084A928), the applicant stated, in relevant part, that all ESF actuation functions of the safety-related I&C systems identified in Table 7.3-7 of DCD Tier 2, which includes the ESF response time requirements assumed in the safety analysis, are addressed separately in Tables 2.5.1-3 and 2.5.4-4 of DCD Tier 1. This is identified in DCD Tier 1, Section 2.5.4.1, "Design Description," which states that the sensors, APC-S and the ESFAS portions of the PPS are described in Sections 2.5.1 and 2.5.4 describes the EFS-CCS." In addition, Item 20 in DCD Tier 1 Table 2.5.4-4 states that the ESF-CCS provides ESF actuation within required response time for ESF function identified in Table 2.5.4.2 in DCD Tier 1, which includes all ESF systems actuated. For the same ESF actuation function, the sum of each response time requirement stated in Tables 2.5.1-3 and 2.5.4-4 of DCD Tier 1 does not exceed the corresponding function's requirement in Table 7.3-7. The Response Time Analysis TeR provides all response time requirements for reactor trip functions and ESF actuation functions based on Tables 7.2-5 and 7.3-7 of DCD Tier 2. Therefore, the design commitment and associated inspections, tests, and analyses are able to ensure that the integrated safety-related I&C system can meet the response times required in the safety analyses and also proposed in the Response Time Analysis TeR. Thus, the staff found that the response to RAI 300-8297, Question 07.03-3, is acceptable and the issues identified in the above RAI, is closed and resolved.

In the April 5, 2016, response to RAI 300-8297, Question 07.03-4 (ML16096A460), the applicant stated, in relevant part, that the reason why the response times are calculated differently for some safety actuations signals generated from the same ESF-CCS is that each signal path within the ESF-CCS is different depending on the actuated components, offsite power status, and EDG loading sequence. The signal path of the ESF-CCS is categorized into eight cases. In the revised response to RAI 300-8297, Question 07.03-4 (ML16279A534), the applicant provided analyses and specific ESF-CCS calculated response times for the eight signal paths. In the initial and supplemental design information submitted in the RAI responses, the applicant identified the critical points in time and corresponding response times, for which the protective actions shall be actuated. Therefore, the staff finds that the Response Time Analysis TeR combined with initial and supplemental RAI responses provide adequate design information on the eight signal flow paths to demonstrate compliance with Clause 4.10, in IEEE Std 603-1991, regarding identification of the critical points in time for protective actions. However, the staff found that the supplemental design information has not been incorporated in Revision 1 of the Response Time Analysis TeR. Hence, RAI 300-8297, Question 07.03-4, was being tracked as a confirmatory item. The staff verified that the proposed markups have been incorporated in the Response Time Analysis TeR, Revision 2. As such, this confirmatory item has been satisfied.

Additional evaluation of response time analysis is addressed in Sections 7.1.4.9 and 7.9 of this SER.

Clause 4.11, in IEEE Std 603-1991, requires the documentation of any equipment protective provisions that prevent the safety-related systems from accomplishing their safety functions. In the APR1400 design, there is no equipment protective provision that prevents the safety-related systems from accomplishing their safety functions. Therefore, the staff found that the PPS and ESF-CCS design for the ESFAS complies with the requirements in Clause 4.11 of IEEE Std 603-1991.

Clause 4.12, in IEEE Std 603-1991, requires identification of any other special design basis that may be imposed on the system design. The safety-related I&C system is designed to reduce the failure of redundant divisions anticipated by CCF. The APR1400 design provides a DAS, which is a non-safety system and is diverse and separate from the safety PPS and ESF-CCS. The DAS consists of the DPS, DMA, and DIS and provides functions necessary to reduce the risk associated with postulated CCFs of critical protection systems. DCD Tier 2 Section 7.8 has documented the design bases for each DAS subsystem, including the bases for diversity, interlocks, and regulatory criteria. The staff found that Clause 4.12, of IEEE Std 603-1991, has been adequately addressed in the FSAR and is evaluated in detail in Sections 7.1.4.4 and 7.8 of this SER.

7.3.4.3.2 Single Failure Criterion (IEEE Std 603-1991, Clause 5.1)

Clause 5.1, of IEEE Std 603-1991, states, in part, that any single failure within the safety-related system shall not prevent proper protective action when required. Appendix A to 10 CFR Part 50 defines a single failure as an occurrence, which results in the loss of capability of a component to perform its intended safety functions. SRP Appendix 7.1-C for IEEE Std 603-1991, Clause 5.1, states, in part, that the applicant's safety analysis should confirm that the requirements of the single failure criterion are satisfied. Specific guidance in the application of the single failure criterion is provided in RG 1.53, Revision 2.

The staff provided a general evaluation on whether the APR1400 application addressed the single failure criterion appropriately in the design of the safety-related I&C systems in Section 7.1.4.5 of this SER. Specific evaluation for the ESFAS is provided in this section. The bistable processor in the PPS for the safety-related I&C system provides their trip signals to the LCL processor located in the four redundant divisions. The LCL processors determine the LCL trip based on the state of the four bistable trip signals and their respective bypasses. Single failures at the LCL level are accommodated by either redundancy within each division or redundancy across the four divisions. The coincidence trip signals are used in the generation of the ESF-CCS initiation. The PPS is designed so that any single failure within the system will not prevent proper protective action at the system-level, even when a channel is intentionally bypassed for test or maintenance. No single failure will defeat more than one of the four protective divisions associated with any one trip function.

The ESFAS initiation signals from the PPS are sent to separate ESF-CCS cabinets. Each cabinet contains the actuation logic for only one division; therefore, a failure in one cabinet will not affect the circuitry and actuated equipment of the other divisions.

The wiring in the system is grouped so that no single fault or failure, including either an open or shorted circuit, will negate protective system operation. Signal conductors and power leads coming into or going out of each cabinet are protected and routed separately for each division of each system to avoid possible interaction.

Single failures of the actuation (or control) logic will cause, at worst, only a failure of a component, group of components, or one entire redundant train. However, actuation of the remaining redundant division is sufficient for the protective action.

In addition to the method of performing a single failure analysis in IEEE Std 379-2000, an FMEA has also been provided and used to demonstrate compliance with the single failure criterion. The FMEA provided in DCD Tier 2 Table 7.3-8 for the ESFAS and its control system also states

that no single failure will prevent the actuation of ESFAS, nor will a single failure result in spurious actuation of ESFAS.

In reviewing information in Section 7.3 of the FSAR, the staff notes that there is no adequate design information on how the single failure requirements in Clause 5.1, of IEEE Std 603-1991, is met in the safety-related I&C system when one channel is put in the bypass mode due to maintenance and other reasons while another channel has a single failure at the same time. Also there is lack of design information on how the coincidence voting logic in the LCL and ESF-CCS would be changed for the above scenario. In addition, DCD Tier 2 Section 7.3 states that one-out-of-two logics is used in for the BOP ESFAS systems, such as FHEVAS. However, the applicant did not provide sufficient design information to justify exceptions to requirements in Clauses 5.1, 6.3, and 6.7 of IEEE Std 603-1991. For the above reasons, the staff requested the applicant in RAI 323-8281, Questions 07.03-6 and 07.03-7 to provide supplemental design information to demonstrate that the design of the ESFAS and its control systems meets the single failure requirements in Clause 5.1 of IEEE Std 603-1991.

In the April 25, 2016, response to RAI 323-8281, Question 07.03-6 (ML16116A402), the applicant stated, in relevant part, that the safety portion of the I&C system for the FHEVAS has the required redundancy to meet the single failure criterion of Clause 5.1 of IEEE Std 603-1991. Having two divisions of initiating FHEVAS ensures that if there is a loss of safety-related I&C equipment that takes one safety division out of service, the other safety division will remain in service to perform the required ESFAS initiation. The safety portion of the FHEVAS I&C system is designed as Class 1E, seismic Category I, and remains functional during and following a safe shutdown earthquake. Controls, interlocks, sensors, and devices of the safety-related I&C system for FHEVAS are also functionally checked, adjusted, and tested to provide reasonable assurance of intended operation and performance.

In the March 4, 2016, response to RAI 323-8281, Question 07.03-7 (ML16064A060), the applicant also states, in relevant part, that the resulting voting logic would become 1oo2 if the single failure of one channel causes a spurious channel trip condition while another channel is placed in bypass mode. However, the resulting voting logic would become 2oo2 if a single failure does not cause a spurious channel trip condition while another channel is placed in bypass mode. In addition, if a bypass is applied to one channel where a single failure has occurred to avoid spurious reactor trip and ESF initiation due to that channel, the voting logic would become 2oo3. If the bypass is not applied to the channel experiencing a single failure, then the resulting voting logic would remain as 2oo4, if the single failure does not cause a spurious trip condition. However, the resulting voting logic would become 1oo3 if the single failure causes a spurious trip condition.

In the September 19, 2016, supplemental response to RAI 323-8281, Question 07.03-7 (ML16263A434), the applicant further clarified that a single failure of one channel normally occurs in either side of the two redundant PPS cabinets within one channel. If a single failure occurs in one PPS cabinet of that channel and does not cause a spurious trip condition, then the resulting voting logic would remain as 2oo3 while another channel is placed in bypass because the other PPS cabinet of the channel with the single failure is capable of performing its safety function.

The staff found that the above RAI responses provided necessary supplemental design information on how Clause 5.1, of IEEE Std 603-1991, is met for the single failure criterion. The staff finds the proposed changes to the FSAR in RAI 323-8281, Questions 07.03-6 and 07.03-7, are acceptable. The staff verified that the proposed markups have been incorporated into

Revision 1 of DCD Tier 2 Section 7.3.1.3 and Section 4.2.2.1 and A.6.7 of the Safety I&C System TeR. As such, this confirmatory item has been satisfied.

Based on the discussion above and the evaluation in Section 14.3.5 of this SER, and the verification during the implementation of the ITAAC, as defined in DCD Tier 1 Table 2.5.1-5 for ESF initiation and Table 2.5.4-4 for ESF-CCS, the staff found that the APR1400 design meets the requirements on the single failure in Clause 5.1 of IEEE Std 603-1991 for the ESFAS and ESF.

7.3.4.3.3 Quality of Components and Modules (IEEE Std 603-1991, Clause 5.3)

Clause 5.3 of IEEE Std 603-1991 requires that components and modules shall be of a quality that is consistent with minimum maintenance requirements and low failure rates. Safety system equipment shall be designed, manufactured, inspected, installed, tested, operated, and maintained in accordance with a prescribed quality assurance program. SRP Appendix 7.1-C for IEEE Std 603-1991, Clause 5.3 states, in part, that the applicant should confirm that quality assurance provisions of Appendix B to 10 CFR Part 50 are applicable to the safety-related I&C system. For digital computer-based systems, the applicant should also address the quality requirements described in Section 5.3 of IEEE Std 7-4.3.2-2003, which was endorsed in RG 1.152, Revision 3.

Sections 3.10, 3.11, 7.1.4.3, 7.1.4.7, and 7.1.4.8 of this SER evaluate in general whether the quality of components and modules meets the requirements in Clause 5.3 of IEEE Std 603-1991. Specific evaluation for the quality of the ESFAS is provided in this section. The ESFAS is implemented by using Class 1E components. The quality and qualification of ESF components will be verified during the implementation of the ITAAC items, as defined in DCD Tier 1 Table 2.5.1-5 for ESF initiation and Table 2.5.4-4 for the ESF-CCS.

The staff found in Section 8 of the Safety I&C System TeR that the Common Q platform, which includes the FPD system, will be used for the safety-related I&C system. However, there is lack of information in the APR1400 application on whether the FPD system in the Common Q platform approved by the NRC will be used for the ESCM, QIAS-P, and operator module or not. In addition, there are a few types of qualified flat display panels in the Common Q platform, but it was not clear which qualified display panels will be adopted for the above safety display panels in the safety-related I&C system.

As such, the staff requested in RAI 323-8281, Question 07.03-8 that the applicant identify the flat-panel displays that will be used to implement the ESCM, QIAS-P, and operator module and how requirements in Clause 5.3 of IEEE Std 603-1991 are met for these displays. In the March 15, 2016, response to RAI 323-8281, Question 07.03-8 (ML16075A425), the applicant stated, in relevant part, that the Common Q FPD system qualified in Common Q Platform Topical Report, Revision 3 is used for implementation of the safety FPDs for the ESCM, the QIAS-P, and the operator module. The applicant also stated that these FPDs are designed as Class 1E, and the development is performed under a quality assurance program in accordance with 10 CFR Part 50, Appendix B. In addition, the software development is verified and validated as ITS software grade. The communication module and dual ported buffer memory are added into the ESCM FPD to interface to the IFPD. This module and memory will be qualified in the same manner as the ESCM FPD. The response to this RAI question was reviewed and found acceptable by the staff. The staff finds the proposed changes to the Safety I&C System TeR in RAI 323-8281, Question 07.03-8, are acceptable. The staff verified that the

proposed markups have been incorporated into Revision 1 of the Safety I&C System TeR. As such, this confirmatory item has been satisfied.

Based on the evaluation above, the additional evaluation in Sections 7.1 and 14.3.5 of this SER, and the verification during the implementation of the associated ITAAC items in DCD Tier 1 Table 2.5.1-5 for ESF initiation and Table 2.5.4-4 for ESF-CCS, the staff found that the ESFAS and ESF design meets the requirements in Clause 5.3 of IEEE Std 603-1991 for the quality of components and modules.

7.3.4.3.4 Independence (IEEE Std 603-1991, Clauses 5.6 and 6.3)

Clauses 5.6 and 6.3 in IEEE Std 603-1991 require independence between redundant portions of a safety-related system, between safety-related systems and effects of DBEs, and between safety-related systems and other systems. SRP Appendix 7.1-C for IEEE Std 603-1991, Clause 5.6 states, in part, that independence is required between (1) redundant portions of a safety-related systems, (2) safety-related systems and the effects of DBEs, and (3) safety-related systems and other systems. Three aspects of independence should be addressed in each case: physical independence, electrical independence, and communications independence. SRP Appendix 7.1-C for IEEE Std 603-1991, Clause 6.3 states, in part, that the technical review should be conducted to confirm that non-safety system interactions with safety-related I&C systems are limited such that the requirements of 10 CFR 50 Appendix A, GDC 24 are met.

For the ESFAS, the locations of the sensors and the points at which the sensing lines are connected to the process loop have been selected to provide physical separation of the divisions within the system, thereby precluding a situation in which a single event could remove or negate a protective action and safety function. The cabling routing and sensing lines from sensors are designed according to RG 1.75, Revision 3, and RG 1.151, respectively. Cables for each division are physically separated. I&C cables are routed separately from the power cables.

The ESFAS initiation logic is located in four PPS cabinets for NSSS ESFAS signals and the ESF actuation devices are controlled from four ESF-CCS cabinets. The geographical separation and electrical isolation between these cabinets reduces the possibility of a CCF. The outputs of each division are isolated from each other. The loss of one division does not cause loss of the system function. For the ESFAS, there are a few non-safety control signals connected to the ESF-CCS. However, the staff found that those non-safety signals are hardwired with qualified isolation, which meets the independence requirement between the ESFAS and non-safety control signals.

Section 7.1.4.10 of this SER provides a general evaluation on the independence and separation features for the safety-related I&C systems.

Based on the discussion above, the evaluation in Sections 7.1.4.10 and 14.3.5 of this SER, the verification during the implementation of the ITAAC, as defined in DCD Tier 1 Table 2.5.1-5 for ESF initiation and Table 2.5.4-4 for ESF-CCS, and the resolution of the open item associated with RAI 45-7883, Question 07.09-2, the staff determined that the applicant has provided sufficient information to demonstrate the requirements in IEEE Std 603-1991, Clauses 5.6 and 6.3 are met for the ESFAS and ESF.

7.3.4.3.5 Completion of Protective Actions (IEEE Std 603-1991, Clause 5.2)

Clause 5.2, in IEEE Std 603-1991, requires that the safety-related system be designed so that once initiated automatically or manually, the intended sequence of protective actions of the execute features shall continue until completion. SRP Appendix 7.1-C for IEEE Std 603-1991, Clause 5.2 states that the staff's review of this regulatory requirement should include review of functional and logic diagrams to ensure that "seal-in" features are provided to enable system-level protective actions to go to completion.

Section 7.1.4.6 of this SER evaluates the completion of protective actions in general for the safety-related I&C system. Specific evaluation for the ESFAS is provided in this section. The safety-related I&C system is designed to ensure that, once initiated, the protective action will proceed to completion and return to normal operation requires manual reset action by the operator. An ESFAS function is initiated when the 2oo4 voting logic in the PPS is met. A protective and mitigating action is completed when all of the appropriate ESF components are actuated to the proper state for their ESF function. The ESF components remain in the actuated safe state until the ESF system-level actuation signal is manually reset after the trip condition in the PPS is cleared.

As shown in Figure 4-15 in the Safety I&C System TeR, there are two types of ESF signals: ESF-1 and ESF-2. According to the logics illustrated in Figure 4-15, ESF-1 signals cannot be overridden until the plant reaches steady state condition and the ESF command is reset. But, the staff found that ESF-2 commands could be overridden by erroneous commands from ESCM on the operator console. In addition, it was not clear what those ESF-1 and ESF-2 signals are. There was also lack of design information in the FSAR to demonstrate that the ESF-2 initiation signals from the PPS will not be overridden or prevented from the completion of the protection function by the erroneous commands from the ESCM on the operator console which could be initiated from the non-safety IFPD. In addition, it was not clear either in the FSAR where the ESF signals are manually reset after steady state conditions are reached. As such, the staff requested in RAI 300-8297, Question 07.03-5, that the applicant provide additional information to demonstrate that the requirements on the completion of protective actions are met for the ESFAS.

In the March 14, 2016, response to RAI 300-8297, Question 07.03-5 (ML16074A298), the applicant explained, in relevant part, that ESF-2 initiation signals from the PPS can be overridden by commands from the ESF-CCS ESCM due to the existence of certain plant conditions where manual override is necessary. The ESCM sends the component level command to the ESF-CCS loop controller. Divisional redundancy of the ESF-CCS ensures that if there are spurious commands from the ESCM on the operator console, the same component in other safety divisions will remain in service to perform the required safety function. There is very low potential of spurious commands from the ESCM on the operator console causing a single failure of an ESF-CCS division because a spurious signal alone cannot cause the ESF-2 signal to be overridden. Two distinct manual actions (component selection and command selection) are required to override an ESF-2 signal. An ESF signal is reset by either a remote manual reset or a local manual reset. The remote manual reset is performed on the operator module on the safety console. The local manual reset is performed on the MTP cabinet in the I&C equipment room. Because of the additional design information provided by the applicant in the above RAI response that demonstrates how completion of protective functions is achieved to meet the requirements in Clause 5.2 of IEEE Std 603-1991, the staff found the RAI response is acceptable. Therefore, RAI 300-8297, Question 07.03-5, is closed and resolved.

The staff noted that in Section 4.4.2 of the Safety I&C System TeR, the ESFAS signals are generally categorized as ESF-1 and ESF-2. However, there is lack of design information regarding the identification of those ESF components associated with ESF-1 and ESF-2 safety command signals. As such, the staff asked the applicant in RAI 323-8281, Question 07.03-20, to provide a list of components associated with ESF-1 and ESF-2 safety command signals and location in the ESF-CCS where these safety command signals are generated. In the May 3, 2016, response to RAI 323-8281, Question 07.03-20 (ML16124B195), the applicant provided a list of components associated with ESF-1 and ESF-2 safety command signals. The ESF-1 and ESF-2 command signals are generated and split in the ESF-CCS group controller, and distributed to the ESF-CCS loop controller through the SDL. Hence, the staff finds the proposed changes to the Safety I&C System TeR, Revision 0, in the response to RAI 323-8281, Question 07.03-20 are acceptable. The staff verified that the proposed changes have been incorporated into Revision 1 of Section 4.4.2 of the Safety I&C System TeR. As such, this confirmatory item has been satisfied.

The staff was not able to identify in Chapter 7 of DCD Tier 2 on how the control functions are implemented for auxiliary systems that support safe shutdown functions, such ESWS, CCWS, essential chilled water system (ECWS), Class 1E power system, and the HVAC system. As such, the staff asked the applicant in RAI 323-8281, Question 07.03-12, to provide adequate design information accordingly in the application on how the control functions for those auxiliary systems are implemented to support the safe shutdown systems. In addition, the staff also asked the applicant to describe the impact of the loss of HVAC for the safety-related I&C equipment and any mitigating measures to address such loss. This would include the amount of time to when I&C equipment would fails due to rising temperatures. In the March 15, 2016, initial response to RAI 323-8281, Question 07.03-12 (ML16075A425), the applicant stated, in part, that discrete control and modulation control functions for auxiliary safety-related systems such as ESWS, CCWS, Class 1E power system, and HVAC system are implemented in the ESF-CCS loop controller. Each ESF-CCS loop controller cabinet is distributed in I&C equipment rooms or remote multiplexer rooms throughout the plant. The safety HVAC systems connected to the I&C equipment rooms or remote multiplexer rooms of each division maintain the mild (non-harsh) environments to meet the cabinet environmental design requirements specified in Table 7-2 of the Common Q Platform Topical Report, Revision 3. The long-term loss of safety-related HVAC system may result in the loss of safety-related I&C equipment. However, divisional redundancy ensures that if there is a loss of safety-related I&C equipment that takes one safety division out of service, the second safety division will remain in service to perform the required safety function.

The staff found that the March 15, 2016, response did not clarify how the regulatory requirement on completion of protection and independence were addressed in the design of the I&C system for those auxiliary safety-related systems. In the August 8, 2016, supplemental response to RAI 323-8281, Question 07.03-12 (ML16221A735), the applicant stated, in part, that the manual component control of these auxiliary support systems is performed by divisionalized ESF-CCS ESCMs, which are located on the operator consoles and the safety console, or by the minimum inventory switches, which are located on the safety console. Also, automatic control function is provided for these auxiliary support systems to ensure adequate auxiliary supporting features for the safety function. All components of the auxiliary support systems that are required for a safety function receive the ESF actuation signal from the ESF-CCS group controller for automatic actuation. To meet the requirements on independence in Clause 5.6 of IEEE Std 603-1991, the physical separation and electrical isolation of the divisions within the auxiliary support systems are provided. In general, the component in one division of the auxiliary safety-related systems does not receive an interlock signal from another division. However,

there are a few instances where the component in one division of the auxiliary safety-related systems receives an interlock signal from another division through hardwired signals with fiber optic isolation. Because of the commitment to use hardwired signals using fiber optic isolation for transmitting interlock signals between redundant safety divisions, the staff finds the above RAI response adequately demonstrated compliance with requirements on independence in Clause 5.6 of IEEE Std 603-1991 for the ESFAS. Hence, the staff finds the proposed changes to the FSAR in the response to RAI 323-8281, Question 07.03-12 are acceptable. The staff verified that the proposed markups have been incorporated into Revision 1 of DCD Tier 2, Sections 7.4.1 and 7.4.3. As such, this confirmatory item has been satisfied.

The staff noticed that in Figure 7.3-1 in DCD Tier 2 Section 7.3, and Figure 4-13 in the Safety I&C System TeR, the CIM is illustrated to actuate all ESF components without differentiation between on-off and modulating ESF components. Figure 5.3-1 of the CIM TeR shows discrete inputs only to the priority logic section of the CIM for the ESF components. In the APR1400 application there is lack of design information on how safety control functions are implemented in the ESS-CCS system for ESF modulating components. As such, the staff asked the applicant in RAI 323-8281, Question 07.03-14, to provide a clear description on how modulating control functions for certain ESF components are accomplished and also update the technical report and FSAR figures and descriptions accordingly.

In the April 16, 2016, response to RAI 323-8281, Question 07.03-14 (ML16107A027), the applicant stated, in part, that the ESF-CCS provides modulating control functions of safety components. For modulating control in ESF-CCS, the sensors and actuators for modulating control are directly interfaced to the analog input module and the analog output (module in the ESF-CCS loop controller. Any non-discrete components which require modulation are controlled via the analog output module in the ESF-CCS loop controller without the CIM. The ESCM provides the means for manual modulating control of safety components. The ESCM sends component control signals to the CCG through the SDN. The CCG sends component control signals to the ESF-CCS loop controller through the SDN. The ESCM sends manual operator demands such as auto/manual mode change, setpoint value in auto mode, and output value in manual mode, to the ESF-CCS loop controller through the CCG, and the ESF-CCS loop controller sends the actuator demand output. The CIM is bypassed for any modulating control function. The related sections and figures in DCD Tier 2 Section 7.3, the CIM TeR, and the Safety I&C System TeR were also revised accordingly.

Because of the additional design information submitted by the applicant in the RAI response regarding the operation of the modulating control functions in the ESF-CCS, the staff finds the proposed changes to DCD, Section 5.3 of the CIM TeR, and Figure 4-13 of the Safety I&C System TeR, Revision 0, in the response to RAI 323-8281, Question 07.03-14, are acceptable to close this RAI question. The staff verified that the proposed changes have been incorporated into Revision 1 of DCD Tier 2, Section 7.3 and the Safety I&C System TeR. As such, this confirmatory item has been satisfied.

In Section 4.4.2 of the Safety I&C System TeR, the staff found that the valve logics for AFAS are not latched. Similarly, in Section 7.3.1.3 in DCD Tier 2 an exception was taken for the ESF actuation signals for the cycling portion of the AFAS. But, there is lack of justification for such an exception. As such, the staff asked the applicant in RAI 323-8281, Question 07.03-18, to provide justification and description for these ESF commands without latching functions.

In the March 15, 2016, response to RAI 323-8281, Question 07.03-18 (ML16075A425), the applicant states, in part, that the AFWS is started automatically on an AFAS. Under this

emergency signal, both motor-driven and turbine-driven auxiliary feedwater pumps aligned to the affected SGs, are started simultaneously, and the auxiliary feedwater modulating valves to the SGs are automatically placed in the modulation mode. When an AFAS presents, the auxiliary feedwater modulation valves are automatically opened or closed depending on SG level. The auxiliary feedwater modulating valves are designed to fail open if control power is lost. In the unlikely event of such an occurrence, auxiliary feedwater isolation valves will be controlled by a cycling signal generated from the PPS. The cycling AFAS to the auxiliary feedwater isolation valves is not locked, while the latching AFAS signal to the pump is locked. The latching AFAS signal must be manually reset at the ESF-CCS cabinets. This is to allow the SG level to be automatically adjusted between the predetermined high and low levels. When the SG water level reaches the predetermined high level, the cycling AFAS makes the auxiliary feedwater isolation valves for the affected SG close. When the SG water level drops to the low level again, the auxiliary feedwater isolation valves on the flow paths to the affected SG reopen. Opening and closing of the isolation valves continues to occur depending on the water level of the affected SG. The relevant DCD Tier 2 Section 7.3.1.9 was revised accordingly.

Because the applicant added supplemental technical information that adequately describes how the AFWS will be controlled, the staff finds the proposed changes to the FSAR in the response to RAI 323-8281, Question 07.03-18, are acceptable. The staff verified that the proposed changes have been incorporated into Revision 1 of DCD Tier 2 Section 7.3.1.9. As such, this confirmatory item has been satisfied.

The staff found that the L-R (latch-reset) memory and S-R (set-reset) memory are used extensively in the safety-related I&C systems of the FSAR, but the logic associated with setting and resetting the memories is not defined. Such memory components could impact the completion of protective actions. As such, the staff asked the applicant in RAI 323-8281, Question 07.03-15, to provide truth tables, signal diagrams, or other logic-based means to demonstrate the operation of the L-R memory and S-R memory in Figure 7.1-2, “Symbol & Legend Diagram” of DCD Tier 2 for all possible signal combinations. In addition, the staff found that some symbols used for safety-related I&C system diagrams in the FSAR are not included in the above Figure 7.1-2. Hence, the staff also asked the applicant in RAI 323-8281, Question 07.03-15 to include a legend in Figure 7.1-2 for all symbols used in safety-related I&C system diagrams in the FSAR. In the March 15, 2016 response to RAI 323-8281, Question 07.03-15 (ML16075A425), the applicant provided logic tables for the L-R and S-R memories and their explanations. The applicant also added a few symbols to Figure 7.1-2. Based on the provision of these logic tables, explanations, and additional symbols in the RAI response, the staff found that the proposed markups are acceptable to address the issues identified in RAI 323-8281, Question 07.03-15. The staff verified that the proposed changes have been incorporated into Revision 1 of DCD Tier 2, Section 7.1, Figure 7.1-2. As such, this confirmatory item has been satisfied.

Based on the discussion above, evaluation in Sections 7.1.4.6 and 14.3.5 of this SER, and the verification during the implementation of the ITAAC, as defined in DCD Tier 1 Table 2.5.1-5 for ESF initiation and Table 2.5.4-4 for ESF-CCS, the staff found that the APR1400 design for the ESFAS meets the requirements in Clause 5.2 of IEEE Std 603-1991.

7.3.4.3.6 Diversity and Defense-in-Depth

10 CFR 50.62, “Requirements for reduction of risk from anticipated transients without scram events for light-water-cooled nuclear power plants,” identifies design requirements for ATWS mitigation systems and equipment. NRC position on D3 is described in SRM to SECY-93-087,

“Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs.” Diverse manual controls and display systems that are provided to comply with NRC position on D3 shall be independent and diverse from the associated safety-related I&C systems.

Section 7.1.4.21 of this SER evaluates in general the regulatory requirements and guidance on the D3 for the safety-related I&C system. Specific evaluation related to the CIM is provided in this section. The D3 TeR provides detailed design information on D3.

The D3 features for the ESF-CCS are implemented by the DPS and DMA switches. The control signals from the ESF-CCS, DPS, DMA switches, and FPC switches are input control signals to the CIM, and then the CIM prioritizes the control signals according to the established priority logic.

However, the CIM TeR states, in part, that the FPGA portion of the CIM is also safety-related and is used for the diagnostic and surveillance features. But, its software design follows system integrity level 3 classification (i.e., important to safety). As shown in Figure 4.2-1 in the above CIM technical report, several outputs from the non-safety FPGA portion of the CIM are sent back to the safety-related ESF-CCS loop controller. The safety-related DPS is also an FPGA-based system. As such, the staff found that the FSAR did not provide sufficient information to address the potential for software CCF between the two FPGA-based systems. Thus, the staff requested in RAI 37-7882, Question 07.03-1, that the applicant provide design information to demonstrate that the potential for software CCF is addressed between the DPS and CIM. In addition, it was not clear in the APR1400 application how the signals from the non-safety diagnostic section of the CIM will not interfere with the safety functions of the ESF-CCS LCs. In RAI 323-8281, Question 07.03-13, the staff also requested the applicant to describe what measures have been taken to prevent those non-safety diagnostic signals from interfering with the safety functions of the ESF-CCS LCs.

In the August 28, 2015, response to RAI 37-7882, Question 07.03-1 (ML15240A055), the applicant states, in relevant part, that the FPGA-based diagnosis section of the CIM receives status inputs from the base section and the priority logic section of the CIM and provides no outputs to those sections. The outputs of the priority logic section and the base section provide high impedance interfaces with the diagnosis section, so that the counter electromotive force from the diagnosis section cannot adversely affect the other sections. The failure of the diagnosis section cannot adversely affect functions of the priority logic section and the base section because those sections do not receive any signals from the diagnosis section. The results of the diagnosis section are sent to the ESF-CCS loop controller for the purpose of maintenance. The signals are not used in the component control logic in the ESF-CCS loop controller and are used as information to be provided on the MTP.

The application program used to process the signals has no interface with other application programs which are involved in processing component control functions in an ESF-CCS loop controller. A CCF of the diagnosis section may lead to erroneous inputs to dedicated application programs in processing these signals in the ESF-CCS loop controller. These erroneous inputs will only lead to provision of incorrect information for indication on the MTP, but do not adversely affect the application programs of the component control logic because the input signals from the diagnosis section are not used in component control logic. The diagnosis section is developed in accordance with RG 1.152, Revision 3, and SRP BTP 7-14. The V&V of the diagnosis section is carried out in accordance with IEEE Std 1012-2004, software integrity level 3, because the diagnosis section of the CIM only monitors functions and does not perform

any safety actuation function. However, all sections of the CIM are designed and manufactured as Class 1E devices under 10 CFR 50, Appendix B quality assurance program.

In the April 25, 2016, response to RAI 323-8281, Question 07.03-13 (ML16116A402), the applicant stated, in part, that the diagnosis section generates signals that are transmitted to the IPS through the ESF-CCS loop controller and the MTP for the purpose of monitoring. These signals are used only for monitoring by the IPS; and they do not perform any safety function within the ESF-CCS loop controller. Therefore, these signals completely bypass all component control logic functions within the ESF-CCS loop controller. This means there is no interface between these monitoring signals and any ESF-CCS loop controller logic functions. However, the RAI response does not clarify how the implementation of application software for the diagnostic signals will not adversely impact the safety functions in ESF-CCS loop controller. In the August 17, 2016, revised response to RAI 323-8281, Question 07.03-13 (ML16230A400), the applicant stated, in part, that the results of the diagnosis section are sent to the ESF-CCS loop controller through a hardwired connection.

Section 4.2 of the CIM TeR was revised to include the supplemental design information provided in the above RAI responses. The revised design changes to use hardwired connections for the signals from the diagnostic section in the CIM will prevent the diagnostic portion from adversely impacting on the safety logic functions. Because of these design changes proposed in the RAI response, the staff finds the proposed changes to the CIM TeR in the responses to RAI 37-7882, Question 07.03-1, and RAI 323-8281, Question 07.03-13, are acceptable. The staff verified that the proposed changes have been incorporated into Revision 1 of the CIM TeR. As such, this confirmatory item has been satisfied.

Based on the discussion above, general evaluation in Sections 7.1.4.21 and 14.3.5 of this SER, and the verification during the implementation of the ITAAC, as defined in DCD Tier 1 Table 2.5.2-5 for DAS, the staff found that the I&C design meets the requirements on D3.

7.3.4.3.7 System Testing and Inoperable Surveillance (IEEE Std 603-1991, Clauses 5.7, 5.8, and 6.5)

Clauses 5.7 and 6.5, of IEEE Std 603-1991, require capability for testing and calibration of safety-related systems equipment while retaining the capability of the safety-related systems to accomplish their safety functions. Clause 5.8 of IEEE Std 603-1991 states, in part, that the display instrumentation provided for manually controlled actions for which no automatic control is provided and the display instrumentation required for the safety-related systems to accomplish their safety functions shall be part of the safety-related systems and shall meet the requirements of IEEE Std 497-1981, "IEEE Standard Criteria for Accident Monitoring Instrumentation for Nuclear Power Generating Stations." SRP Appendix 7.1-C for IEEE Std 603-1991, Clauses 5.7 and 6.5 states, in part, that guidance on periodic testing of the protection system is provided in RG 1.22, Revision 0, and in RG 1.118, Revision 3. The staff's review for IEEE Std 603-1991, Clause 5.8 on information displays should be coordinated with other technical branches to confirm that the information display and the characteristics of the displays (e.g., location, range, type, and resolution) support operator awareness of system and plant status and will allow plant operators to make appropriate decisions. The review of information displays for manually controlled actions should include confirmation that displays will be functional (e.g., power will be available and sensors are appropriately qualified) during plant conditions under which manual actions may be necessary. Safety system bypass and inoperable status indication should conform to the guidance in RG 1.47, Revision 1.

The ESF system integrity is confirmed through periodic testing during power operation or shutdown. The tests cover the trip actions from sensor input to field actuation device. The system test does not interfere with the protective function. The tests are conducted according to the criteria of IEEE Std 338, which are endorsed by RG 1.118, Revision 3 and RG 1.22, Revision 0. The test equipment consists of divisionalized MTP, ITP, and associated interface circuits. Test results are verified at the MTP. Bypasses and the inoperable status of the safety-related system are displayed at the MTP and operator module in accordance with RG 1.47, Revision 1. Status information including input variable value, setpoint, trip, pre-trip, initiation, trip channel bypass, and operating bypass is displayed at the MTP, operator module, and IPS. Manual testing of the ESF system consists of sensor check, bistable logic test, LCL test, initiation logic test, actuation logic test, selective group test, response time test, and EDG loading sequencer test.

Section 7.1.4.11 of this SER provides evaluation of regulatory requirements in Clauses 5.7 and 6.5 of IEEE Std 603-1991 on system capability for test and calibration and Sections 7.1.4.12 and 7.5 of this SER include evaluation of the regulatory requirements for the information display as required by Clause 5.8 of IEEE Std 603-1991 for the safety-related I&C system.

7.3.4.3.8 Use of Digital Systems (IEEE Std 7-4.3.2-2003)

Section 7.3.2.6 in the FSAR states that all ESFAS functions rely on digital systems. However, the staff found that the CIM, which is used between the ESF Loop Controller and field safety components, is hardware based, as stated in the CIM TeR. The staff also found that the portion for diagnostic and surveillance features in the CIM is the FPGA-based, which, however, is also safety-related. However, as discussed in Section 7.3.4.3.6 of this SER, the staff found that the initial design of the CIM included sending the non-safety diagnostic soft signals to the ESF-CCS safety logic system. The staff issued RAI 323-8281, Question 07.03-13, asking the applicant to address how to prevent the potential adverse interference in the safety logic function from the soft diagnostic signals. In the August 17, 2016, response to this RAI (ML16230A400), the applicant revised the design by using hardwired connections, instead of using soft signals for the diagnostic signals to prevent their potential interference in the safety logic functions. Therefore, based on the staff's evaluation in Section 7.3.4.3.6, the staff found that the use of the hardware for the CIM is acceptable.

Section 7.1.4.7 of this SER evaluates specific features for the use of digital systems in the safety-related I&C system in accordance with IEEE Std 7-4.3.2-2003, as endorsed by RG 1.152, Revision 3. According to evaluation in Section 7.1.4.7 of this SER, the staff found that the safety-related I&C system design meets the criteria listed below for the use of digital systems:

- software development,
- software quality metrics,
- software tools,
- V&V,
- IV&V,
- software configuration management,

- software project risk management,
- computer system testing,
- qualification of existing commercial computers,
- independence, and
- control of access.

7.3.4.3.9 Setpoint Determination

The nominal trip setpoints for the ESFAS are determined based on the safety analysis in DCD Tier 2 Chapter 15. The setpoint methodology follows the methodology in ISA-S67.04-1994, Part 1, as endorsed by RG 1.105, Revision 3. When determining uncertainties, the worst environment conditions considering ESF actuation are assumed for each different event. The methodology for calculating uncertainty is provided in the Uncertainty Methodology TeR. The methodology for combining uncertainty in a division and determining the final actuation setpoint is provided in the Setpoint Methodology TeR. The response time of the I&C division for the ESFAS is the signal propagation time from the process sensor to the final actuation device. The response time for the ESF should meet that assumed in safety analyses in DCD Tier 2 Chapter 15. The ESFAS instrumentation response times assumed in the safety analyses in DCD Tier 2 Chapter 15 are shown in DCD Tier 2 Table 7.3-7. The methodology for calculating system response time is provided in the Response Time Analysis TeR.

Section 7.1.4.25 of this SER provides evaluation of the setpoint determination and methodology for the safety-related I&C system, which includes the ESF systems. Additional evaluation of the response time for the ESFAS and its control systems is conducted in Section 7.3.4.3.1 of this SER.

7.3.4.3.10 Engineered Safety Features for Control System As Required by GDC 34, 35, 38, and 41

The GDC 34, 35, 38, and 41 establish functional requirements for ESF I&C systems which are provided to initiate, control, and protect the integrity of (1) reactor coolant makeup, (2) residual heat removal, (3) emergency core cooling, (4) containment heat removal, (5) containment atmosphere cleanup, and (6) cooling water systems for protection against small breaks in the reactor coolant pressure boundary. In addition, GDC 34, 35, 38, and 41 establish the requirements for testability, operability with onsite and offsite electrical power (assuming only one source is available), and single failures.

The ESF-CCS actuates the ESF shutdown cooling function and performs its ESF component control through the ESFAS portion of the PPS. The ESF-CCS also performs the ESF containment spray function and executes its ESF component control through the ESFAS portion of the PPS. The ESF-CCS performs selective 2oo4 coincidence voting logic for the four-division ESFAS initiation signals derived from the PPS and then control logic of ESF components.

Chapters 5 and 6 of this SER provide technical evaluation on how the APR1400 design complies with GDC 34, 35, 38, and 41. Section 7.3.4.3 above evaluated the I&C design for initiation and control, testability, and single failure for the ESFAS and its control systems.

GDC 34, 35, 38, and 41 set forth requirements for the safety-related systems for which the access to both onsite and offsite power sources must be provided.

Based on the review above and evaluations in Sections 7.3.4.3, Chapters 5, 6, and 8 of this SER, the staff found that the design of the ESFAS and its control systems meets the relevant requirements of GDC 34, 35, 38, and 41.

7.3.5 Combined License Information Items

No applicable items were identified in the FSAR for the ESF systems. No additional COL information items need to be included in DCD Tier 2 Table 1.8-2, "Combined License Information Items," for ESF systems consideration.

7.3.6 Findings and Conclusions

The staff reviewed the design of ESFAS and its control system for compliance with applicable regulations and conformance to relevant regulatory guidance. The staff's review was intended to confirm that the applicant addressed the regulatory requirements related to the ESFAS of the APR1400 design. The applicant has identified adequate high-level functions and included necessary ITAAC items in DCD Tier 1 to verify that ESFAS and its control system is designed in compliance with the applicable regulatory requirements. The staff concludes that the applicant provided adequate and sufficient design information to demonstrate that all the regulatory requirements and acceptance criteria given in SRP Section 7.3 are met for the design of the ESFAS.

7.4 Systems Required for Safe Shutdown

7.4.1 Introduction

The objective of the review is to confirm that the systems that perform the safe shutdown functions satisfy the requirements of the acceptance criteria and guidelines applicable to safety-related systems and that they will perform their safety functions under all plant conditions for which they are required.

The I&C systems and components that support safe shutdown implement the following functions associated with achieving and maintaining a safe shutdown condition: reactivity control; reactor coolant makeup; RCS pressure control; decay heat removal; process monitoring associated with safe shutdown; and support systems, such as electrical power and cooling water systems.

Normal shutdown can be achieved from the MCR or the RSR using both safety-related and non-safety systems whereas safe shutdown is achieved using only safety-related I&C systems. The definition of safe shutdown, the criteria applicable to the specific shutdown scenario, and the equipment that can be used to reach safe shutdown depend upon the plant conditions requiring safe shutdown. To the extent that the ESF systems are used to achieve and maintain safe shutdown, the review of these systems in this section is limited to those features that are unique to safe shutdown and not directly related to accident mitigation.

7.4.2 Summary of Application

DCD Tier 1: The Tier 1 information associated with this section is found in DCD Tier 1 Section 2.5, "Instrumentation and Control."

DCD Tier 2: The applicant provided a system description in DCD Tier 2 Section 7.4, "Systems Required for Safe Shutdown," summarized here, in part, as the following:

The safety-related systems that are required for a safe shutdown are defined as the systems that are essential for pressure and reactivity control, coolant inventory makeup, and removal of residual heat once the reactor has been brought to a subcritical condition. In addition, the alignment of shutdown functions associated with the ESF system that are invoked under postulated limiting fault conditions is addressed in Section 7.3 and Chapter 6 of this SER.

The safety-related systems that are required to a) prevent the reactor from achieving criticality in violation of the Technical Specifications and b) provide an adequate heat sink such that design and safety limits are not exceeded, are listed below.

- AFWS.
- Main steam system (MSS) – atmospheric dump.
- Shutdown cooling system (SCS).
- SIS.
- Safety depressurization and vent system (SDVS).
- Reactor coolant gas vent system (RCGVS).

The auxiliary supporting safety-related systems that are required for a safe shutdown are as follows.

- ESWS.
- CCWS.
- Class 1E EDG system.
- EDG fuel storage and transfer system.
- Class 1E power system.
- HVAC systems.

The ESF systems are used to achieve and maintain safe shutdown. Initiation of the ESF systems are performed by the PPS and RMS. The ESF-CCS actuates and automatically controls safety related systems once the systems have been initiated by the PPS and RMS. The ESF-CCS group controller provides grouped command execution, once the commands are initiated from the ESF-CCS. This is designed to provide control of the safety-related systems that are needed to reach safe shutdown of the plant. The HSI is the ESCM and IFPD. Monitoring and control of the safety-related systems are both available in the MCR and the

RSR. In addition, a minimum inventory switch in each division is available to manually initiate a safe shutdown when all of the operator consoles become unavailable.

Remote shutdown console (RSC) equipment and systems are provided to allow (1) achieving hot standby of the reactor, (2) maintaining the unit in a safe condition during hot shutdown, and (3) achieving cold shutdown of the reactor through the use of operating procedures from outside the MCR.

ITAAC: The evaluation of ITAAC is in Section 14.3.5 of this SER.

Technical Specifications: The Technical Specifications associated with safe shutdown systems are given in DCD Tier 2 Chapter 16 (specifically Sections 3.3.12 and B 3.3.12 of the Technical Specifications). The evaluation of the Technical Specifications for the safe shutdown systems is located in Chapter 16 of this SER.

Technical Reports: Safety I&C System TeR.

7.4.3 Regulatory Basis

The relevant NRC regulations for this area of review, and the associated acceptance criteria, are given in SRP Section 7.4, "Safe Shutdown Systems," and are summarized below. Review interfaces with other SRP sections are found in SRP Section 7.4.

The following requirements apply to DCD Tier 2 Section 7.4:

1. GDC 1, 2, 4, 13, 19, 24, 34, 35, and 38.

2. 10 CFR 50.55a(h)(3), "Safety Systems," states that IEEE Std 603-1991, including the January 30, 1995, correction sheet, is approved for incorporation by reference. For safe shutdown systems that are not safety-related systems as defined by IEEE Std 603-1991 and that are isolated from safety-related systems , the applicable requirements of 10 CFR 50.55a(h)(3) are IEEE Std 603-1991, Clause 5.6.3, "Independence Between Safety Systems and Other Systems"; and IEEE Std 603-1991, Clause 6.3, "Interaction Between the Sense and Command Features and Other Systems."

3. 10 CFR 50.34(f)(2)(xx) or equivalent TMI action plan requirements imposed by Generic Letters.

4. 10 CFR 52.47(b)(1), which requires that a design certification application contain the proposed ITAAC that are necessary and sufficient to provide reasonable assurance that, if the inspections, tests, and analyses are performed and the acceptance criteria met, a plant that incorporates the design certification is built and will operate in accordance with the design certification, the provisions of the Atomic Energy Act, and the NRC's regulations.

Acceptance criteria adequate to meet the above requirements include:

1. Specific acceptance criteria acceptable to meet the relevant requirements of the NRC's regulations identified above are included in SRP Section 7.1, Table 7-1, and Appendix 7.1-A, which list standards, RGs, and SRP BTPs.

2. SRP Appendix 7.1-C provides acceptance criteria for safety-related system compliance with 10 CFR 50.55a(h)(3).

3. SRP Appendix 7.1-D provides acceptance criteria for the digital I&C compliance with IEEE Std 7-4.3.2-2003, as endorsed by RG 1.152, Revision 3.

4. SRP Section 14.3.5 provides the guidance on the ITAAC related to I&C systems.

SRP Table 7-1, Section 3 (SRMs), Section 4 (RGs), and Section 5 (RGs), lists the SRP acceptance criteria applicable to systems required for safe shutdown.

7.4.4 Technical Evaluation

The objective of the staff's review is to confirm that the safe shutdown systems satisfy NRC regulations through a set of acceptance criteria and that they can perform their safety functions for all plant conditions for which they are required.

The primary HSI is the ESCM. Monitoring and control of the safety-related systems are both available in the MCR and the RSR. The operator uses the ESCM and IFPD as the HSI in the MCR and the RSR to achieve and maintain a safe shutdown condition.

The SRP Section 7.4, lists five major design considerations that should be emphasized for the review of safe shutdown systems: (1) independence; (2) use of digital systems; (3) periodic testing; (4) remote shutdown capability; and (5) safe shutdown. Sections 7.1.4.9 and 7.9.4.6 of this SER addresses independence, and periodic testing is addressed in Section 7.1.4.10 of this SER. Use of digital systems, remote shutdown capability, and safe shutdown are addressed in Sections 7.4.4.1 and 7.4.4.2 of this SER.

Several other design considerations are addressed in other sections of this SER, as indicated in Table 7.4-1 below:

Table 7.4-1: Section 7.4 Design Considerations Referenced in Other Sections of this SER.

Design Considerations	Report Section(s)
10 CFR 50.55a(h)(3)	7.1.4.4
10 CFR 50.34(f)(2)(xx)	7.5.4.1.1, 8
10 CFR 52.47(b)(1)	14.3.5
GDC 1	7.1.4.3, 7.1.4.7
GDC 2, GDC 4	7.1.4.8, 3.10, 3.11
GDC 13, GDC 19	7.1.4, 7.5.4.1.2, 7.6.4.6, 7.9.4.3.4, 7.9.4.7, Chapter 18
GDC 34	7.1.4, 7.3.4.3.10, and 8.3.1
GDC 35	7.1.4, 7.3.4.3.10, 8.3.1, 9.3.4
GDC 38	7.1.4, 7.3.4.3.10, 8.3.1

Design Considerations	Report Section(s)
Single failure criterion	7.1.4.5, 7.3.4.3.2
Technical specifications	Chapter 16
ESF	6, 7.3
Independence & GDC 24	7.1.4.10, 7.9.4.6
Capability for Test and Calibration	7.1.4.11
Fire protection program	9.5.1
Information systems	7.1.4.12, 7.5.4.1
Control of access	7.1.4.13, 7.9.4.3.6
Use of digital systems	7.3.4.3.8, 7.7.4.15, Chapter 18

7.4.4.1 Remote Shutdown Capability

GDC 13, requires, in part, instrumentation be provided to monitor variables and systems over their anticipated ranges for normal operation, for AOOs, and for accident conditions as appropriate to assure adequate safety, including those variables and systems that can affect the fission process, the integrity of the reactor core, the reactor coolant pressure boundary, and the containment and its associated systems. GDC 19 requires, in part, that equipment at appropriate locations outside the control room be provided (1) with a design capability for prompt hot shutdown of the reactor, including necessary I&C to maintain the unit in a safe condition during hot shutdown, and (2) with a potential capability for subsequent cold shutdown of the reactor through the use of suitable procedures. The staff used the guidance in SRP Appendix 7.1A and SRP Section 7.4 to determine whether the APR 1400 design meets the requirements of GDC 13 and 19.

The APR1400 design provides for control in locations removed from the MCR that may be used for manual control and alignment of safe shutdown system equipment needed to achieve and maintain hot and cold shutdown. This control equipment should be capable of operating independently of (i.e., without interaction with) the equipment in the MCR. This equipment may include the remote shutdown station and other local controls.

7.4.4.1.1 Operating Independently

The SRP Section 7.4 states that plant designs should provide for control in locations remote from the MCR that may be used for manual control and alignment of safe shutdown system equipment needed to achieve and maintain hot and cold shutdown. SRP Section 7.4 also states that remote shutdown equipment should be capable of operating independently of (i.e., without interaction with) the equipment in the MCR. This equipment may include the RSR and other local controls. Additionally, RSR control transfer devices should be located remotely from the MCR and their location should conform to the procedures for remote, alternative, and dedicated shutdown, as appropriate.

DCD Tier 2 Section 7.4.1.l, “Emergency shutdown from outside the MCR,” identifies the RSR as an independent alternative shutdown location that is physically and electrically independent of the MCR, containing necessary equipment to bring the plant to a safe shutdown state during an event requiring evacuation of the MCR. The ESCM provide the controls while the IFPD and shutdown overview display panel (SODP) provide displays in the RSR to allow for monitoring and control of safe shutdown functions during a fire in the MCR, or during an event that could cause the MCR to become uninhabitable coupled with a single failure, as stated in DCD Tier 2 Section 7.4.2.1.

Additionally, DCD Tier 2 Section 7.4.1.l, states that the MCR/RSR transfer switches maintain divisional independence, so that an electrical failure in one safety division cannot affect another safety division. The transfer switches are each associated with a single division of the safety-related control and allow transfer of control without entry into the MCR. Divisional independence is evaluated in Section 7.1.4.10 of this SER. Data communication independence is evaluated in Section 7.9.4.6 of this SER. DCD Tier 2 Section 7.7.1.2, “Main Control Room Facility,” states that the transfer switches will be located in a separate fire zone than the MCR.

The 10 CFR Part 50, Appendix R, III.G, “Fire Protection of Safe Shutdown Capability,” requires, in part, fire protection features be provided for structures, systems, and components important to safe shutdown. SRP Section 9.5.1.1, “Fire Protection Program,” provides guidance and acceptance criteria for fire protection programs and is evaluated in Section 9.5.1 of this SER.

DCD Tier 2 Section 9.5.1.1, “Design Basis,” states, that the APR1400 design provides an MCR and RSR that are physically separated, electrically isolated, and provide redundant shutdown capability. DCD Tier 2 Sections 7.1.1.4 and 7.4.1 and Tables 7.4-1 and 7.4-2, describe the capabilities and indications needed to achieve both hot and cold shutdown conditions from the RSR for an emergency shutdown outside of the MCR.

DCD Tier 2 Section 7.7.1.2, states that the MCR/RSR master transfer switches are provided in the RSR and I&C equipment rooms for transfer of control from the MCR to the RSR. If a fire is detected within the MCR consoles, as indicated by an early warning smoke detector, the operator actuates the switches. Actuation of the switches initiates each channel of the ESF-CCS and each channel of the P-CCS to perform a soft transfer to deactivate the MCR consoles as a control interface and to activate the RSC control interface. The MTP provides interlocks for performing the transfer of control from the MCR to the RSR.

In RAI 44-7877, Question 07.04-1, the staff requested the applicant to demonstrate in the FSAR how the transfer of control functions from the MCR to the RSR operates independently and to describe how the hardware transfer switches that trigger software switches within the software portion of the design shown in DCD Tier 2, Figures 7.4-1, 7.4-2, and 7.4-3, maintain independence. In the August 11, 2015, response to this RAI (ML15223B082), the applicant revised the Safety I&C System TeR by adding Figures 4-29 and 4-30 and a discussion in Section 4.7.6 that demonstrate how the transfer of control functions from the MCR to the RSR operates independently. It should be noted that as shown in Figure 4-30 and its discussion, the minimum inventory switch signals are blocked when the MCR/RSR master transfer switches are in the RSR position. The proposed changes to the FSAR describe how the hardware transfer switches that trigger software switches within the software portion of the design as shown in the added figures, however, there are some follow-up items concerning Figure 4-29 and a similar figure provided in RAI 44-7877, Question 07.04-2; therefore, the staff found the issue of RAI 44-7877, Question 07.04-1 open at the time. In the December 23, 2015, Revision 1, response to this RAI (ML15357A437), the applicant revised Safety I&C System TeR,

Figures 4.2.9 and 4.30 and the discussion in Section 4.7.6 that demonstrate independence of the transfer of control functions from the MCR to the RSR. The staff reviewed the information submitted by the applicant and concluded that the proposed changes to the Safety I&C System TeR in RAI 44-7877, Question 07.04-1 provide with reasonable assurance that the 10 CFR Part 50, Appendix A, GDC 19 requirements for equipment at appropriate locations outside the control room be provided and capable of operating independently of (i.e., without interaction with) the equipment in the MCR. The incorporation of the proposed markup into the next revision of the Safety I&C System TeR was a confirmatory item. The staff verified that the proposed markups have been incorporated into Revision 1 of Safety I&C System TeR, Section 4.7.6. As such, this confirmatory item has been satisfied.

In RAI 44-7877, Question 07.04-2, the staff requested the applicant to clarify in the DCD Tier 2 Section 7.4.1.l, how the use fiber optic cables for the MCR/RSR master transfer switches provides the isolation between the ESF-CCS divisions and the P-CCS. However, as shown in DCD Tier 2, Figure 7.4-1 and 7.4-2, the isolation occurs in software switches within the ESF-CCF and the P-CCS. The staff requested the applicant to clarify the design descriptions for interconnections involving the MCR/RSR Master Transfer Switches. In the August 11, 2015, response to this RAI (ML15223B082), the applicant provided in more detail how the use of fiber optic cables and hardwire as inputs to the MCR/RSR master transfer switches provide the isolation between the ESF-CCS and the P-CCS. However, there were some follow-up items concerning the Figure 4-29 proposed in RAI 44-7877, Question 07.04-1, and a similar figure provided in this response. Based on the proposed changes made in RAI 44-7877, Question 07.04-1, above and the December 23, 2015, Revision 1 response to this RAI (ML15357A437) that further clarifies the how isolation between the ESF-CCS divisions and the P-CCS is maintained, the staff concludes with reasonable assurance that the revision to the Safety I&C System TeR figures detailing the isolation between the MCR/RSR master transfer switches using hardwire and fiber optic cables satisfies the requirements of 10 CFR Part 50, Appendix A, GDC 24 for separation of protection and control systems. Therefore, RAI 44-7877, Question 07.04-2, is closed.

In RAI 44-7877, Question 07.04-3, the staff requested the applicant to clarify in the FSAR whether equipment in the RSR is fully operational after the transfer of control has taken place. The staff was not able to find in the application whether the equipment in the RSR needs to be booted up, or it was already in an operational condition when a transfer of control is made from the MCR. In the August 11, 2015, response to this RAI (ML15223B082), the applicant stated the RSR is key-locked and it is under administrative control. To access the IFPD for control of the component, a password login is required. DCD Tier 2 Section 7.4.1.l, is modified to state that the IFPDs in the RSR are in operation ready, but control is normally blocked. Based on the proposed change to the FSAR to state the operational conditions when transfer of control from the MCR to the RSR occurs, the staff concludes with reasonable assurance that the proposed changes to the FSAR in RAI 44-7877, Question 07.04-3, satisfies the requirements of GDC 19 for equipment located outside of the control room being capable of operating independently. The incorporation of the proposed markup into the next revision of FSAR was a confirmatory item. The staff verified that the proposed markups have been incorporated into Revision 1 of DCD Tier 2 Section 7.4.1.l. As such, this confirmatory item has been satisfied.

In RAI 44-7877, Question 07.04-4, the staff requested the applicant to clarify in the FSAR how signals from ESF-CCS ESCM in both the MCR and RSR are transferred via the MCR/RSR Master Transfer Switches. DCD Tier 2 Section 7.4.1.l, states “all signals from the MCR are disabled and signals from the RSR are enabled. This includes signals from the ESCM and signals interfaced via the [CPMs].” The staff found in DCD Tier 2 Figure 7.1-1, that signals from

the ESCMs (located in safety console, MCR, and RSR) input into the Safety System Networks; whereas, signals from the CPMs (located on the safety console and RSR) have serial data links into the ESF-CCF group controller. It was unclear how the Safety System Networks signals are transferred to the RSR using the MCR/RSR Master Transfer Switches. In the August 11, 2015, response to this RAI (ML15223B082), the applicant describes the conditions required to trigger the software switch to active mode, so that the data from the ESCM on the RSC can be transmitted to the loop controllers. In addition, Figures 4-29 and 4-30 show the simplified logic of the conditions required to trigger the transfer and discussion in Section 7.7.6 of the Safety I&C System TeR explains how independence is maintained for the transfer of control. Based on the proposed changes made in RAI 44-7877, Questions 07.04-1 and 07.04-2, and the clarifications described in this response, and the editorial change provided in Revision 1 to this RAI response, dated December 23, 2015 (ML15357A437), the staff concludes with reasonable assurance that the response to RAI 44-7877, Question 07.04-4, satisfies the requirements of GDC 19 for equipment located outside of the control room being capable of operating independently. RAI 44-7877, Question 07.04-4, is closed.

In RAI 44-7877, Question 07.04-5, the staff requested the applicant to clarify in the FSAR what control signals are being transferred in ITAAC Item 8 of DCD Tier 1, Tables 2.5.1-5 and 2.5.4-4. Item 8 of DCDDCD Tier 1 Table 2.5.1-5, describes each PPS division being controlled from either the MCR or the RSR as selected from the master transfer switches and Item 8 of Table 2.5.4-4, describes each ESF-CCS division is controlled by the transfer switches. However, DCD Tier 2 Figure 7.4-1, only shows signals from the ESF-CCF going through the transfer switch, not the PPS. The staff requested that the applicant identify the DCD Tier 2 sections that describe the signals being transferred by the master transfer switches as they relate to the ITAAC described in Item 8 of DCD Tier 1, Tables 2.5.1-5 and 2.5.4-4.

In the August 11, 2015, response to this RAI (ML15223B082), the applicant clarified that for the PPS (ITAAC Item 8 of Table 2.5.1-5), the only control functions that will be affected by the state of the MCR/RSR transfer switch are the Operating Bypass and Variable Setpoint Reset requests. For the ESF-CCS (ITAAC Item 8 of Table 2.5.4-4), the ESCMs and the minimum inventory switches in the MCR are interfaced with the ESF-CCS. DCD Tier 2 Figure 7.4-1, and Sections 7.2.1.2, 7.2.1.6, and 7.3.1.5 are being revised as part of the response. Based on the proposed changes to the FSAR to show what controls are transferred in the PPS and the ESF-CCF, when control from the MCR to the RSR occurs. The staff reviewed the information submitted by the applicant and concluded with reasonable assurance, that the proposed changes to the FSAR in RAI 44-7877, Question 07.04-5, are acceptable and satisfies the ITAAC requirements of 10 CFR 52.47(b)(1). The incorporation of the proposed markup into the next revision of the FSAR was a confirmatory item. The staff verified that the proposed markups have been incorporated into Revision 1 of DCD Tier 2, Sections 7.2.1.2, 7.2.1.6, 7.3.1.6, and Figure 7.4-1. As such, this confirmatory item has been satisfied.

In RAI 44-7877, Question 07.04-6, the staff requested the applicant to clarify in the FSAR what control signals are transferred for the PCS and P-CCS as described in ITAAC Item 3 of DCD Tier 1 Table 2.5.5-2, and also to describe how those signals are controlled in the RSR (i.e., what components). DCD Tier 2 Section 7.4 does not describe what signals from the PCS and P-CSS are transferred, and DCD Tier 2, Figure 7.1-1, does not show any interface of the PCS and P-CSS except via the Non-Safety Network. Additionally, DCD Tier 2 Figure 7.1-1, and Section 7.4, do not identify the component(s) that control the PCS and P-CSS signals in the RSR. In the August 11, 2015, response to this RAI (ML15223B082), the applicant provided Figure 4-31 and a discussion in Section 7.7.6 of the Safety I&C System TeR describing that there are two sets of master transfer switches for non-safety divisions: one set located at the

RSC and one set located in the P-CCS cabinet in the I&C equipment room to ensure a single failure does not prevent the transfer. When control is switched from the MCR to the RSR, the control of all components that are controlled by the P-CCS and PCS is transferred to the RSR (ITAAC Item 3 of Table 2.5.5-2). Based on the proposed changes to the FSAR to identify the component(s) that control the PCS and P-CSS signals, when control from the MCR to the RSR occurs. The staff reviewed the information submitted by the applicant and concluded with reasonable assurance, that the proposed changes to the Safety I&C System TeR in RAI 44-7877, Question 07.04-6, are acceptable and satisfies the ITAAC requirements of 10 CFR 52.47(b)(1). The incorporation of the proposed markup into the next revision of the Safety I&C System TeR was a confirmatory item. The staff verified that the proposed markups have been incorporated into Revision 1 of Safety I&C System TeR, Section 4.7.6. As such, this confirmatory item has been satisfied.

The staff reviewed the information submitted by the applicant and concluded with reasonable assurance that the I&C design demonstrates compliance with the requirements in GDC 13, 19 and 24, and IEEE Std 603-1991, Clauses 5.6.3 and 6.3 for independent operation of the RSR and the control transfer switches are met.

7.4.4.1.2 Appropriate Displays and Parameters

The SRP Section 7.4 states that the design of the RSR should provide appropriate displays so that the operator can monitor the status of the shutdown. The design should also maintain parameter indications such that the operators at the MCR and RSR both have access to the same parameters that are being relied upon for safe shutdown.

The DCD Tier 2 Sections 7.4.1.l and 7.4.1.3.4, states the displays in the MCR and the RSR contain real time plant data prior to, during, and after the control transfer from one station to the other. The RSR data are populated from the same information buses that supply data to the MCR. As such, during the time that control is transferred from the MCR to the RSR or vice versa, data is not lost or interrupted. The RSR contains HSI workstations and select communication equipment, necessary to bring the plant to, and maintain it in a safe shutdown state. The HSI control functions of the RSR are isolated during normal, emergency, routine shutdown, refueling, or maintenance operations as long as the MCR is available. The HSI workstations in the MCR and the RSR will continue to display all parameters available on each workstation while the control functions in the RSR are isolated. Information systems important to safety that are necessary to achieve safe shutdown are evaluated in Section 7.5 of this SER.

In RAI 276-8304, Question 07.04-8, the staff requested the applicant to clarify the discrepancies between FSAR Chapter 7, Table 7.4-1 and Chapter 16, Table 3.3.12-1, listings of the remote shutdown equipment. In the January 7, 2016, response to this RAI (ML16007A202), the applicant stated that the tables will be revised as noted in the response so that both Tables 7.4-1 and 3.3.12-1 contain the correct listings of the remote shutdown equipment. The staff reviewed the information submitted by the applicant and concluded with reasonable assurance that the proposed changes to the FSAR in RAI 276-8304, Question 07.04-8, are acceptable. The incorporation of the proposed markup into the next revision of FSAR was a confirmatory item. In the September 11, 2017, the applicant provided a response to this RAI (ML17251A175) to correct typing errors. The staff finds the proposed changes to the FSAR in RAI 276-8304, Question 07.04-8, are acceptable. The incorporation of the proposed markups into the next revision of FSAR was a confirmatory item. The staff verified that the proposed markups have been incorporated into Revision 2 of DCD Tier 2, Chapter 7, Table 7.4-1 and Chapter 16, Table 3.3.12-1. As such, this confirmatory item has been satisfied.

The staff reviewed the information submitted by the applicant and concluded with reasonable assurance that the I&C design demonstrates that the RSR meets the requirements in GDC 13 and 19 for appropriate displays and parameters.

7.4.4.1.3 Accommodating Expected Plant Response

The SRP Section 7.4 states that remote shutdown capability should be capable of accommodating expected plant response following a reactor trip, including protective system actions that could occur as a result of plant cooldown.

The DCD Tier 2 Section 7.4.1.l states that there are sufficient indications and controls provided outside the MCR according to GDC 19 to: (1) achieve hot standby of the reactor, (2) maintain the unit in a safe condition during hot shutdown, and 3) achieve cold shutdown of the reactor through the use of operating procedures. Additionally, DCD Tier 2 Section 7.4.1.n, states that hot shutdown and cold shutdown can be achieved at the RSC by using the direct controls and indications of the equipment listed in Tables 7.4-1 and 7.4-2.

Safe shutdown system's compliance to 10 CFR 50.34(f)(2)(xx) is evaluated in Section 7.5.4.1.1 of this SER.

Because of the provision of indications and controls outside the MCR to achieve and maintain shutdown conditions, the staff finds that the RSR design adequately addresses the design requirement for accommodating expected plant responses as specified in GDC 19.

7.4.4.1.4 Control of Access

The SRP Section 7.4 states that access to the RSR should be under strict administrative controls, and use of the control transfer devices should initiate an alarm in the control room. Additional staff discussion on control of access is provided in Sections 7.1.4.13 and 7.9.4.3 of this SER.

The DCDDCD Tier 2 Section 7.4.1.l, states that the RSR is key locked and under administrative control. In addition, the status of a control transfer is indicated at both the MCR operator consoles and the RSC. The system provides an alarm for each division to the operator that the MCR/RSR master transfer logic has transferred the controls to the RSC. The component controls within each division also report the component group transfer status to the IPS. The transfer status is also indicated on the MCR/RSR master transfer switches by an indication light or on the displays without control and monitoring functions because of the transfer.

The staff reviewed the information submitted by the applicant and concluded with reasonable assurance that the safety-related I&C system design meet the requirements for control of access to the RSR.

7.4.4.1.5 Use of Digital Systems

The DCD Tier 2 Section 7.4.2.5 states that the RPS and ESFAS functions rely on digital systems with the exception of manual actuation switches. The Safety I&C System TeR, Appendix B addresses conformance to IEEE Std 7-4.3.2-2003. The use of digital systems for is evaluated in Sections 7.3.4.3.8 and 7.7.4.15 of this SER. DCD Tier 2 Section 7.7.1, states that the HSI design for both safety-related systems and non-safety systems in the MCR and the RSR are subject to the HFE design processes described and evaluated in Chapter 18 of this SER.

For digital computer-based systems, the applicant addressed the acceptance criteria described in IEEE Std 7-4.3.2-2003, which was endorsed in RG 1.152, Revision 3.

The staff reviewed the information submitted by the applicant and concluded with reasonable assurance that the safe shutdown system design adequately addresses the requirements for the use of digital systems.

7.4.4.2 Safe Shutdown

The staff used the guidance in SRP Appendix 7.1 A and SRP Section 7.4 to determine whether the APR1400 design meets the requirements of single failure criterion, provide the required capacity and reliability to perform intended safety functions on demand, provide the required capacity to function during and after DBEs such as earthquakes and AOOs, operate with onsite electric power available (assuming offsite power is not available) and with offsite electric power available (assuming onsite power is not available) as required by GDC 34, 35, and 38, and provide the capability to be tested during reactor operation.

7.4.4.2.1 Single failure Criterion

The DCD Tier 2 Section 7.4.2.1, states that the I&C required for safe shutdown are designed and arranged so that no single failure can prevent a safe shutdown. The single failures that are considered include electrical faults and physical events resulting in mechanical damage. Each system is composed of redundant trains, including I&C that are physically separated. In addition, a safety console for maintaining the plant in safe condition, which is functionally independent of the operator consoles. A safety console is located in the left side of the MCR. Class 1E hardwired switches are provided as fixed position controls on the safety console for manual actuation of the safety-related systems and components. Hence, the MCR operators can still mitigate the accident and maintain the plant in safe condition using the safety console in the unlikely event that all operator consoles are postulated to fail.

The staff reviewed the information submitted by the applicant and concluded with reasonable assurance that the safety-related I&C system design meet the single failure requirements of IEEE Std 603-1991, Clause 5.1.

7.4.4.2.2 Perform intended safety functions on demand

The DCD Tier 2 Section 7.4.3.3.1, states that none of the essential control or monitoring instrumentation relies solely on instrument air. Where necessary, safety-related accumulator tanks are provided or the failure mode of pneumatic devices upon loss of air is designed to fail in the safe position. Therefore, loss of instrument air does not degrade the I&C associated with systems required for plant shutdown.

The DCD Tier 2 Section 7.4.3.3.2, states that a loss of cooling water to vital equipment does not affect the safe shutdown function because the safety-related CCWS has two separate divisions of cooling water systems.

Additionally, DCD Tier 2 Section 7.4.3.3.3, states that in the event of a LOOP associated with plant load rejection or turbine trip, the power for safe shutdown is provided by the EDGs. The EDGs provide power for operation of pumps and valves; the batteries, or EDGs via the battery chargers, provide power for operation of I&C systems required to actuate and control essential components.

The staff reviewed the information submitted by the applicant and concludes with reasonable assurance, that the safe shutdown system has multiple and sufficient means to address the requirements to perform intended safety functions on demand as required by IEEE Std 603-1991, Clause 5.

7.4.4.2.3 Function during and after DBEs

The alignment of shutdown functions associated with the ESFs that are invoked under postulated limiting fault conditions is addressed in Chapter 6 and Section 7.3 of this SER. GDC 1, 2, and 4 are evaluated in Sections 7.1.4.3, 7.1.4.7, 7.1.4.8, 3.10, and 3.11 of this SER.

The staff reviewed the information submitted by the applicant and concluded with reasonable assurance that the safe shutdown system adequately addresses the requirement to function during and after DBEs.

7.4.4.2.4 Operate with onsite electric power available (assuming offsite power is not available) and with offsite electric power available (assuming onsite power is not available)

The DCD Tier 2 Section 7.4.1.i, states that there are four independent, 100 percent capacity EDGs (one per division) that provide a dependable onsite power source. Four EDGs are capable of starting and supplying the essential loads necessary to shut the plant down safely and reliably. The EDGs maintain the plant in a safe shutdown condition under a LOOP event. The EDGs start automatically by an undervoltage signal (LOOP event detected on the associated Class 1E 4.16 kV bus), AFAS, SIAS, or CSAS. Section 8.3.1 of this SER evaluates the non-Class 1E alternate alternating current gas turbine generator standby power supply. The emergency diesel engine starting system is evaluated in Section 9.5.6 of this SER.

Based on the staff's evaluations in Sections 8.3.1 and 9.5.6 of this SER, the staff concludes with reasonable assurance that the safe shutdown system adequately addresses the requirement to operate with onsite electric power available (assuming offsite power is not available) and with offsite electric power available (assuming onsite power is not available) as required by GDC 34, 35, and 38.

7.4.4.2.5 Capability to be tested during reactor operation

The DCD Tier 2 Section 7.4.2.4, states that the I&C components required for safe shutdown that are not normally in operation are capable of being tested periodically. The components include I&C for the SCS, SIS, and the rapid depressurization function of SDVS. All automatic and manual actuation devices are capable of being tested to verify their operability. The MCR/RSR master transfer switches are also tested periodically.

Based on the provision of periodical testing capabilities for I&C components required for safe shutdown, automatic and manual actuation devices, and MCR/RSR master transfer switches, the staff concludes with reasonable assurance, that the APR1400 safe shutdown system adequately addresses the requirements for periodic testing as specified in IEEE Std 603-1991, Clause 5.7, and GDC 21 and 18.

7.4.4.3 ITAAC

The evaluation of ITAAC is in Section 14.3.5 of this SER.

7.4.5 Combined License Information Items

No applicable items were identified in the FSAR. No additional COL information items need to be included in DCD Tier 2 Table 1.8-2, for systems required for safe shutdown consideration.

7.4.6 Findings and Conclusions

The staff reviewed the information submitted by the applicant and concluded with reasonable assurance that the I&C system maintain variables and systems that can affect the fission process, the integrity of the reactor core, the reactor coolant pressure boundary, and the containment and its associated systems within prescribed operating ranges during plant shutdown. I&C functions have been provided within the MCR to allow actions to be taken to maintain the nuclear power unit in a safe condition during shutdown, including a shutdown following an accident. Equipment at appropriate locations outside the control room provide (1) a design capability for prompt, hot shutdown of the reactor, including necessary I&C to maintain the unit in a safe condition during hot shutdown, and (2) potential capability for subsequent cold shutdown of the reactor through the use of suitable procedures. The staff finds with reasonable assurance that the I&C systems required for safe shutdown adequately address the requirements of GDC 1, 2, 4, 13, 19, 24, 34, 35, and 38; 10 CFR 50.55a(h)(3) which include applicable requirements in IEEE Std 603-1991, Clauses 5.6.3 and 6.3; 10 CFR 50.34(f)(2)(xx); and 10 CFR 52.47(b)(1).

7.5 Information Systems Important to Safety

7.5.1 Introduction

The objective of this review is to confirm that the information systems important to safety satisfy the requirements of the acceptance criteria and guidelines applicable to these systems, and that they will provide the information to ensure plant safety under all plant conditions for which they are required.

Information systems important to safety include I&C systems that provide information to the plant operators for: (1) assessing plant conditions, safety-related system performance and making decisions related to plant responses to abnormal events; and (2) pre-planned manual operator action related to accident mitigation. The information systems reviewed in this section also provide the necessary information from which appropriate actions can be taken to mitigate the consequences of AOOs.

Specific information systems include AMI; BISI for safety-related systems; plant annunciator (alarm) systems; the safety parameter display system (SPDS); and Information systems associated with the emergency response facilities (ERF) and emergency response data system (ERDS).

7.5.2 Summary of Application

DCD Tier 1: The Tier 1 information associated with this section is found in DCD Tier 1 Section 2.5.

DCD Tier 2: The applicant has provided a system description in DCD TierTier 2 Section 7.5, and summarized as the following.

The information systems important to safety are described I&C systems that provide information to the plant operators for (1) assessing plant conditions and safety-related system performance, (2) making decisions related to plant responses to abnormal events, and (3) taking pre-planned manual operator actions related to accident mitigation. Information systems important to safety also provide the necessary information from which appropriate actions can be taken to mitigate the consequences of AOOs and postulated accidents.

The information systems important to safety.

- AMI.
- ICC monitoring instrumentations.
- BISI.
- Alarm system.
- SPDS.
- ERF and ERDS.

The information important to safety is available for display at the following facilities.

- MCR.
- RSR.
- TSC.
- EOF.

ITAAC: The evaluation of ITAAC is in Section 14.3.5 of this SER.

Technical Specifications: The Technical Specifications associated with DCD Tier 2 Section 7.5, are given in DCD Tier 2 Chapter 16, Sections 3.3.11, 3.3.12, B 3.3.11, and B 3.3.12.

Technical Reports: The Safety I&C System TeR.

7.5.3 Regulatory Basis

The relevant NRC regulations for this area of review, and the associated acceptance criteria, are given in the SRP Section 7.5, “Information Systems Important to Safety,” and are summarized below. Review interfaces with other SRP sections can be found in SRP Section 7.5.

Requirements applicable to AMI and ICC monitoring instrumentations:

1. GDC 1, 2, 4, 13, 19, and 24.

2. 10 CFR 50.55a(h), “Safety Systems,” requires compliance with IEEE Std 603-1991, and the January 30, 1995, correction sheet. For AMI isolated from the protection system, the applicable requirements of 10 CFR 50.55a(h) for IEEE Std 603-1991 are Clause 5.6.3,

"Independence between Safety Systems and Other Systems," and Clause 6.3, "Interaction between the Sense and Command Features and Other Systems."

3. 10 CFR 50.34(f), "Additional TMI-Related Requirements." The following portions of 10 CFR 50.34(f) applies to AMI:

   a. 10 CFR 50.34(f)(2)(v), as it relates to BISI.

   b. 10 CFR 50.34(f)(2)(xi), as it relates to direct indication of relief and safety valve position.

   c. 10 CFR 50.34(f)(2)(xii), as it relates to AFWS flow indication (applicable to PWRs only).

   d. 10 CFR 50.34(f)(2)(xvii), as it relates to AMI.

   e. 10 CFR 50.34(f)(2)(xviii), as it relates to ICC instrumentation.

   f. 10 CFR 50.34(f)(2)(xix), as it relates to instruments for monitoring plant conditions following core damage.

   g. 10 CFR 50.34(f)(2)(xx), as it relates to power for pressurizer level indication.

Requirements applicable to BISI:

1. GDC 1 and 24.

2. 10 CFR 50.55a(h)(3), "Safety Systems," requires compliance with IEEE Std 603-1991 and the January 30, 1995, correction sheet. For BISI, the applicable requirements for IEEE Std 603-1991 are Clause 5.8.3, "Indication of Bypasses." For BISI that are isolated from the safety-related systems the requirements for IEEE Std 603-1991 are Clauses 5.6.3 and 6.3.

3. 10 CFR 50.34(f)(2)(v) as it relates to BISI.

Requirements applicable to annunciator systems:

1. GDC 1, 13, 19, and 24.

2. 10 CFR 50.55a(h)(3) requires compliance with IEEE Std 603-1991 and the January 30, 1995, correction sheet. For annunciators that are isolated from the protection system, the applicable requirement(s) of 10 CFR 50.55a(h)(3) for IEEE Std 603-1991 are Clauses 5.6.3 and 6.3.

Requirements applicable to the review of SPDS, ERF, and ERDS information systems:

1. GDC 1 and 24.

2. 10 CFR 50.55a(h)(3) requires compliance with IEEE Std 603-1991 and the January 30, 1995, correction sheet. For SPDS, ERF information systems, and ERDS information systems isolated from the protection system, the applicable requirements of 10 CFR 50.55a(h)(3) for IEEE Std 603-1991 are Clauses 5.6.3, and 6.3.

3. 10 CFR 52 CFR 52.47(b)(1), which requires that a design certification application contain the proposed ITAAC that are necessary and sufficient to provide reasonable assurance that, if the inspections, tests, and analyses are performed and the acceptance criteria met, a plant that incorporates the design certification is built and will operate in accordance with the design certification, the provisions of the Atomic Energy Act, and the NRC's regulations.

Acceptance criteria adequate to meet the above requirements include:

1. Specific acceptance criteria acceptable to meet the relevant requirements of the NRC's regulations identified above are included in SRP Section 7.1, Table 7-1, and Appendix 7.1- A, which list standards, RGs, and SRP BTPs.

2. SRP Appendix 7.1-C, which provides acceptance criteria for safety-related system compliance with 10 CFR 50.55a(h)(3).

3. SRP Appendix 7.1-D, which provides acceptance criteria for the digital I&C compliance with IEEE Std 7-4.3.2-2003 as endorsed by RG 1.152, Revision 3.

4. Item 18, II.Q, "Defense Against Common Mode Failures in Digital Instrument and Control Systems," of the SRM on SECY 93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and ALWR Designs," provides guidance on D3. SRP BTP 7-19, "Guidance for Evaluation of Diversity and Defense-in-Depth in Digital Computer-Based Instrumentation and Control Systems," Revision 6, provides additional guidance.

5. SRP Section 14.3.5 provides the guidance on the ITAAC related to I&C systems.

6. RG 1.97, Revision 4, describes methods acceptable to the staff for providing instrumentation to monitor variables for accident conditions. SRP BTP 7-10, "Guidance on Application of Regulatory Guide 1.97," provides guidance on the application of RG 1.97, Revision 4. SRP Table 7-1, Section 3 (SRMs), Section 4 (RGs), and Section 5 (BTPs), lists the SRP acceptance criteria applicable to information systems important to safety.

7.5.4 Technical Evaluation

The objective of the staff's review is to confirm that information systems important to safety satisfy NRC regulations through a set of acceptance criteria and that the information systems important to safety can perform the intended safety functions for all plant conditions.

Information necessary to monitor the NSSSs, containment systems, and BOP is displayed on the operator console and the various screens and panels located within the MCR. Information systems important to safety are those systems that provide information to control and operate the unit safely through all operating conditions, including AOO, and accident and post-accident conditions. However, this SER section is limited to the discussion of those display instruments that provide information (1) to enable the operator to assess reactor status, onset, and severity of accident conditions, and ESF actuation status and performance, or (2) to enable the operator to reliably perform vital manual actions such as safe shutdown and initiation of manual ESF actuation.

Information systems important to safety are broken down into four subsystems. SRP Section 7.5, Revision 5, lists the following major design considerations that should be emphasized for the review of each system:

- AMI.
- Conformance to RG 1.97, Revision 4, and SRP BTP 7-10.
- Use of digital systems.
- EOP action points.
- Monitoring for severe accidents.
- Performance assessment.

Bypassed or Inoperable Status Indication for Safety Systems

- RTS and ESFAS.
- SRP BTP 7-1, “Guidance on Isolation of Low-Pressure Systems from the High-Pressure RCS.”
- SRP BTP 7-2, “Guidance on Requirements of Motor-Operated Valves in the Emergency Core Cooling System Accumulator Lines.”
- SRP BTP 7-6, “Guidance on Design of Instrumentation and Controls Provided to Accomplish Changeover from Injection to Recirculation Mode.”
- Conformance to RG 1.47, Revision 1.
- Independence.
- Use of digital systems.

Plant Alarm Systems:

- Reliability.
- Use of digital systems.
- Independence.
- Redundancy.

SPDS, Information systems associated with the ERF, and ERDS:

- Independence.

Additionally, the SRP lists other criteria that should also be considered. Several of these design considerations are addressed in other sections of this SER, as indicated in Table 7.5-1 below:

Table 7.5-1: Design Considerations Referenced in Other Sections of this SER

Design Considerations	Report Section(s)
10 CFR 50.55a(h)(3)	7.1.4.4
10 CFR 52.47(b)(1)	14.3.5
GDC 1	7.1.4.3, 7.1.4.7
Independence & GDC 24	7.1.4.10, 7.9.4.6
Separation of Protection and Control Systems	7.1.4.10.4
SRP BTP 7-1	7.6.4.7
SRP BTP 7-2	7.6.4.7
GDC 13 and 19	7.1.4, 7.4.4.1, 7.6.4.6, 7.9.3.4, 7.9.4.7, Chapter 18
Automatic and Manual ESF Initiation	7.1.4.22
Setpoint Requirements	7.1.4.25
SRM to SECY-93-087, Item II.T	7.1.4.21, 7.3.4.3.6
Use of Digital Systems	7.3.4.3.8, 7.7.4.15, Chapter 18

7.5.4.1 Accident Monitoring Instrumentation

The SRP Section 7.5 identifies regulations applicable to AMI. These regulations are addressed below in Sections 7.5.4.1.1 and 7.5.4.1.2 of this SER.

The QIAS-P provides a continuous display of AMI variables (Types A, B, and C) and indication of the approach and recovery from ICC as a backup to the SPDS. The QIAS-N displays AMI Type A, B, C, and selected sets of Type D and E variables. The IPS provides displays for all AMI variables.

The recording function for Type A, B, and C variables is performed in the IPS. The QIAS-P calculates representative core exit temperature, primary coolant saturation margins, and reactor vessel coolant water level. The QIAS-P provides output signals to the QIAS-P display via the SDN, to the MTP for the IPS (via unidirectional Ethernet datalink), and to the ITP for the QIAS-N (via the SDL). In all cases, these output signals are for display of sensor signals, ICC variables, and AMI variables.

The QIAS-P has two divisions. Each QIAS-P cabinet is located in its division I&C equipment room. The QIAS-P receives AMI variables from the PPS and the ESF-CCS via the SDN; and APC-S and process instrumentation via hard-wired connection. The QIAS-P also displays the status of containment isolation valves (CIVs) from both QIAS-P divisions. The status of the other QIAS-P division CIVs are obtained from the ITP through the interdivisional SDL.

7.5.4.1.1 TMI-Related Requirements

The TMI action plan requirements for I&C systems important to safety are imposed by 10 CFR 50.34(f). SRP Appendix 7.1-A identifies both the 10 CFR Part 50 and TMI action plan reference

numbers for the TMI action plan requirements relevant to Chapter 7. The guidance in SRP Appendix 7.1-A identifies specific acceptance criteria for TMI action plan items.

The following portions of 10 CFR 50.34(f)(2) are applicable to AMI:

(v) BISI.

(xi) direct indication of relief and safety valve position.

(xii) auxiliary feedwater system flow indication.

(xvii) AMI.

(xviii) inadequate core cooling instrumentation.

(xix) monitoring plant conditions following core damage.

(xx) power for pressurizer level indication.

The DCD Tier 2 Table 7.1-1, which is evaluated in Section 7.1 of this SER, the applicant identified that the following TMI action plan items that are applicable to the APR1400 design and are discussed as follows:

The 10 CFR 50.34(f)(2)(v) requires an automatic indication of the bypassed and inoperable status of safety-related systems. The Safety I&C System TeR, Section 3.1, states that the indications of bypasses and inoperable status of the safety-related I&C system are available on the operator module, MTP, QIAS-N and IPS displays.

The 10 CFR 50.34(f)(2)(xii) requires automatic and manual auxiliary feedwater system initiation and flow indication in the MCR. Section 7.3.4.2.2 of this SER discusses automatic and manual), AFAS initiation. The Safety I&C System TeR, Section 3.1, states that the low SG water level trip signal initiates a reactor trip when the measured water level in a SG's downcomer region falls to a low preset value. Separate initiations are provided for the RPS and AFAS to allow different setpoints for reactor trips and auxiliary feedwater actuations. The AFAS continues to deliver auxiliary feedwater to the SG until a preset water level has been reestablished. Manual actuation is provided to permit the operator to actuate the AFAS. Auxiliary feedwater flow rate is displayed on the QIAS-N, IPS, and DIS. DCD Tier 2 Section 10.4.9.3, "Safety Evaluation," states that the AFWS can be manually or automatically actuated by an AFAS from the MCR to safely operate and maintain the plant under normal and accident conditions.

For 10 CFR 50.34(f)(2)(xi), (f)(2)(xvii), (f)(2)(xviii), (f)(2)(xix), and (f)(2)(xx) requirements, the Safety I&C System TeR, Section 3.1, states that AMI Types A, B, and C variables are displayed on the QIAS-P, QIAS-N, and IPS. The QIAS-N displays selected variables of Types D and E to support plant safe shutdown and the EOP. All variables of Types D and E are displayed on the IPS. DCD Tier 2 Table 7.5-1, provides the list of all variables that allow the operator to assess the state of the plant following DBEs by monitoring instruments, equipment, or systems that provide automatic action.

7.5.4.1.2 Post-Accident Monitoring Instrumentation

The GDC 13 and 19 address AMI. GDC 13 requires, in part, that instrumentation be provided to monitor variables and systems over their anticipated ranges for normal operation, for AOOs,

and for accident conditions as appropriate to assure adequate safety, including those variables and systems that can affect the fission process, the integrity of the reactor core, the reactor coolant pressure boundary, and the containment and its associated systems. GDC 19 requires, in part, that a control room be provided from which actions can be taken to operate the nuclear power unit safely under normal conditions and to maintain it in a safe condition under accident conditions, including LOCAs. To assess the AMI design against the regulations, the staff used the guidance found in SRP Appendix 7.1 A, SRP Section 7.5, RG 1.97, Revision 4, RG 1.105, Revision 3, and SRP BTP 7-10.

A. Conformance to RG 1.97, Revision 4 and SRP BTP 7-10

DCD Tier 2 Table 7.5-1, identifies a list of AMI variables and establishes that the design conforms to RG 1.97, Revision 4. However, the applicant did not clearly demonstrate how they conform to RG 1.97, Revision 4, for each variable, including the analysis or basis for the variable. In RAI 38-7878, Question 07.05-1, the staff requested the applicant to provide in the DCD Tier 2 Section 7.5.1.1, the basis or analysis for the selection of the AMI variables.

As stated above, the QIAS-P provides a continuous display of AMI variables (Types A, B and C), QIAS-N displays AMI Types A, B, C, and selected sets of Types D and E variables and the IPS provides displays for all AMI variables. Providing means for monitoring these variables provide reasonable assurance of safety by including those variables and systems that can affect the fission process, integrity of the reactor core, reactor coolant pressure boundary, or containment and its associated systems.

The AMI listed in Table 7.5-1 allows the operator to assess the state of the plant following DBEs by monitoring instruments, equipment, or systems that provide automatic action. The June 10, 2016 response to this RAI (ML16162A561) did not satisfactorily resolve all of the staff's concerns, therefore, RAI 38-7878, Question 07.05-1 remained open. RAI 38-7878, Question 07.05-1, was tracked as an open item. In the supplemental responses to RAI 38-7878, Question 07.05-1 (ML16292A489, ML17271A079, ML17290B224, and ML17331B467), the applicant revised DCDDCD Tier 1 Table 2.5.3-2 and Table 2.5.4-6, DCD Tier 2, Sections 7.5.1.1, 7.5.1.2, Table 7.5-1, Figure 7.7-12, and added a new Table 7.5-2 to provide additional AMI variables and the bases for their selection. The response also included proposed markups to revise DCD Tier 2 Chapter 16, Table 3.3.11-1 and Sections B 3.3.11, B 3.4.7, B 3.4.8, B 3.4.9, and B 3.4.16. Revisions were also made to the Safety I&C System TeR, Section 4.5 and Table 4-6 and to the D3 TeR, Appendix C. The staff finds these responses provide an adequate list, the methodology, and the basis for selection of AMI Types A, B, C, D, and E variables in accordance with the guidance of RG 1.97, Revision 4. Hence, the staff finds the proposed changes to the FSAR in RAI 38-7878, Question 07.05-1 are acceptable. The incorporation of the proposed markups into the next revision of FSAR and TeRs was a confirmatory item. The staff verified that the proposed markups have been incorporated into Revision 2 of DCD Tier 1, Tables 2.5.3-2 and 2.5.4-6, Revision 2, of DCD Tier 2 Table 7.5-1, Chapter 16, Table 3.3.11-1 and the Bases for TS 3.3.11, Revision 2, of the Safety I&C TeR, and the D3 TeR. As such, this confirmatory item has been satisfied.

In RAI 294-8302, Question 07.05-7, the staff requested the applicant to clarify in the FSAR, the instrumentation provided to monitor variables and systems over their anticipated ranges for normal operation, for AOOs, and for accident conditions as

required by GDC 13 and to revise the FSAR/technical report or table to show that the IFPD and ESCM are the primary controls for safety related equipment during normal, accident, and abnormal conditions. In the December 31, 2015, response to this RAI (ML15365A555), the applicant's response conflicts with previous submitted documents. In response 1, dated August 30, 2016, to this Tier 2 Section 7.5 that shows when the IFPD and the ESCM are used as the primary and backup means for control during normal, abnormal, and DBA conditions (includes CCF and MCR evacuation). Section 7.7.1.2 further describes what components are controlled by the IFPD and ESCMs and during what mode of operation. The staff finds the proposed changes to the FSAR in RAI 294-8302, Question 07.05-7, are acceptable. The incorporation of the proposed markup into the next revision of FSAR was a confirmatory item. The staff verified that the proposed markups have been incorporated into Revision 1 of DCD Tier 2, Figure 7.5.3-3, Sections 7.7.1.2, and 7.2.3. As such, this confirmatory item has been satisfied.

The QIAS-P is designed to meet the requirements of GDC 13 and 19. RG 1.97, Revision 4, indicates that the AMI variables should be selected based on emergency guidelines and procedures. As endorsed by RG 1.97, Revision 4, IEEE Std 497-2002, provides performance-based criteria for selecting variables and recommends determining the variable type according to its accident management function. The accident management function is to be identified by its use in the Emergency Procedure Guidelines, Emergency Operating Procedures, and Abnormal Operating Procedures. The development of these guidelines and procedures is discussed in DCD Tier 2 Section 13.5 and evaluated in Section 13.5 of this document.

Furthermore, by conforming to RG 1.97, Revision 4, certain AMI equipment will meet environmental and seismic qualification per 10 CFR 50.49(b)(3). IEEE Std 497-2002, Clause 7, presents the environmental and seismic qualification criteria of Types A, B, C, D, and E variables. The staff review and discussion of how the APR1400 design addresses equipment qualification is located in Section 3.11 of this SER.

In RAI 38-7878, Question 07.05-2, the staff requested the applicant to clarify in the DCD why the APR1400 design has no Type A variables when there are manual actions described in DCD Tier 2 Chapter 15 (e.g., manual actions for a SGTR). In the August 3, 2015 response to this RAI (ML15216A459), the applicant's response did not provide sufficient justification for why Type A variables are not needed for the APR1400 design. Therefore, the applicant did not provide sufficient information to demonstrate the requirements of GDC 13 and the guidance provided by RG 1.97, Revision 4 and IEEE 497-2002, Section 4.1 as it pertains to Type A variables are met. Instead of a supplemental question to this RAI, the staff closed this RAI and created a new RAI. RAI -Question -In RAI 294-8302, Question 07.05-6, the staff requested the applicant provide a table of all operator actions required by Chapter 15; listing all indications that the operator would rely on, the location and qualification for each indication that is needed by the operator to demonstrate how the requirements of GDC 13 and the guidance provided by RG 1.97, Revision 4 and IEEE 497-2002, Section 4.1 as it pertains to Type A variables. In the June 1, 2016, response to this RAI (ML16153A476), the applicant provided the following in their response; "The result of evaluating manually controlled actions performed by control room operating staff in this manner is that no Type A variables exist for the APR1400." The response has not satisfactorily resolved all of the staff's concerns, therefore, RAI 294-8302, Question 07.05-6 remains open. In the June 1, 2016 response to RAI 294-8302, Question 07.05-6 (ML16153A476), the

applicant provided a list of AMI Type A variables as part of the response for RAI 38-7878, Question 07.05-1 (ML16292A491). The staff finds that the response in to RAI 294-8302, Question 07.05-6, and the proposed changes to the FSAR, the Safety I&C System TeR and the SPM TeR in RAI 38-7878, Question 07.05-1, are acceptable because the applicant provided adequate AMI Type A variable identification. The incorporation of the proposed markups into the next revision of FSAR and TeRs was a confirmatory item. The staff verified that the proposed markups have been incorporated into Revision 1 of FSAR Revision 1 of the Safety I&C System TeR and the SPM TeR. As such, this confirmatory item has been satisfied.

The DCD Tier 2 Section 7.5.2, describes how the AMI complies with the acceptance criteria in RG 1.97, Revision 4 and IEEE 497-2002.

1) Single failure

   The QIAS-P consists of two divisions that are electrically and physically isolated from each other so that AMI information is still displayed if any single failure within the system occurs. The QIAS-P is also independent and separate from the QIAS-N and IPS. The QIAS-N is classified as a non-safety system, therefore single failure criterion does not apply.

2) CCF

   To avoid complete AMI information loss caused by a CCF, the QIAS-P and the QIAS-N are implemented using a PLC-based platform while the IPS is implemented using a DCS-based platform.

3) Independence and separation

   Redundant AMI channels for the QIAS-P are electrically independent of and physically separated from each other.

4) Isolation

   The QIAS-P is isolated from the QIAS-N and the IPS. The isolation device meets the guidance of IEEE Std 384-1992, as endorsed by RG 1.75, Revision 3.

5) Information ambiguity

   To resolve the information ambiguity, additional variables are provided as listed in DCD Tier 2 Table 7.5-1.

6) Power supply

   The QIAS-P is powered from Class 1E battery and EDG-backed, Vital Instrument power buses A and B. The QIAS-N is classified as non-safety system but is powered from Vital Instrument Power Bus D, which is battery and EDG-backed. The IPS is powered from non-Class 1E vital instrument power which is also battery backed.

7) Calibration, testability, and access control

Calibration and testing are performed after the related systems are offline. Redundant design features provide reasonable assurance of the continuous display of AMI variables during calibration or test. Periodic tests are performed following the guidance of RG 1.118, Revision 3, and access to any sensor or module for calibration or testing is administratively controlled. Devices are located outside the containment so that they can be accessed for maintenance during accident conditions.

8) Direct measurement

The QIAS-P provides direct measurement of desired variables.

B. Use of Digital Systems

The DCD Tier 2 Section 7.5.1.4 states that all alarm functions are implemented by digital systems. The IPS displays all AMI variables on the IFPD of the consoles in the MCR and RSR. The AMI protects against the potential for a software CCF because the IPS is configured by diverse hardware and software from the QIAS-P and QIAS-N. The Safety I&C System TeR, Appendix B addresses conformance to IEEE Std 7-4.3.2-2003. The use of digital systems for RPS and ESFAS is evaluated in Sections 7.1.4, and 7.3.4.3.8 of this SER. DCD Tier 2 Section 7.7.1, states that the HSI design for both safety-related systems and non-safety systems in the MCR and the RSR are subject to the HFE design processes described and is evaluated in Chapter 18 of this SER.

For digital computer-based systems, the applicant addressed the requirements described in IEEE Std 7-4.3.2-2003, which was endorsed in RG 1.152, Revision 3. The staff reviewed the information submitted by the applicant and concluded with reasonable assurance, that the information system important to safety adequately addresses the requirements for the use of digital systems.

The DCD Tier 2 Section 7.5.3, states that during and after plant accident conditions, the QIAS-N and QIAS-P provide all information required for achieving plant safe shutdown and performing EOPs even though the IPS is unavailable.

In RAI 294-8302, Question 07.05-5, the staff requested the applicant to provide a basis for EOP action points that accounts for measurement uncertainties. RG 1.105, Revision 3, provides acceptable guidance for establishing these uncertainties. In the July 13, 2015, response to this RAI (ML16195A530), the applicant specified that the instrument uncertainties for the EOP action points are determined by the COL applicant. COL Item 7.5(3) was added to DCD Tier 2 Table 1.8-2 in response to RAI 294-8302, Question 07.05-5. The Uncertainty Methodology TeR provides the methodology for calculating instrumentation uncertainties. Sections 4 and 5 of the Uncertainty Methodology TeR describe the environmental and/or seismic conditions and instrumentation effects, such as calibration uncertainties, loop errors, and drift, which are considered when performing uncertainty calculations. Based on the proposed addition of COL Item 7.5(3), the staff finds the proposed changes to the FSAR in RAI 294-8302, Question 07.05-5, are acceptable. The incorporation of the proposed markup into the next revision of the FSAR was a confirmatory item. The staff verified that the proposed

markups have been incorporated into Revision 1 of DCD Tier 2 Table 1.8-2. As such, this confirmatory item has been satisfied.

C. Monitoring of Severe Accidents

The DCD Tier 2 Table 19.2 3-4, lists the severe accident systems, instrumentation, and equipment to mitigate the effects of a severe accidents. Section 19.2.3.3.7 describes the equipment survivability qualification. Severe accident mitigation for the APR1400 design is evaluated in Section 19.2.3 of this SER.

D. Performance Assessment

The IEEE Std 497-2002, Clause 5.6, require that an assessment for each of the performance criteria shall be conducted and documented. The assessment performed is to assure that the as-designed performance meets or exceeds the performance criteria. DCD Tier 2 Section 7.5.2.1.e discusses the performance assessment. In RAI 294-8302, Question 07.05-4, the staff requested the applicant to provide the performance criteria assessment including the allowances for calibration uncertainties, loop errors, and drift (consistent with the methodology given in ISA Std 67.04-1994, Part 1) the magnitude and direction of errors imposed on the AMI by environmental and/or seismic conditions during and after the postulated event. In the July 13, 2015, response to this RAI (ML16195A530), the applicant committed to update DCD Tier 2, Sections 7.5.2.1, 7.5.4 and 7.5.5 and Table 1.8-2 that specifies that the plant-specific setpoint bases document for the EOPs provided by the COL applicant and provides the method for determining the setpoints applicable to the plant specific EOPs. The instrumentation uncertainties used in determining the EOP action points are derived from final design data conforming to RG 1.105, Revision 3. The final design data will be incorporated into the bases document during the plant construction stage. COL Item 7.5(3) requires that the COL applicant provide the bases document for the EOP action points. Based on the proposed addition of COL Item 7.5(3), the staff finds the proposed changes to the DCD in RAI 294-8302, Question 07.05-4, are acceptable. The incorporation of the proposed markup into the next revision of the FSAR was a confirmatory item. The staff verified that the proposed markups have been incorporated into Revision 1 of DCD Tier 2, Sections 7.5.2.1, 7.5.4, 7.5.5, and Table 1.8-2. As such, this confirmatory item has been satisfied.

7.5.4.1.3 Inadequate Core Cooling Monitoring Instrumentation

The ICC monitoring instrumentation is part of the MCR and is designed to meet the intent of the guidance identified in NUREG-0737, “Clarification of TMI Action Plan Requirements.” The ICC monitoring instrumentation and displays provide sufficient information to permit the operator to evaluate the potential for the core being uncovered by coolant, and gross breach of protective barriers including the resultant release of radioactivity to the environment. The ICC monitoring instrumentation provides an unambiguous, easy-to-interpret indication of ICC. The SPDS displays ICC variables as a primary display and the QIAS-P displays the ICC monitoring signals as backup.

The DCD Tier 2 Section 7.5.2.2, states that the ICC monitoring is designed to meet the requirements of 10 CFR 50.34(f)(2)(xviii) and the criteria in NUREG-0737, Item II.F.2.

7.5.4.1.4 Conclusions

The staff reviewed the information submitted by the applicant and concluded with reasonable assurance, that the applicant provided sufficient information in the APR1400 design certification application to demonstrate that the requirements of 10 CFR 50.34(f)(2)(v), (2)(xi), (2)(xii), (2)(xvii), (2)(xviii), (2)(xix), (2)(xx), (2)(xxiv), GDC 1, 2, 4, 13, 19, and 24, and IEEE Std 603-1991, Clauses 5.6.3 and 6.3 are met.

7.5.4.2 Bypassed and Inoperable Status Indication

The SRP Section 7.5 identifies the regulations as applicable to BISI.

The BISI is processed by the IPS and displayed on the LDP and IFPD. The BISI provides system-level indication of deliberately introduced inoperability of the protection system, which is required for safe operation of the plant. The system-level alarms are actuated when a component actuated by a protection system is bypassed or deliberately rendered inoperable.

The DCD Tier 2 Section 7.5.2.3, states that the BISI is designed to meet the requirements of 10 CFR 50.34(f)(2)(v) and RG 1.47, Revision 1. 10 CFR 50.34(f)(2)(v) is demonstrated by the indications of bypasses and inoperable status of the safety-related I&C system are available on the operator module, MTP, QIAS-N and the IPS displays. DCD Tier 2 Section 7.5.1.3, states that to conform with RG 1.47, Revision 1, the APR1400 design uses flags, at the system level to:

- Actuate alarms when a component actuated by a protection system is bypassed or deliberately rendered inoperable.
- Indicate bypassed or deliberately induced inoperability for auxiliary and support systems or indication that effectively bypasses or renders a protection system inoperable or the systems actuated or controlled by the protection system.
- Provide indication in the control room for each bypassed or deliberately induced inoperable status in a protection system.
- Ensure that the operator is able to activate each system-level bypass indicator manually in the control room.

Bypasses and inoperable status conditions are classified into the following groups.

a. Operating bypasses

   Operating bypasses are provided to permit orderly startup and shutdown of the plant and to allow low power testing. The operating bypass for the RPS is described in DCD Tier 2 Section 7.2.1.6, and the operating bypass for ESFAS is described in DCD Tier 2 Section 7.3.1.5 and are evaluated in Sections 7.1.4.23 and 7.1.4.24 of this SER.

b. Trip channel bypasses

   Trip channel bypasses are used to individually bypass channel trip inputs to the protection system logic for maintenance or testing. The trip logic is converted from a 2oo4 to a 2oo3 logic for the parameters being bypassed, while maintaining a

coincidence of two for actuation. The trip channel bypass for the RPS is described in DCD Tier 2 Section 7.2.1.6, and the trip channel bypass for ESFAS is described in Section 7.3.1.5 and evaluated in Sections 7.1.4.23 and 7.1.4.24 of this SER.

c. ESF components inoperable

The bypassed or inoperable condition of ESF components is communicated to the IPS, which indicates a system-level bypassed or inoperable condition. The IPS also provides status information at the component level. The operator has the ability to manually activate each RPS and ESF system-level bypass indication in the MCR. Inoperable indication is shown on the IPS displays and LDP.

There are no system-level bypasses for the RPS or ESFAS. DCD Tier 2 Section 7.5.1.3 also provides the list of the system-level status indication of BISI, which is provided for the protection systems and auxiliary or supporting systems and are required for safe operation of the plant. In addition, the BISI includes bypass and inoperable status of all interlock systems important to safety that are evaluated in Section 7.6 of this SER; thus, meeting the guidance of SRP BTPs 7-1 and 7-2. The APR1400 has no recirculation mode; therefore SRP BTP 7-6 is not applicable.

In RAI 38-7878, Question 07.05-3, the staff requested the applicant to clarify in the FSAR the classification of BISI, demonstrate how BISI conforms to RG 1.47, Revision 1, and to identify all signal paths in and out of BISI to safety-related and non-safety systems. In addition, describe how the trip logic is converted from a 2oo4 to a 2oo3 logic for the parameters being bypassed, while maintaining a coincidence of two for actuation. In the August 3, 2015, response to this RAI (ML15216A459), the applicant committed to update DCD Tier 2 Section 7.5.1.3, to reflect that the BISI is a non-safety system. The applicant provided additional information on how the APR1400 conforms to the guidance of RG 1.47, Revision 1, as follows:

<u>Positions 1 and 2</u>

BISI automatically indicates bypass or inoperability of safety-related systems and auxiliary or supporting systems in accordance with RG 1.47, Revision 1. BISI, at a system level, provides a continuous indication of the bypassed or inoperable status of safety-related systems and auxiliary or supporting systems on the LDP. The system level BISI page is also displayed on the IFPD. The operating bypass and trip channel bypass statuses are indicated at the MTP in the I&C equipment room and the operator module and IFPD in the MCR.

For inoperable indication, the switch of each component provides indication of inoperable status on the ESF-CCS ESCM for safety-related components and on the IFPD for non-safety components. The flashing inoperable indication goes to steady when inoperable pushbutton is operated and to off when the inoperable condition returns to normal.

The BISI, at a system level, has dedicated bypass switches. When a component is in maintenance, the operator manually sets the bypass switches to bypass mode. After maintenance is complete, the operator manually returns the bypass switches to normal status.

<u>Position 3</u>

The self-test and self-diagnostics of the digital computer-based I&C safety-related systems are described in DCD Tier 2, Sections 7.2.2.5 and 7.3.2.5. When the PPS and ESF-CCS are

undergoing testing or experiencing trouble, they are indicated on the IFPD. The self-test and self-diagnostics are evaluated in Sections 7.2 and 7.3 of this SER.

Position 4

The BISI is implemented in the IPS as a part of systems. The IPS contains several diagnostic tools available to determine the health of all servers and controllers on the DCN-I. The alarm server in the IPS allows for detecting and displaying abnormal conditions of system status as well as abnormal plant conditions on the IFPDs. The system status display shows detailed information about the status of the IPS servers. Therefore, the operator can acknowledge operable status of the BISI during normal operation.

Position 5

The BISI system receives the bypass and inoperable information from the ESF-CCS to provide the operator the following information to determine if continued reactor operation is permissible:

- ESF-CCS network failure by channel.
- QIAS-N network failure.
- Minimum inventory switch operability by channel.
- Status of each safety cabinet.
- Status of each ESF-CCS controller.
- Operability of each safety component.

This BISI information is continuously displayed on the LDP and IFPD during normal and abnormal operation conditions.

Position 6

The BISI system only receives the bypassed and inoperable information from the safety-related systems through unidirectional communication and fiber optic isolation. No results from the BISI system are sent to the safety-related system for control and monitoring purposes. Therefore, any failures or miss-operation of the BISI system cannot adversely affect the performance of safety functions.

Finally, the applicant described how the trip logic is converted from a 2oo4 to a 2oo3 logic for the parameters being bypassed, while maintaining a coincidence of two for actuation.

The staff reviewed the information submitted by the applicant and concluded with reasonable assurance that the proposed changes to the FSAR in the response to RAI 38-7878, Question 07.05-3, are in accordance with RG 1.47, Revision 1, and are therefore acceptable. The incorporation of the proposed markup into the next revision of the DCD was a confirmatory item. The staff verified that the proposed markups have been incorporated into Revision 1 of DCD Tier 2 Section 7.5.1.3. As such, this confirmatory item has been satisfied.

The staff reviewed the information submitted by the applicant and concluded with reasonable assurance, that the APR1400 BISI system adequately addresses the requirements of 10 CFR 50.34(f)(2)(v), GDC 1 and 24, and IEEE Std 603-1991, Clauses 5.6.3, 5.8.3, and 6.3.

7.5.4.3 Alarm Systems

The SRP Section 7.5 identifies applicable regulations for annunciator systems. GDC 13 requires, in part, that instrumentation be provided to monitor variables and systems over their anticipated ranges for normal operation, AOOs, and accident conditions as appropriate to assure adequate safety, including those variables and systems that can affect the fission process, integrity of the reactor core, reactor coolant pressure boundary, and containment and its associated systems. GDC 19 requires, in part, that a control room be provided from which actions can be taken to operate the nuclear power unit safely under normal conditions and to maintain it in a safe condition under accident conditions, including LOCAs. The staff used the guidance in SRP Appendix 7.1-A, SRP Section 7.5, and RG 1.97, Revision 4, to assess how the annunciator system design meets the requirements of GDC 13 and GDC 19.

The APR1400 design for the alarm system alerts the operators by means of visual and audible signals of abnormal conditions that require operator action and is designed to perform the following functions:

a) alerting the operators to off-normal conditions that require the operator to take action,

b) guiding the operators to the appropriate response, and

c) assisting the operators in determining and maintaining an awareness of the state of the plant and its systems or functions.

The DCD Tier 2 Section 7.5.1.4, describes the reliability, use of digital, and independence of the alarm system. For reliability, the alarm system is implemented in both the IPS and QIAS-N. Alarms that are used for all operating modes including normal, AOOs, and PAs are provided in redundant operator workstation consoles by the IPS. The IPS has redundant alarm servers.

The IPS is configured by diverse hardware and software from the QIAS-N. The IPS performs online diagnostics for continuous self-health monitoring. The QIAS-N also includes automatic online diagnostics. The QIAS-N hardware is seismically and environmentally qualified. The QIAS-N is implemented as important-to-availability software. All alarm functions are implemented by digital systems. For independence, the IPS is isolated from the QIAS-N by qualified isolation devices. The QIAS-N is powered from Class 1E, and the IPS is powered from non-Class 1E. The communication independence between the IPS and the QIAS-N is described in Section 7.9.4.6.1 of this SER.

The DCD Tier 2 Section 7.5.2.4, states that the alarm system is designed to meet the positions of the SRM to SECY-93-087, Item II.T and is further evaluated in Section 7.5.4.1 above. Additionally, the Safety I&C System TeR, Section 3.3.2, states that the alarm systems are designed to meet the requirements of the SRM to SECY 93-087, Item II.T, and are implemented in both the IPS and QIAS-N. This is demonstrated by multi-division information displayed by the QIAS-N is independently processed and displayed by the IPS. The QIAS-N receives the processed information from each division of four ITPs and alarms any discrepancies from its own corresponding multi-division information calculators.

The DCD Tier 2 Section 7.1.1.5.d, states that the alarm systems are redundantly implemented by the IPS and QIAS-N. The IPS and QIAS-N are independent and diverse from each other. The IPS receives alarm signals through fiber optic data link using unidirectional Ethernet via MTP from the PPS and ESF-CCS. The QIAS-N also receives alarm signals through unidirectional SDL via each division of ITP from the PPS and ESF-CCS. Therefore, the alarm functions by the IPS and QIAS-N would not impact the safety-related systems such as the PPS or ESF-CCS as well as the performance of the QIAS-N functions and any single alarm system failure will not cause a total loss of the plant's alarm system.

The Safety I&C System TeR, Section 3.2.h, states that the MCR safety console is equipped with hardwired minimum inventory switches including manual reactor trip switches and manual ESF system-level actuation switches, and operator modules shared by the PPS, CPCS, and ESF-CCS. The MCR also has operator consoles and LDP. Monitoring for safe operation is implemented with the QIAS-P, QIAS-N and IPS displays. Also, the DPS, DIS, and DMA switches are provided as protection against CCFs in the safety-related I&C system coincident with DBEs.

Based on the provision of reliable digital non-safety alarm systems (i.e. IPS and QIAS-N) that is independent from safety systems and additional safety-related alarms on the QIAS-P, the staff concludes with reasonable assurance, that the annunciator systems adequately address the requirements of 10 CFR Part 50, Appendix A, GDC 1, 13, 19, and 24, and IEEE Std 603-1991, Clauses 5.6.3 and 6.3.

7.5.4.4 Emergency Response Information

The SRP Section 7.5 identifies applicable regulations for the SPDS and for information system associated with the ERDS; GDC 1 and 24.

The DCD Tier 2 Section 7.5.1.5, states that the SPADES+ provides the information for monitoring the critical safety parameters and DCD Tier 2 Section 7.5.1.6, states that the ERF includes the MCR, TSC, operational support center, and the EOF. In addition, the ERF includes the SPDS and ERDS. The IPS associated with the ERF provides important safety information to support emergency response decision making. The ERDS transmits reactor process variables and radiological data as well as site meteorological data of the plant to the NRC.

The DCD Tier 2 Section 18.7.1, indicates that the same HSI methods evaluated in Section 18.7.1 of this SER apply to the SPDS indications provided in the MCR and the TSC.

The DCD Tier 2 Section 7.1.1.5, Items e and f, indicates that the SPDS, ERDS and TSC are designed and implemented in accordance with NUREG-0696, "Functional Criteria for Emergency Response Facility," and NUREG-0737. DCD Tier 2 Section 7.7.1.4, states that the IPS is a non-safety system that performs non-safety functions, and is not required to operate during or after a seismic event. However, the IPS is seismically qualified for structural integrity so that no control room missile hazards result as a consequence of a seismic event. The SPADES+ program is implemented in the IPS. SPADES+ is designed to meet the criteria for the SPDS.

The DCD Tier 2 Section 7.7.1.2, states that the IPS provides the necessary interfaces with the TSC, EOF, and ERDS to make the same information that is available to the operating staff available to other interested personnel. The TSC, operational support center, EOF, and ERDS, which are associated with emergency planning, are evaluated in Section 13.3 of this SER.

Based on the staff's conclusions in Chapter 18 and Section 13.3 of this SER regarding SPDS and ERDS as well as the provision of a seismically qualified IPS to provide information to support emergency response decision making, the staff concludes with reasonable assurance, that the SPDS and the information system (e.g. IPS) associated with the ERDS adequately address the requirements of 10 CFR Part 50, Appendix A, GDC 1 and 24, and IEEE Std 603-1991, Clauses 5.6.3 and 6.3.

7.5.4.5 ITAAC

The evaluation of ITAAC is in Section 14.3.5 of this SER.

7.5.5 Combined License Information Items

Three COL information items are included in DCD Tier 2 Table 1.8-2, for information systems important for safety, and these are sufficient and no others are needed.

Table 7.5-2 Combined License Information Items Identified in the DCD

Item No.	Description	Section
7.5(1)	The COL applicant is to provide a description of the site-specific AMI variables such as wind speed, and atmosphere stability temperature difference.	7.5
7.5(2)	The COL applicant is to provide a description of the site-specific EOF.	7.5
7.5(3)	The COL applicant is to provide the bases document accounting for measurement uncertainties for the EOP action points.	7.5

7.5.6 Findings and Conclusions

The staff reviewed the information submitted by the applicant and concluded with reasonable assurance, that the APR1400 information systems important to safety design meet the relevant requirements of 10 CFR 50.34(f), 10 CFR 50.55a(h)(3), and 10 CFR Part 50, Appendix A, GDC.

7.6 Interlock Systems Important to Safety

7.6.1 Introduction

The interlock functions important to safety reduce the probability of occurrence of specific events or maintain safety-related systems in a state that provides reasonable assurance of their availability. These interlock functions include:

- Interlock to prevent over-pressurization of low-pressure systems (e.g., residual heat removal) when these systems are connected to high-pressure systems (e.g., primary coolant).

- Interlocks to prevent over-pressurization of the primary coolant system during low-temperature operation of the reactor vessel.

- Valve interlocks to assure the availability of emergency core cooling system (ECCS) accumulators.

- Interlocks to isolate safety-related systems from non-safety systems (e.g., seismic and non-seismic portions of auxiliary supporting systems), and interlocks to preclude inadvertent inter-ties between redundant safety or diverse systems where such inter-ties exist for the purposes of testing or maintenance.

7.6.2 Summary of Application

DCD Tier 1: The Tier 1 information associated with this section is found in DCD Tier 1 Section 2.4.3, "Safety Injection System"; Section 2.4.4, "Shutdown Cooling System"; Section 2.5.4, "Engineered Safety Features – Component Control Systems"; and Section 2.7.2.2, "Component Cooling Water System."

DCD Tier 2: The applicant has provided a system description in DCD Tier 2 Section 7.6, "Interlock Systems Important to Safety," summarized here in part, as follows:

The interlock systems important to safety that are credited in the safety analysis to:

a. Prevent over-pressurization of low-pressure systems.

<u>Shutdown Cooling System Suction Line Isolation Valve Interlocks</u>

The SCS is a low-temperature and low-pressure system used to remove decay heat from the RCS. An interlock associated with the SCS suction line isolation valves prevents the isolation valves from being opened at RCS pressures above 450 psia. The interlock provide reasonable assurance that the pressure at the valves does not exceed the low temperature over-pressurization protection (LTOP) valve setpoint when the SCS is aligned to the RCS for normal shutdown cooling.

b. Prevent over-pressurization of the RCS during low-temperature operations of the reactor vessel.

<u>Shutdown Cooling System Suction Line Relief Valve Interlocks</u>

Over-pressure protection of the RCS during low temperature conditions is provided by the relief valves located in the SCS suction lines. One relief valve is installed in each SCS suction line to provide LTOP for the RCS when the SCS is aligned to the RCS to provide decay heat removal during plant shutdown and startup operations. Because the LTOP relief valve setpoint pressure is much lower than the design pressure of the SCS, these valves also provide over-pressure protection of the SCS.

c. Provide reasonable assurance of the availability of safety injection tank (SIT) isolation valves.

SIT Isolation Valve Interlocks

The SIS is designed to inject borated water into the RCS upon receipt of the SIAS and to provide RCS cooling in conjunction with other systems following an accident. The SIT permissive interlocks are used to allow isolation of the SITs below the pressure required for mitigation following a LOCA.

d. Provide reasonable assurance of the availability of component cooling water (CCW) supply and return header tie line isolation.

Component Cooling Water Non-essential Supply and Return Header Isolation Valve Interlocks

The CCW system removes heat from all safety components required for normal power plant operation, and normal and emergency shutdown of the plant, and transfers the heat to the essential service water through the CCW heat exchangers. The CCW system also provides cooling water for some non-safety components required for plant operation.

Non-essential supply and return header isolation valves are provided to isolate the non-essential supply and return headers from the essential supply and return headers in the event of an accident. These valves are two in series electric motor operated valves and can be remotely operated. These valves are automatically closed on an SIAS or low-low CCW surge tank level signal. The valve closure times are set to prevent complete loss of surge tank volume due to a break in the non-safety piping. These safety-related valves can be manually opened and closed from the MCR.

e. Provide reasonable assurance of the independence of each safety mechanical divisions of the CCW system.

CCW Cross Connection Line Isolation Valve Interlocks

The CCW system consists of two independent and redundant closed loop safety divisions. There are two cross connection lines between the two separate divisions, and each cross connection line has two in series motor-operated isolation valves.

f. Provide reasonable assurance of the availability of interlocks for both shutdown cooling pumps and containment spray pumps.

Interlocks for Both Shutdown Cooling Pumps and Containment Spray Pumps

The containment spray primary function is achieved by two redundant and independent containment spray pumps (CSPs) of divisions C and D. Each CSP has 100 percent capability for the containment spray function. The shutdown cooling pumps are designed as backups to the CSPs with 100 percent capability of the containment spray function if the CSPs are not available.

Bypassed and inoperable status of all interlocks is provided via the BISI, as described and evaluated in Section 7.5 of this SER.

The interlocks important to safety are implemented in the ESF-CCS group controller and loop controller. The ESF-CCS loop controller interfaces with controlled plant components and reflects the result of combining the interlock control signals.

ITAAC: The evaluation of ITAAC is in Section 14.3.5 of this SER.

Technical Specifications: The Technical Specifications associated with DCD Tier 2 Section 7.6, are given in DCD Tier 2 Chapter 16, Sections 3.4.11, 3.4.13, 3.5.1, 3.7.7 and Sections B 3.4.11, B 3.4.13, B 3.5.1, B 3.7.7. The evaluation of the Technical Specifications associated with Interlock Systems Important to Safety is discussed in Chapter 16 of this SER.

Technical Reports: none

7.6.3 Regulatory Basis

The relevant requirements of the NRC regulations for this area of review, and the associated acceptance criteria, are given in SRP Section 7.6, "Interlock Systems Important to Safety," and are summarized below. Review interfaces with other SRP sections also can be found in SRP Section 7.6.

1. 10 CFR 50.55a(h)(3), "Safety Systems," states that IEEE Std 603-1991, including the correction sheet dated January 30, 1995, is approved for incorporation by reference. For interlock systems that are not safety-related systems as defined by IEEE Std 603-1991 and isolated from the safety-related systems, the applicable requirements of 10 CFR 50.55a(h)(3) are IEEE Std 603-1991, Clause 5.6.3, and IEEE Std 603-1991, Clause 6.3.

2. GDC 1, 2, 4, 13, 19, and 24.

3. 10 CFR 50.34(f)(2)(v), "Additional TMI-Related Requirements, Bypass and Inoperable Status Indication," or equivalent TMI action requirements imposed by Generic Letters.

4. 10 CFR 52.47(b)(1), which requires that a design certification application contain the proposed ITAAC that are necessary and sufficient to provide reasonable assurance that, if the inspections, tests, and analyses are performed and the acceptance criteria met, a plant that incorporates the design certification is built and will operate in accordance with the design certification, the provisions of the Atomic Energy Act, and the NRC's regulations.

Additional requirements applicable to safety-related systems with which interlock systems may interact are provided below. These criteria are used as guidelines, when applicable, in establishing the functions important to safety performed by interlock systems:

1. GDC 10, 15, 16, 25, 28, 33, 34, 35, 38, 41, and 44.

Acceptance criteria adequate to meet the above requirements include:

1. Specific acceptance criteria acceptable to meet the relevant requirements of the NRC regulations identified above are included in SRP Sections 7.1 and 7.6, Table 7-1, Appendix 7.1-A, which list standards, RGs, and SRP BTPs. SRP BTPs 5-2, 7-1, and 7-2 are specifically applicable to interlocks important to safety.

2. SRP Appendix 7.1-C provides acceptance criteria for safety-related system compliance with 10 CFR 50.55a(h)(3).

3. SRP Appendix 7.1-D provides acceptance criteria for the digital I&C compliance with Institute of IEEE Std 7-4.3.2- 2003, as endorsed by RG 1.152, Revision 3.

4. SRP Section 14.3.5 provides the guidance on the ITAAC related to I&C systems.

The SRP Table 7-1, Section 3 (SRMs), Section 4 (RGs), and Section 5 (RGs), lists the SRP acceptance criteria applicable to interlock systems important to safety.

7.6.4 Technical Evaluation

The objective of the staff's review is to confirm that the interlock systems important to safety satisfy NRC regulations through a set of acceptance criteria and that they can perform their safety functions for all plant conditions.

The SRP Section 7.6, lists the following major design considerations that should be emphasized for the review of interlock systems important to safety:

- Single failure criterion,
- Quality of components and modules,
- Independence,
- System testing and inoperable surveillance,
- Use of digital systems,
- Interlocks to prevent over-pressurization of low-pressure systems,
- Interlocks to prevent over-pressurization of the primary coolant during low-temperature operations of the reactor vessel,
- Interlocks for ECCS accumulator valves,
- Interlocks required to isolate safety-related systems from non-safety systems, and
- Interlocks required to preclude inadvertent inter-ties between redundant safety-related or diverse systems.

Several of these design considerations are addressed in other sections of this SER, as indicated in Table 7.6-1 below. The remaining major design considerations are discussed below. Additionally, the SRP lists other requirements applicable to interlock systems, including I&C available to operators, control room design, and bypass and inoperable status indication, which are addressed below.

Table 7.6-1: References to Other Sections of the Report

Design Consideration	Report Section(s)
10 CFR 50.55a(h)(3)	7.1.4.4
10 CFR 52.47(b)(1)	14.3.5
GDC 1	7.1.4.3, 7.1.4.7
Single Failure	7.1.4.5, 7.2.4.3, 7.3.4.3.2
Independence & GDC 24	7.1.4.10, 7.9.4.6
Capability for Test and Calibration	7.1.4.11
GDC 2 and 4	7.1.4.8, 3.10, 3.11
GDC 10	7.1.4
GDC 13 and 19	7.1.4, 7.1.4.1, 7.5.4.1.2, 7.9.4.3.4, 7.9.4.7, Chapter 18
GDC 15	5.2.2.1
GDC 16	6.2.1.1, 6.2.4
GDC 25	7.2.6
GDC 28 and 33	9.3.4
GDC 34	7.1.4, 7.3.4.3.10, 7.4.4.2, 8.3.1
GDC 35	6.2.2, 7.1.4, 7.3.4.3.10, 7.4.4.2.4, 8.3.1
GDC 38	6.2.1.1, 6.2.2, 7.1.4, 7.3.4.3.10, 7.4.4.2, 8.3.1
GDC 41	6.2.5, 6.5.2, 7.1.4, 7.3.4.3.10, 8.3.1
GDC 44	7.1.4, 8.3.1
Technical Specifications	Chapter 16
Use of Digital Systems	7.3.4.3.8, 7.7.4.15, Chapter18

7.6.4.1 Single Failure Criterion

The staff used the guidance found in SRP Section 7.6 and SRP Appendix 7.1-C to determine how the APR1400 design meets IEEE Std 603-1991, Clause 5.1.

The DCD Tier 2 Sections 7.6.1.1 through 7.6.1.6 provide a functional description of how the interlock systems important to safety adequately address the single failure criterion.

<u>Shutdown Cooling System Suction Line Isolation Valve Interlocks</u>

Each SCS suction line has independent, redundant motor-operated isolation valves to prevent over-pressurization and provide isolation between the RCS and the SCS. The interlocks do not prevent achieving cold shutdown from the MCR after a single failure. No single failure can prevent the operator from aligning the valves, on at least one suction line, for shutdown cooling

after the RCS pressure requirements are satisfied. In addition, no single failure can result in a suction line being spuriously opened.

Shutdown Cooling System Suction Line Relief Valve Interlocks

One relief valve is installed in each SCS suction line to provide LTOP for the RCS when the SCS is aligned to the RCS to provide decay heat removal during plant shutdown and startup operations. No single failure of an isolation valve or its associated interlock prevents one relief valve from performing its intended function.

SIT Isolation Valve Interlocks

During normal operation, each tank has a motor-operated isolation valve that is normally open with power removed from its motor circuit to eliminate the possibility of spurious isolation. Physically separate and independent signals are provided for SIT isolation valve interlocks.

Component Cooling Water Non-essential Supply and Return Header Isolation Valve Interlocks

Non-essential supply and return header isolation valves are provided to isolate the non-essential supply and return headers from the essential supply and return headers in the event of an accident. These valves are two in series electric motor operated valves that automatically close on a SIAS control signal from different divisions as depicted in Table 9.2.2-6 of DCD Tier 2 Chapter 9. In addition, they can be remotely operated. A single interlock failure may result in valve malfunction within a single division, but this does not adversely affect the other division.

CCW Cross Connection Line Isolation Valve Interlocks

Two cross connection lines between the two separate divisions of CCW, and each cross connection line has two in series motor-operated isolation valves powered from different divisions. The valves are normally locked closed and automatically close on a SIAS or low-low CCW surge tank level signal in the event of an accident or transient.

Interlocks for Both Shutdown Cooling Pumps and Containment Spray Pumps

Single failure for the containment spray primary function is achieved by two redundant and independent 100 percent capacity CSPs of divisions C and D. Each CSP is backups by two redundant and independent 100 percent capacity shutdown coolant pump (SCP)s of divisions A and B, such that no single failure prevents the containment spray function if one division is unavailable.

The staff reviewed the information submitted by the applicant and concluded with reasonable assurance, that by using independent and redundant design methods, the interlock systems important to safety adequately address the requirements of IEEE Std 603-1991, Clause 5.1.

7.6.4.2 Quality of Components and Modules

The DCD Tier 2 Section 7.6.2.1.c, states that the important-to-safety interlock systems discussed in Sections 7.6.1.1 through 7.6.1.6 are designed in accordance with GDC 1 and in conformance with IEEE Std 603-1991, Clause 5.3. IEEE Std 603-1991, Clause 5.3 is evaluated in Sections 7.1.4.3 and 7.1.4.7 of this SER. GDC 1, 2, and 4 are evaluated in Sections 7.1.4.3, 7.1.4.7, 7.1.4.8, 3.10, and 3.11 of this SER.

The staff reviewed the information submitted by the applicant and concluded with reasonable assurance that the interlock systems important to safety meets the requirements of IEEE Std 603-1991, Clause 5.3, because the interlocks important to safety will be Class 1E qualified to operate in the anticipated worst environment.

7.6.4.3 Independence

The DCD Tier 2, Sections 7.6.1.1 through 7.6.1.6 provide a functional description of how the interlock systems important to safety adequately address independence.

Shutdown Cooling System Suction Line Isolation Valve Interlocks

Each SCS suction line has independent, redundant motor-operated isolation valves to prevent over-pressurization and provide isolation between the RCS and the SCS. The RCS pressure signals used for these interlocks are provided by physically independent pressurizer pressure safety channels.

Shutdown Cooling System Suction Line Relief Valve Interlocks

One relief valve is installed in each SCS suction line to provide LTOP for the RCS when the SCS is aligned to the RCS to provide decay heat removal during plant shutdown and startup operations. The SCS suction line relief valve is a self-actuating spring-loaded liquid relief valve, and control circuitry is not required. The valve opens when the RCS pressure exceeds its setpoint.

SIT Isolation Valve Interlocks

During normal operation, each tank has a motor-operated isolation valve that is normally open with power removed from its motor circuit to eliminate the possibility of spurious isolation. Physically separate and independent signals are provided for SIT isolation valve interlocks.

Component Cooling Water Supply and Return Header Tie Line Isolation Interlocks

Non-essential supply and return header isolation valves are provided to isolate the non-essential supply and return headers from the essential supply and return headers in the event of an accident. These valves are two in series electric motor operated valves and can be remotely operated. These interlocks provide reasonable assurance of the independence between essential supply and return headers, and non-essential supply and return headers.

CCW Cross Connection Line Isolation Valve Interlocks

The interlocks provide reasonable assurance of the independence of each safety mechanical division of the CCW system, thereby providing cooling water to safety components required for mitigating an event. The CCW system consists of two independent and redundant closed loop safety divisions. There are two cross connection lines between the two separate divisions, and each cross connection line has two in series motor-operated isolation valves.

Interlocks for Both Shutdown Cooling Pumps and Containment Spray Pumps

Two redundant and independent 100 percent capacity CSPs of Divisions C and D. Each CSP is backups by two redundant and independent 100 percent capacity SCPs of Divisions A and B. For communication between safety divisions, the data flow between redundant PPS divisions is

buffered at the outgoing side of the communication processor of the bistable processor and at the incoming side of the communication processor of the LCL processor to ensure independence of the redundant safety divisions. One way communication over fiber optic cable is used to ensure communication independence and electrical isolation between redundant portions of the safety-related system. The communication independence is evaluated in Section 7.9.4.6 of this SER.

The application of GDC 24 to interlock systems important to safety is evaluated in Sections 7.1.4.10 and 9.6.4.6 of this SER. Note in Section 7.1.4.10 this evaluation is performed for all interfaces between safety and non-safety systems and between redundant portions of safety systems.

The staff reviewed the information submitted by the applicant and concluded with reasonable assurance that the interlock systems important to safety meet the requirements of IEEE Std 603-1991, Clauses 5.6 and 6.3 and GDC 24 because physical, electrical and communication independence will be provided between (1) redundant divisions, and (2) safety-related and non-safety portions of interlock systems important to safety.

7.6.4.4 Capability for Testing and Calibration

Clause 5.7 of IEEE Std 603-1991, requires capability for test and calibration of safety-related system equipment, while retaining capability of the safety-related systems to accomplish their safety functions. Clause 5.8 requires information displays for manually controlled actions, system status indication, indication of bypasses, and accessibility to the operator. Clause 6.5 requires capability for test and calibration of sense and command equipment. 10 CFR 50.34(f)(2)(v) requires an automatic indication of the bypassed and inoperable status of safety-related systems. For review of how the APR1400 design meets Clauses 5.7, 5.8, 6.5, and 10 CFR 50.34(f)(2)(v), the staff used the guidance found in SRP Section 7.6 and SRP Appendix 7.1-C.

The DCD Tier 2, Sections 7.6.2.2.g, states that complete testing capability of the SCS isolation valve interlocks, SIT isolation valve interlocks, CCW non-essential supply and return header isolation valves interlocks, CCW cross connection line isolation valve interlocks, and interlocks for both CSP and SCP exist. The tests, using the built-in ESF-CCS test logic, include testing of the interlock logic, valve control circuits, and actuation of the individual valves. This testability is equivalent to the testability required for ESF circuits.

Additionally, DCD Tier 2, Section 7.6.2.2.t states that the removal of one division for testing does not degrade system reliability. Failure of one of the remaining divisions during a test outage does not generate an unacceptable situation because the valve position indication monitoring, with alarms and administrative controls, effectively precludes inadvertent opening or closing of the valves by the operator.

Safety-related I&C systems are designed to provide bypass and inoperable status information to the operator. Sufficient indications are provided to the operator to evaluate the status of each interlock as described in DCD Tier 2 Section 7.6.2.2.h.

Finally, DCD Tier 2, Sections 7.6.2.3 states that the Inservice Testing Program for MOVs, safety, and relief valves of the interlocks important to safety are described in DCD Tier 2, Sections 3.9.6.2, 3.9.6.3.1, and 3.9.6.3.6.

The staff finds the interlock systems important to safety adequately address the requirements of IEEE Std 603-1991, Clauses 5.7 and 6.5, by having periodic manual testing while maintaining interlock functions and having automatic self-testing performed both at power and during outages. The safety-related I&C systems provide bypass and inoperable status information, as well as indications to evaluate the status of each interlock, thus satisfying IEEE Std 603-1991, Clause 5.8, and 10 CFR 50.34(f)(2)(v). Additional review of BISI is discussed in Section 7.5.4.2 of this SER.

7.6.4.5 Use of Digital Systems

The DCD Tier 2 Section 7.6.2.4 states the interlocks important to safety are implemented in the ESF-CCS group controller and loop controller. The Safety I&C System TeR, Appendix B addresses conformance to IEEE Std 7-4.3.2. The use of digital systems for RPS and ESFAS is evaluated in Sections 7.1.4, 7.3.4.3.8, and 7.7.4.15 of this SER. DCD Tier 2 Section 7.7.1, states that the his design for both safety-related systems and non-safety systems in the MCR and the RSR are subject to the HFE design processes described and evaluated in Section 18 of this SER.

For digital computer-based systems, the applicant addressed the requirements described in IEEE Std 7-4.3.2-2003, which was endorsed in RG 1.152, Revision 3. The staff reviewed the information submitted by the applicant and concluded with reasonable assurance, that because the design conforms to the guidance in RG 1.152, Revision 3, the interlock systems important to safety satisfy the requirements for the use of digital systems.

7.6.4.6 I&C and Control Rooms

The 10 CFR Part 50, Appendix A, GDC 13, requires that instrumentation be provided to monitor variables and systems over their anticipated ranges for normal operation, for AOOs, and for accident conditions as appropriate to assure adequate safety, including those variables and systems that can affect the fission process, the integrity of the reactor core, the reactor coolant pressure boundary, and the containment and its associated systems. GDC 19 requires, in part, that a control room be provided from which actions can be taken to operate the nuclear power unit safely under normal conditions and to maintain it in a safe condition under accident conditions, including LOCAs. For the review of how the APR1400 design meets GDC 13 and 19, the staff used the guidance found in SRP Appendix 7.1 A and SRP Section 7.6.

The applicant states that the interlock systems important to safety are designed to conform with GDC 13, as described in DCD Tier 2, Sections 7.6.1.1, 7.6.1.3, 7.6.1.4, 7.6.1.5, and 7.6.1.6, and maintain interlock variables within safe states by observing the setpoint conditions as depicted in Figures 7.6-1A through 7.6-4 and as shown in Tables 7.6-1 and 7.6-2. The applicant stated that except SCS suction line relief valve interlock in the MCR, I&C systems for the all interlock systems important to safety are designed in conformance with GDC 19 to be maintained in a safe condition under accident conditions.

The SCS suction line relief valves are not required to comply with 10 CFR 50.34(f)(2)(xi) because the requirement for position indication has been applied only to safety relief valves directly connected to the RCS. The SCS suction line relief valves are located in the SCS line and normally isolated from the RCS.

The interlocks support actions to operate the nuclear power plant safely under normal conditions and maintain it in a safe condition under accident conditions. In RAI 46-7879,

Question 07.06-1, the staff requested the applicant to clarify in the FSAR what signals go through the MCR/RSR Master Transfer Switches. DCD Tier 2, Figures 7.6-1A, B, C and 7.6-2, show control from both MCR and RSR, but do not reflect the signals going through the MCR/RSR Master Transfer Switches described in DCD Tier 2 Section 7.7.1.2. DCD Tier 2, Figure 7.6-3, does not show any control from RSR, but the status of valves goes to both MCR and RSR. DCD Tier 2 Section 7.6.2.1.k states, "Instrumentation and control systems for the all interlock systems important to safety except SCS suction line relief valve interlock in the MCR are designed in conformance with GDC 19 to be maintained in a safe condition under accident conditions (see Figures 7.6-1A through 7.6-3)." In the August 11, 2015, response to this RAI (ML15223B175), the applicant clarified that DCD Tier 2, Figures 7.6-1A, B, C, 7.6-2, and 7.6-3 functionally show how the interlocks are combined and that the transfer of control between the MCR and the RSR is implemented and controlled as per the typical interface diagrams of the MCR/RSR master transfer switch provided in Figures 7.4-1 and 7.4-3. Additionally, DCD Tier 2 Section 7.6.2.4, states that the interlocks important to safety are implemented in the ESF-CCS group controller and loop controller. The ESF-CCS loop controller interfaces with controlled plant components and reflects the result of combining the interlock control signals.

The staff reviewed the information submitted by the applicant and concluded with reasonable assurance, that the RSR design adequately addresses the design requirement that equipment at appropriate locations outside the control room be provided and should be capable of operating independently of (i.e., without interaction with) the equipment in the MCR, as specified in GDC 19. Therefore, RAI 46-7879, Question 07.06-1, is closed.

Based on the applicant's commitment to maintain interlock variables within safe states by observing the setpoint conditions, the staff concludes with reasonable assurance, that the interlock systems important to safety meet the requirements of GDC 13 and GDC 19.

7.6.4.7 Reactor Coolant System Valve Interlocks

The regulations in 10 CFR Part 50, Appendix A, GDC 10 require, in part, that the reactor core and associated coolant, control, and protection systems shall be designed with appropriate margin to assure that specified fuel design limits are not exceeded during any condition of normal operation, including the effects of AOOs. To meet this requirement, DCD Tier 2, Sections 7.6.1.1 through 7.6.1.5 and Table 7.6-2 describe how the interlock systems important to safety contribute to reactor design margin by providing conservatism in the setpoints and fault-tolerant features.

The regulations in 10 CFR Part 50, Appendix A, GDC 15 require, in part, that the RCS be designed with sufficient margin to assure that the design conditions of the RCS pressure boundary are not exceeded. SRP BTP 7-1 provides guidance on the isolation of low-pressure systems from the high pressure RCS. SRP BTP 7-1 states, in part, that the interfaces between low-pressure and high-pressure RCS should have the following features:

- At least two valves in series to isolate any subsystem whenever the primary system pressure is above the pressure rating of the subsystem.
- Systems where both valves are motor-operated; the valves should have independent and diverse interlocks to prevent both from opening unless the primary system pressure is below the subsystem pressure. Also, valve operators should receive a signal to close automatically whenever the primary system pressure exceeds the subsystem design pressure.

- Suitable valve position indication should be provided in the control room.

The SRP BTP 5-2 states, in part, that the system should be designed and installed to prevent exceeding the applicable technical specifications and 10 CFR Part 50, Appendix G, “Fracture Toughness Requirements,” limits while operating at low temperatures. The system should be capable of relieving pressure during all anticipated over-pressurization events at a rate sufficient to satisfy the technical specification limits, particularly while the RCS is in a water solid condition. LTOP should be operable during startup and shutdown conditions below the Appendix G limit temperature.

To meet this guidance, DCD Tier 2, Sections 5.2.2.1.1, 5.2.2.1.2, 7.6.1.1, and 7.6.1.2 provide a functional description of how the interlock systems important to safety adequately address 10 CFR Part 50, Appendix A, GDC 15, SRP BTP 5-2, and SRP BTP 7-1.

Shutdown Cooling System Suction Line Isolation Valve Interlocks

Each SCS suction line has three independent, redundant motor-operated isolation valves to prevent over-pressurization and provide isolation between the RCS and the SCS; two on the high side and one on the low side of the system interface. An interlock associated with the SCS suction line isolation valves prevents the isolation valves from being opened at RCS pressures above 450 psia. The interlock setpoint is calculated considering tolerances necessary to provide reasonable assurance that the pressure at the valves does not exceed the LTOP valve setpoint when the SCS is aligned to the RCS for normal shutdown cooling. DCD Tier 1 Table 2.4.4-2, shows that controls and indication for the MOVs are located in both the MCR and the RSR.

Shutdown Cooling System Suction Line Relief Valve Interlocks

One relief valve is installed in each SCS suction line to provide LTOP for the RCS when the SCS is aligned to the RCS to provide decay heat removal during plant shutdown and startup operations. The SCS suction line relief valve is a self-actuating spring-loaded liquid relief valve, and control circuitry is not required. The valve opens when the RCS pressure exceeds its setpoint.

The SRP BTP 7-2 states, in part, that the following features should be incorporated into the design of MOVs for SITs:

- Automatic opening of the valves when either primary coolant system pressure exceeds a preselected value, or an safety injection signal is present.
- Visual indication in the control room of the open or closed status of the valve.
- BISI.
- Utilization of the SI signal to remove automatically any bypass feature that may allow an isolation valve to be closed.

To address this guidance, DCD Tier 2 Section 7.6.1.3 provide a functional description of how the interlock systems important to safety adequately address SRP BTP 7-2.

SIT Isolation Valve Interlocks

Each accumulator is connected to the RCS through two check valves and a motor operated isolation valve in series. During normal operation, each tank has a motor-operated isolation valve that is normally open with power removed from its motor circuit to eliminate the possibility of spurious isolation. As the RCS pressure is reduced during plant shutdown, the low pressurizer pressure trip setpoint is reduced to avoid inadvertent initiation of safety injection, the SITs are depressurized to a value below the SCS entry pressure, and the isolation valves are closed. The SIT permissive interlocks are used to allow isolation of the SITs below the pressure required for mitigation following a LOCA. The isolation valves are manually closed when RCS pressure drops below the setpoint so that the SITs cannot cause over-pressurization of the SCS while the SITs are maintained above atmospheric pressure. As RCS pressure increases, the valves automatically reopen at the set pressure. If the isolation valves are closed and an SIAS is initiated, the isolation valves automatically open. The SIAS overrides the interlock or any manual signal. DCD Tier 1 Table 2.4.3-2, shows that controls and indication for the SIT discharge valves are located in both the MCR and the RSR.

The DCD Tier 2 Section 7.6.1, states that the bypassed and inoperable status of all interlocks is provided via the BISI, and is evaluated in Section 7.5.4.2 of this SER. Based on these design commitments, the staff finds that the APR1400 design addresses the guidance of SRP BTP 7-2.

The SRP Section 7.6, major design consideration Item I, indicates that interlocks are required to isolate safety-related systems from non-safety systems.

Component Cooling Water Supply and Return Header Tie Line Isolation Interlocks

Non-essential supply and return header isolation valves are provided to isolate the non-essential supply and return headers from the essential supply and return headers in the event of an accident. These valves are two series electric motor operated valves and can be remotely operated. These valves are automatically closed on an SIAS or low-low CCW surge tank level signal. The valve closure times are set to prevent complete loss of surge tank volume due to a break in the non-safety piping. DCD Tier 1 Table 2.7.2.2-2, shows that controls and indication for the CCW supply and return valves are located in both the MCR and the RSR.

CCW Cross Connection Line Isolation Valve Interlocks

DCD Tier 2 Section 7.6.1.5 states that there are no connections between the CCW safety divisions and therefore does not include any interlocks. However, this statement conflicts with DCD Tier 2, Sections 9.2.2.2.2.4 (second paragraph) and 9.2.2.2.2.4.c, Figure 9.2.2, “Component Cooling Water System Flow Diagram,” DCD Tier 1 Section 2.7.2.2, “Design Description,” Table 2.7.2.2-2, “Component Cooling Water System Components List,” and Figure 2.7.2.2, “Component Cooling Water System,” which reflect cross connection supply and return values (CC-937, 938, 939, and 940) connecting the two CCW divisions and that these two valves in series automatically close on a SIAS control signal from different divisions. In RAI 521-8696, Question 07.06-3, the staff requested the applicant to clarify and update DCD Tier 1 and 2, to reflect whether there are cross-connections between the two divisions of CCW. If there are cross-connections, the applicant was requested to ensure that I&C system descriptions are appropriately corrected to confirm that this interlock conforms to all acceptance criteria and demonstrates that the interlock can perform its safety function during all plant conditions. In the response to this RAI (ML16344A484), and subsequent revised responses (ML17045A734, ML17258A683, and ML17304A603), the applicant revised Section 7.6,

Table 7.6-2, and Figures 7.6-3, 7.6-4, and 7.6-5 to address the regulatory requirements for the CCW cross connection line isolation valves interlock and the interlocks for both shutdown cooling pumps and containment spray pumps. The staff reviewed the changes to DCD Tier 1 Table 2.5.4-4 and DCD Tier 2, Sections 7.1.1.6, 7.6.1, 7.6.1.4, 7.6.1.5, 7.6.2, 7.6.3, Table 7.6-2, and Figure 7.6-3, 7.6-4 and 7.6-5 as updated by the response and concluded that the response provided sufficient information, such that the staff could evaluate if the CCW cross connection line isolation valves interlock and the interlocks for both shutdown cooling pumps and containment spray pumps meet the relevant requirements for interlock systems important to safety. The response has satisfactorily resolved all of the staff's concerns. The incorporation of the proposed markups into the next revision of FSAR was a confirmatory item. The staff verified that the proposed markups have been incorporated into Revision 2 of DCD Tier 1 Table 2.5.4-4 and Revision 2 of DCD Tier 2, Subsections 7.1.1.6, 7.6.1, 7.6.1.4, 7.6.1.5, 7.6.2, and 7.6.3, Table 7.6-2, and Figures 7.6-3, 7.6-4, and 7.6-5. As such, this confirmatory item has been satisfied.

As shown above in Table 7.6-1, GDC 16 is evaluated in Sections 6.2.1.1 and 6.2.4 of this SER, GDC 34 is evaluated in Sections 7.1.4, 7.3.4.3.10, 7.4.4.2, and 8.3.1 of this SER, GDC 35 is evaluated in Sections 6.2.2, 7.1.4, 7.3.4.3.10, 7.4.4.2, and 8.3.1 of this SER, GDC 38 is evaluated in Sections 6.2.1.1, 6.2.2, 7.1.4, 7.3.4.3.10, 7.4.4.2, and 8.3.1 of this SER, GDC 41 is evaluated in Sections 6.2.5, 6.5.2, 7.1.4, 7.3.4.3.10, and 8.3.1 of this SER, and GDC 44 is evaluated in Sections 7.1.4, and 8.3.1 of this SER.

For GDC 25, DCD Tier 2 Section 7.6.2.1, Item l is not applicable to DCD Tier 2 Section 7.6 because the protection system requirements are met by the opening of the reactor trip breakers, which is evaluated in Section 7.2.6 of this SER.

For GDC 28 and 33, DCD Tier 2 Section 7.6.2.1, Items m and n are not applicable to DCD Tier 2 Section 7.6 because reactivity limits and reactor coolant makeup are implemented by the CVCS. The CVCS has no interlocks important to safety and is evaluated in Section 9.3.4 of this SER.

Based on designing the interlock systems important to safety so that these interlocks contribute to reactor design margin and conformance to SRP BTP 5-2, and SRP BTP 7-1, the staff concludes with reasonable assurance, that the applicant provided sufficient information in the APR1400 design certification application to demonstrate the requirements of 10 CFR Part 50, Appendix A, GDC 10 and 15 are met. As stated in proceeding paragraphs, the evaluation to determine if the requirements of GDC 16, 34, 35, 38, 41, and 44 are in other sections of this SER.

7.6.4.8 ITAAC

The evaluation of ITAAC is in Section 14.3.5 of this SER.

7.6.5 Combined License Information Items

No applicable items were identified in the FSAR. No additional COL information items need to be included in DCD Tier 2 Table 1.8-2 for the interlock systems important to safety.

7.6.6 Findings and Conclusions

The staff reviewed the information submitted by the applicant and concluded with reasonable assurance, that the interlock systems important to safety meet the relevant requirements of GDC 1, 2, 4, 10, 13, 15, 16, 19, 24, 34, 35, 38, 41, and 44, 10 CFR 50.34(f)(2)(v), 10 CFR 52.47(b)(1), and 10 CFR 50.55a(h)(3).

7.7 Control Systems Not Required for Safety

7.7.1 Introduction

The control systems not required for safety include plant information, monitoring, and control systems that are not essential for the safety of the plant. The primary function of the non-safety control system is to maintain variables and the systems within normal operational limits. This SER section evaluates control systems not required for safety. This SER section also evaluates the CSCCF TeR.

7.7.2 Summary of Application

DCD Tier 1: The Tier 1 information associated with this section is discussed in DCD Tier 1 Section 2.5.5. This section states that the control systems, which are not required for safety, consist of the PCS and the P-CCS. The PCS and P-CCS provide the control of functions to maintain the plant within it normal operating range for all normal modes of plant operation.

The PCS includes the RRS, the DRCS, and the RPCS. The P-CCS includes NPCS and BOP control systems. The NPCS consists of the FWCS, the SBCS, the PPCS, the PLCS, and other miscellaneous NSSS control systems which include reactor makeup control function of the CVCS.

Control and display interface devices for the PCS and P-CCS are provided in the MCR and in the RSR for control and monitoring of the PCS and P-CCS:

1. The controllers of the PCS and P-CCS are arranged in separate controller groups as identified in Table 2.5.5-1 of DCD Tier 1 Section 2.5.5 (Table 7.7-1 of this safety evaluation).

2. The digital equipment and software used in the PCS and P-CCS are diverse from those of the PPS and the ESF-CCS.

3. The PCS and P-CCS are controlled from either the MCR or RSR, as selected from MCR/RSR master transfer switches.

Table 7.7-1: Controller Group Arrangement of the PCS and P-CCS[3]

Control Function Description	Controller Group Distribution
SG1 feedwater control (FWCS 1)	Separate control group
SG2 feedwater control (FWCS 2)	Separate control group
Pressurizer pressure control (PPCS)	Separate control group
Pressurizer level control (PLCS)	Separate control group
Turbine bypass control (SBCS Main)	Separate control group
Turbine bypass control (SBCS Permissive)	Separate control group
Reactor makeup control (CVCS)	Separate control group
Control rod control (RRS/RPCS)	Separate control group
Control rod control (DRCS)	Separate control group
Reactor coolant pump control	Separate control group
Feedwater HP heater train A control	Separate control group
Feedwater HP heater train B control	Separate control group
Feedwater HP heater bypass line control	Separate control group
Feedwater pumps On/Off	Separate control group
Non-Class 1E alternating current power to the station auxiliaries (13.8 kV Non-Class 1E System)	Separate control group
Condenser vacuum and LP Feedwater heater control	Separate control group
TCS	Separate control group
Miscellaneous BOP - Circulating water pump - Condensate pump - Deaerator - Turbine gland sealing	Separate control group

DCD Tier 2: The applicant provided a system description in DCD Tier 2 Section 7.7, "Control Systems Not Required for Safety." This section states that plant information, monitoring and control systems not essential for plant safety are designed so that credible failures in the

[3] Source: DCD Tier 1 Table 2.5.5-1; CSCCF TeR

systems do not impact the operation of the safety-related systems. Interfaces between safety-related and non-safety systems use isolation devices to maintain electrical independence. Isolation devices are considered part of the safety-related system and are qualified as Class 1E.

In general, the non-safety control system sensors and signal conditioning devices are separated from those used in safety-related control systems. Where safety-related devices provide parameters for control and monitoring, signal isolation is provided between the safety-related systems and the non-safety control and monitoring systems.

The IPS and the QIAS-N receive data from safety-related and non-safety systems through a fiber-optic network that provides the isolation.

The HSI design for both safety-related systems and non-safety systems in the MCR and RSR are subject to the HFE design processes described in Chapter 18. Non-safety consoles are designed to maintain structural integrity so that no missile hazards are generated as a result of a seismic event.

To provide reasonable assurance that the failure of non-safety control systems does not cause plant conditions more severe than those described in the analysis of AOO in Chapter 15, each control function of NSSS is distributed to the separate control group that consists of at least one separate controller. The control groups for NSSS control functions are listed in Table 7.7-1 (Table 7.7-2 of report).

Table 7.7-2: Control Groups for NSSS Control Functions[4]

Control Group	Postulated Events Due to a Single Failure in the Corresponding Control Group				
	Excessive or Deficient Feedwater Flow	Full Open of Any One turbine bypass valve (TBV)	Excessive Charging Flow or Excessive pressurizer (PZR) Spray	Uncontrolled CEA Withdrawal	Inadvertent De-boration
SG1 feedwater control (FWCS 1)	X				
SG2 feedwater control (FWCS 2)	X				
Pressurizer pressure control (PPCS)			X (Excessive PZR Spray)		

[4] Source: DCD Tier 2 Table 7.7-1

Control Group	Postulated Events Due to a Single Failure in the Corresponding Control Group				
	Excessive or Deficient Feedwater Flow	Full Open of Any One turbine bypass valve (TBV)	Excessive Charging Flow or Excessive pressurizer (PZR) Spray	Uncontrolled CEA Withdrawal	Inadvertent De-boration
Pressurizer level control (PLCS)			X (Excessive Charging Flow)		
Turbine bypass control (SBCS Main)		X			
Turbine bypass control (SBCS Permissive)		X			
Reactor makeup control (CVCS)					X
Control rod control (RRS/RPCS)				X	
DRCS				X	

Technical Specifications: N/A

ITAAC: ITAAC associated with the PCS and P-CCS are specified in Table 2.5.5-2 of DCD Tier 1.

Technical Specifications: There are no Technical Specifications associated with control systems.

7.7.3 Regulatory Basis

The relevant requirements of applicable NRC regulations for this area of review, and the associated acceptance criteria, are given in SRP Section 7.7, “Control Systems,” and are summarized below. Review interfaces with other SRP sections also can be found in SRP Section 7.7.

1. GDC 1, 10, 13, 15, 19, 24, 28, 29, and 44.

2. 10 CFR 52.47(b)(1), which requires that a design certification application contain the proposed ITAAC that are necessary and sufficient to provide reasonable assurance that, if the inspections, tests and analyses are performed and the acceptance criteria met, a plant that incorporates the design certification is built and will operate in accordance with the design certification, the provisions of the Atomic Energy Act and the NRC's regulations.

3. 10 CFR 50.55a(h)(3), "Protection and Safety Systems," requires compliance with IEEE Std 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," and the correction sheet dated January 30, 1995. For control systems isolated from safety-related systems, the applicable requirements of 10 CFR 50.55a(h)(3) are defined in IEEE Std 603-1991, Clause 5.6.3, "Independence Between Safety Systems and Other Systems," and IEEE Std 603-1991, Clause 6.3, "Interaction Between the Sense and Command Features and Other Systems."

4. 10 CFR 50.34(f)(2)(xxii), "Additional TMI-Related Requirements" (applies only to Babcock and Wilcox designs).

Acceptance criteria adequate to meet the above requirements can also be found in SRP Section 7.7.

Table 7.7-3: Design Considerations Referenced in Other Sections of this SER

Design Consideration	SER Section(s)
Quality Standards, GDC 1	7.1.4.3
Single Failure Protection, GDC 21	7.1.4.5
Completion of Protective Action, 10 CFR 50.55a(h)	7.1.4.6
Quality, 10 CFR 50.55a(h)(3), GDC 1	7.1.4.7
Independence, 10 CFR 50.55a(h)(3), GDC 21, 22, and 24	7.1.4.10, 7.9
Equipment Qualification, 10 CFR 50.55a(h)(3), GDC 2 and 44	7.1.4.8, 3.10, 3.11
System Integrity, 10 CFR 50.55a(h)(3)	7.1.4.9
Capability for Test and Calibration, 10 CFR 50.55a(h)(3) and GDC 21	7.1.4.11
Information Displays, 10 CFR 50.55a(h)(3), GDC 13, and GDC 19	7.1.4.12, 7.5.4
Control of Access, 10 CFR 50.55a(h)(3)	7.1.4.13, 7.9.4.3
Repair, 10 CFR 50.55a(h)(3)	7.1.4.14
Identification, 10 CFR 50.55a(h)(3)	7.1.4.15
Auxiliary Features, 10 CFR 50.55a(h)(3)	7.1.4.16
Multi-Unit Stations, 10 CFR 50.55a(h)(3)	7.1.4.17
Human Factors Considerations, 10 CFR 50.55a(h)(3) and GDC 19	7.1.4.19, 18.0

Design Consideration	SER Section(s)
Reliability, 10 CFR 50.55a(h)(3) and GDC 21	7.1.4.20
Automatic and Manual Control, 10 CFR 50.55a(h)(3)	7.1.4.22
Derivation of System Inputs, 10 CFR 50.55a(h)(3)	7.1.4.18
Bypasses (Operating and Maintenance), 10 CFR 50.55a(h)(3), GDC 13 and 19	7.1.4.23, 7.1.4.24, 7.5.4.2
Setpoints, 10 CFR 50.55a(h)(3)	7.1.4.25
TMI-Related Requirements, 10 CFR 50.34(f)	7.5.4.1
D3, 10 CFR 50.55a(h) and GDC 22	7.1.4.21, 7.8
ITAAC, 10 CFR 52.47(b)(1)	14.3.5

7.7.4 Technical Evaluation

7.7.4.1 System Description

7.7.4.1.1 PCS

The PCS integrates the control systems that control the reactor power level, which include the RRS, DRCS, and RPCS.

7.7.4.1.1.1 RRS

The RRS automatically adjusts reactor power and reactor coolant temperature to follow the turbine load transients within the established limits. Figure 7.7-1 shows that the RRS receives a turbine load index signal (linear indication of load) and reactor coolant temperature signals.

The desired average temperature is determined by a reference temperature (T_{REF}) program that is inputted with the turbine load index. The hot leg and cold leg temperature signals are averaged (T_{AVG}) in the RRS. The T_{REF} signal is then subtracted from the T_{AVG} signal to provide a temperature error signal. Power range neutron flux is subtracted from the turbine load index to provide compensation to the $T_{AVG} – T_{REF}$ error signal generated.

This resulting error signal is fed to a CEA rate program to determine whether the CEAs are to be adjusted at a high or low rate, and to a CEA motion demand program that determines if the CEAs are to be withdrawn, inserted, or held. The outputs of the rate and motion demand programs are used by the DRCS. If the temperature error signal is high (i.e., TAVG is higher than T_{REF}, or the cold leg temperature (T_{COLD}) is higher than a limit), the RRS provides an automatic withdrawal prohibit (AWP) signal to the DRCS. The withdrawal of CEAs causes the TAVG to increase. Prohibiting a withdrawal prevents an increase in the error signal.

7.7.4.1.1.2 DRCS

The DRCS uses automatic CEA motion demand signals from the RRS or manual motion signals from the DRCS soft control display on the IFPD to convert these signals to direct current pulses that are transmitted to the CEDM coils to cause CEA motion.

The SBCS generates an AWP signal whenever SBCS demand for opening the turbine bypass valves exists. The AWP signal is sent to the DRCS to block its response to the RRS demands for withdrawing CEAs and thus preventing an increase in reactor power when there is excess energy in the NSSS.

A reactor trip initiated by either RPS or the DPS causes the input motive power to be removed from the DRCS, which causes all CEAs to be inserted by gravity, as shown in DCD Tier 2 Figure 7.7-2.

There are five modes of control: sequential group movement in manual and automatic control, manual group movement, manual individual CEA movement, and standby.

Sequential group movement functions such that, when the moving group reaches a programmed low (or high) position, the next group begins inserting (or withdrawing), thus providing for overlapping motion of the regulating groups. The initial group stops upon reaching its lower (or upper) limit. Applied successively to all regulating groups, the procedure allows a smooth continuous rate of change of reactivity. The DRCS group sequencing logic necessitates that the preceding group reach a specified limit before the next group is permitted to move. The DRCS and IPS monitor proper sequential motion and provide an alarm for out-of-sequence conditions.

The DRCS also includes normal CEA control limits and CEA interlocks for all CEAs and part-strength CEAs (PSCEAs). The CEA control limits include both the upper group stop (UGS) and the lower group stop (LGS) for full-strength CEAs and the PSCEAs. Control limits are provided to automatically terminate CEA motion upon reaching the CEA limits of travel. Whenever the DRCS receives an upper electrical limit (UEL) or lower electrical limit (LEL) interlock signals from the reed switch position transmitters (RSPTs), it prohibits the withdrawal or the insertion of the appropriate CEA. These UEL and LEL interlock signals are provided to automatically terminate CEA motion upon reaching the CEA upper and lower limits of travel.

The shutdown CEAs are moved in the manual control mode only, with either individual or group movement. The DRCS soft control permits withdrawal of no more than one shutdown group at any time.

The DCD Tier 2 Section 7.7 did not provide a sufficient level of detail regarding the standby mode of operations for the DRCS. The staff issued RAI 356-7881, Question 07-6, to request the applicant provide more clarity on the standby mode of operation. In a March 4, 2016, response to RAI 356-7881, Question 07-6 (ML16064A371), the applicant provided the staff more information on the 'standby' mode of operation for the DRCS. The applicants states, in part, the following in its response:

> Standby mode prevents CEAs from being moved by the DRCS. Except for when the DRCS is undergoing maintenance, the DRCS is operable when placed in standby mode. When the DRCS is in standby mode, power is supplied to the CEDM coils, and all CEAs are held in their current position. To move CEAs, the operator can change the DRCS control mode from standby mode to one of the other four DRCS control modes by selecting the desired DRCS control mode in the DRCS soft control display on the IFPD.

An operator can put the DRCS in standby mode by selecting the standby mode in the DRCS soft control display on the IFPD. An operator can put the DRCS in standby mode in order to

hold all CEAs in the current position for maintenance of the DRCS or when all CEA motion is to be prohibited according to DCD Tier 2 Chapter 16.

When the DRCS is in standby mode, all CEA movement is inhibited, and all CEAs are held in their current positions. However, the reactor shutdown (reactor trip) function of the RPS and the DPS is not affected because they can remove the motive power from the motor generator set to the DRCS by the RTSS and all CEAs can be inserted by gravity as shown in DCD Tier 2 Figure 7.7-2.

The staff found the applicant's response to RAI 356-7881, Question 07-6, is adequate because the response adequately described the design functionality of the standby mode of operation for the DRCS including the purpose for the standby mode as well as how the standby mode takes place within the scope of the DRCS and the staff considers the issues identified in RAI 356-7881, Question 07-6, is closed and resolved.

The DRCS includes pulse counting to infer each CEA position by electronically monitoring the mechanical actions within each CEDM to determine when a CEDM has raised or lowered the CEA. The pulse counting CEA position signal associated with each CEA is reset to zero whenever the rod drop contact (located within the RSPT housing) is closed. This permits the pulse counting system to automatically reset the position to zero, whenever a reactor trip occurs or whenever a CEA is dropped into the core. This CEA position information is used in MCR displays. The displays provide CEA group information and individual CEA position information.

The DRCS also provides the IPS with each CEA position from the pulse counting system for use in the CEA monitoring displays and alarms and the COLSS as described in Section 7.7.1.4 of DCD Tier 2 Section 7.7.

The DRCS receives a CWP signal from the PPS. This signal stops withdrawal motion of all CEAs. It can be overridden by the operator with the DRCS soft control display on the IFPD in the MCR.

7.7.4.1.1.3 RPCS

The RPCS is a control system designed to accommodate certain types of imbalances by providing a "step" reduction in reactor power. The step reduction in reactor power is accomplished by the simultaneous dropping of one or two preselected groups of full strength regulating CEAs into the core. The CEA groups are dropped in their normal sequence of insertion. The RPCS also provides control signals to the turbine to rebalance turbine and reactor power following the initial reduction in reactor power as well as to restore the SG water level and pressurizer pressure to their normal controlled values. The system accommodates either large load rejections or loss of two main feedwater pumps.

The RPCS receives two of each of the following signals: reactor power cutback demand signals from the SBCS and loss of two feedwater pumps. A 2oo2 logic is required to actuate the system for load rejections. The operator has the capability to manually actuate the system.

The predetermined pattern of appropriate CEA groups for use in the reactor power cutback is accomplished by CEA selection logic in the IPS. This logic utilizes NSSS power, CEA positions, and coolant temperatures, and provides the RPCS with the CEA groups selected for dropping during reactor power cutback. If the IPS CEA selection logic is inoperable, the RPCS control logic can switch to the manual select mode. In the manual select mode, the operator inputs the

CEA group drop selection through the RPCS soft control display. This feature increases the availability of the system.

The RPCS actuation initiates a preselected pattern of CEAs upon receiving 2oo2 coincidence signals indicating large turbine load rejection or loss of two feedwater pumps. There are inhibits in the DRCS to prevent the possibility of the RPCS dropping CEA groups that are not intended to drop for a reactor power cutback (e.g., part-strength groups, shutdown groups). Subsequent insertion of other groups either automatically by the RRS or manually by the operator occurs as necessary.

The RPCS maintains the NSSS within the control band ranges by a rapid reduction of NSSS power at a rate that is greater than that provided by the normal high-speed CEA insertion.

7.7.4.1.2 P-CCS

The P-CCS controls non-safety components such as pumps, valves, heaters, and fans. The P-CCS sends process variables and P-CCS status information to the IPS and QIAS-N. In case the P-CCS is unavailable, non-safety signals for monitoring safe shutdown are hardwired to the QIAS-N. The components are assigned to the group controller for system-level control and loop controller for component-level control to minimize the plant impact due to system or component failures, as shown in Figure 7.7-8 of DCD Tier 2 Section 7.7.

The group controller performs supervisory control of groups of components such as an alternate ac generator control system or turbine/generator control system and provides system-level status information to the IPS and QIAS-N. The P-CCS has master transfer function to disable MCR controls and to enable RSR controls. The P-CCS loop controllers are located in the vicinity of the controlled component. The loop controller and internal data communications are redundant. The P-CCS has soft control HSIs on the IFPD.

7.7.4.1.3 NSSS

The reactivity feedback properties of the NSSS inherently cause reactor power to match the total NSSS load. The resulting reactor coolant temperature is a controlled parameter that is adjusted by changes in the total reactivity implemented through the control element assembly CEA position changes or through the boric acid concentration changes in the primary coolant. The ability of the NSSS to follow the turbine load changes is dependent on the ability of the control systems or the operator to adjust reactivity, feedwater flow, bypass steam flow, reactor coolant inventory, and energy content of the pressurizer such that NSSS conditions remain within normal operating limits.

The ability of the NSSS to follow the turbine load changes is dependent on the ability of the control systems or the operator to adjust reactivity, feedwater flow, bypass steam flow, reactor coolant inventory, and energy content of the pressurizer such that NSSS conditions remain within normal operating limits.

The DCD Tier 2 Section 7.7.1.1 discusses the ability of the APR1400 I&C control system to support load following. The staff did not evaluate the ability of the APR1400 design to load follow since this capability is not credited in the APR1400 design certification application.

7.7.4.1.4 FWCS

The FWCS performs automatic control of steam generator water level. Steam generator level is controlled during the following conditions:

- Steady-state operations:

  1 percent per minute turbine load ramps between 5 percent and 15 percent NSSS power, and 5 percent per minute turbine load ramps between 15 percent and 100 percent NSSS power.

  1 percent turbine load steps between 5 percent and 15 percent NSSS power, and 10 percent turbine load steps between 15 percent and 100 percent NSSS power.

- Loss of one of three operating feedwater pumps.

- Load rejection of any magnitude.

7.7.4.1.5 SBCS

The SBCS is part of the overall turbine bypass system. The SBCS main controller controls for the position of the turbine bypass valves, which bypassed steam travels, past the turbine and onto the unit condenser. The applicant states that the SBCS has been designed to increase plant availability by removing excess NSSS thermal energy in the event of a turbine load rejection by modulation of the turbine bypass valves to control the release of steam.

The SBCS generates an AWP signal whenever SBCS demand for opening the turbine bypass valves exists. The AWP signal's function is to block control rod withdrawal on automatic control mode of the DRCS. The AWP signal blocks the response to the RRS demands for withdrawing CEAs and prevents an increase in reactor power when there is excess energy in the NSSS.

7.7.4.1.6 PPCS

The PPCS maintains the RCS pressure within specified limits by the use of pressurizer heaters and spray valves. The pressurizer provides a water/steam surge volume to minimize pressure variations due to density changes in the coolant.

A pressurizer pressure error signal is generated by comparing a pressure signal with a pressure setpoint and is used in a proportional-integral controller to control the proportional heaters, as shown in Figure 7.7-3 of DCD Tier 2. The heaters are operated to maintain the pressurizer pressure as required. The operator can take manual control to regulate the pressure.

The pressurizer pressure error signal is also sent to a spray valve program. This provides a signal to the spray valves to control their opening. Since reactor coolant is cooler than the water/steam mixture, reactor coolant sprayed in causes some steam to condense in the pressurizer and thereby reduce the system pressure. The operator can take manual control of the spray valves to control the pressure.

If the proportional heaters are being used and system pressure is still decreasing, the backup heaters will actuate automatically. The backup heaters can also be actuated manually.

The control system has a low-level interlock and a high-pressure interlock. The low-level interlock shuts off all the heaters when the level falls below a setpoint. If the pressurizer pressure reaches a high setpoint, all heaters are de-energized to provide reasonable assurance that the heaters will not cause the pressure to increase further.

7.7.4.1.7 PLCS

The PLCS controls RCS coolant level by using the charging control valve and letdown orifice isolation valves in the CVCS described in DCD Tier 2 Section 9.3.4. The PLCS also maintains vapor volume in the pressurizer to account for level surges during transients. DCD Tier 2 Figure 7.7-4, shows the PLCS diagram.

During normal operation, the level setpoint is programmed as a function of RCS TAVG in order to minimize required charging and letdown flow. The TAVG goes through a level setpoint program and the setpoint program signal is compared to the actual level signal. The level error signal is sent to a proportional-integral controller and comparators to control the charging control valve and letdown orifice isolation valves.

If the level error is high, the selected charging control valve is throttled back. If the level error is low, the charging control valve is open. If the level error exceeds a preset setpoint at which the charging control valve is not sufficient to control the level error, the letdown orifice isolation valves are opened or closed to control letdown flow.

The operator can manually control the level by controlling the charging control and letdown orifice isolation valves. The PLCS soft control display on the IFPD allows a selection of the charging control valve operated by the PLCS.

7.7.4.1.8 NIMS

The NIMS detects selected conditions that could indicate deterioration of the RCS pressure boundary. NIMS comprises the following subsystems:

- Intervals vibration monitoring system,
- Acoustic leak monitoring system,
- Loose parts monitoring system, and
- RCP vibration monitoring system.

Alarms that are generated for each system are provided in the MCR.

7.7.4.1.9 IPS

The IPS is a computer-based system that provides operational means for monitoring and control of the plant. The information is derived from other I&C systems and self-contained algorithms called application programs. The IPS makes the information available to the plant operating staff both on a real-time and historical basis.

The IPS is designed to enhance overall power plant operability, availability, and efficiency. These are accomplished through the use of integrated plant information displays and advanced alarm design. Analysis of data assists the operating staff in operating the plant within specified

limits while evaluating the performance of the reactor core, primary and secondary plant systems and components.

The IPS provides the necessary interfaces with the TSC, EOF, and ERDS to make the same information that is available to the operating staff available to other interested personnel. The IPS equipment includes workstations and printers installed, as shown in Figure 7.7-12 and described further in DCD Tier 2 Section 7.7.1.4.

The IPS performs a supervisory monitoring and control function for the NSSS and BOP steam and electrical production processes. It allows the operating staff to obtain detailed plant data by use the HSI displays. These HSI devices are integrated into the MCR in a manner that meets the Style Guide that is described in DCD Tier 2 Chapter 18.

The major functions performed by the IPS include plant wide data acquisition, validation of sensed parameters, execution of NSSS application programs and BOP performance calculations, monitoring of plant safety and general status, presentation of status and calculation results on IPS displays, provision of logs, and determination of alarm conditions.

7.7.4.1.10 Information Displays

The QIAS-N is also implemented on the common PLC platform, even though it is a non-safety system, because it displays the important plant parameters and maintains diversity from the IPS. The IPS consists of redundant servers, display devices, data storage devices, printers, and other support devices.

In the event of failure of the IPS, the operator uses the mini LDP driven by QIAS-N on the safety console. The QIAS-N provides alarms, values, and trends. The operator uses QIAS-N displays to assess operational availability and performance of the plant systems.

According to the applicant, the IFPDs are implemented as part of the IPS. IFPD consists of a FPD, pointing device, display processor, and communication interface. Each IFPD is driven by a dedicated display processor. The display system communicates with the IPS servers and engineering workstation over a data communication network. The ESCMs connected to the IFPD are physically and electrically isolated from the IPS. If a data communication error occurs and is detected, an appropriate message is generated. Diagnostic tests are then performed to identify the cause of the data communication error.

The major functions performed by the IPS include plant wide data acquisition, validation of sensed parameters, execution of NSSS application programs and BOP performance calculations, monitoring of plant safety and general status, presentation of status and calculation results on IPS displays, provision of logs, and determination of alarm conditions.

7.7.4.2 Evaluation of DCD Tier 1 Information

The DCD Tier 1 Table 2.5.5-2, Design Commitment Item #2 states, “The digital equipment and software used in the PCS and P-CCS are independent from those of the [PPS] and the [ESF-CCS].” The associated ITAAC and acceptance criteria for this design commitment also allude to the goal of verifying that software of the PCS and P-CCS were developed by groups independent from the groups that developed software of the PPS and ESF-CCS. Though there is a requirement for these system to be independent from one another based upon their safety classification (i.e., IEEE Std 603-1991, Clause 5.6), the acceptance criteria and ITAAC imply a method of verification that would be associated with defining ‘diversity’ between two sets of

software based upon guidance in NUREG/CR-6303. The staff issued RAI 68-7892, Question 07.07-1, to request the applicant to clarify whether it was imposing independence criterion on the non-safety systems or diversity criterion.

In the September 2, 2015, response to RAI 68-7892, Question 07.07-1 (ML15245A322), the applicant proposed corrected information regarding DCD Tier 1 Section 2.5.5, as well as Table 2.5.5-2. The applicant provided updated information to state that digital equipment and software used to implement the PCS and P-CCS are diverse from digital equipment and software used to implement the PPS and ESF-CCS. The applicant stated that the intent of Design Commitment #2 was to verify diversity criterion and not independence. Independence is addressed in other areas of the licensing basis. The applicant re-affirmed this design commitment in ITAAC Table 2.5.5-2, as an ITAAC item.

The applicant's response to RAI 68-7892, Question 07.07-1, adequately resolves the staff's concerns by confirming that the intent of Design Commitment #2 of DCD Tier 1 Table 2.5.5-2 was to verify diversity criterion. Therefore, the staff finds the applicant's response to RAI 68-7892, Question 07.07-1, and associated proposed changes acceptable. Pending the incorporation of proposed changes into the next revisions of the FSAR, the staff considers this RAI was a confirmatory item. The staff verified that the proposed markups have been incorporated into the Revision 1 of DCD Tier 1. As such, this confirmatory item has been satisfied.

7.7.4.3 DCD Tier 2 Information/Technical Reports

In DCD Tier 2 Section 7.1, the applicant states the following with regard to the non-safety systems:

> Most of the non-safety I&C systems are implemented by a [DCS]-based common platform that has been proven in operating experience in the nuclear industry and other industries. The DCS conducts the functions of the operator interface, component-level control, automatic process control, high-level group control, and data processing for normal operation. The DCS is designed with a redundant and fault-tolerant architecture for high reliability and to prevent the failure of a single component from causing a spurious plant trip.

The applicant does not provide any information specifically outlining the structure of the DCS implementation for the non-safety systems and does not provide any figures or diagrams showing the networked, architectural configuration of the non-safety systems that provide evidence to support the claim that the DCS is redundant and fault tolerant or provides high reliability in DCD Tier 2 Section 7.1. DCD Tier 2 Section 7.7 does not provide a diagram that demonstrate the architectural configuration of the non-safety DCS that would permit better understanding of the non-safety I&C system DCS architecture as per the requirements of 10 CFR 52.47(a)(2), which requires, in part, that the description of the SSCs be sufficient to permit understanding. The PCS and P-CCS are complex systems that contain numerous subsystems and understanding how these systems are networked together is necessary in order to understand the entirety of the non-safety DCS architecture. The staff issued RAI 68-7892, Question 07.07-5, to request the applicant to provide more details on the architectural configuration of the PCS and P-CCS.

In the October 11, 2016, response to RAI 68-7892, Question 07.07-5 (ML16285A534), the applicant provided a new internal network diagram which depicts the following:

- The internal network configuration of the PCS, P-CCS and other non-safety I&C systems.
- The differing types of communications between each portion of the network.
- The safety class designation for each portion of the network including interfaces between safety-related and non-safety control systems.

The new diagram provides an adequate general overview of the overall non-safety DCS along with adequate depictions of various types of communications within the network, both internal and external. The applicant proposed to include the internal network of the PCS and other non-safety I&C systems in the CSCCF TeR. The new network diagram facilitates improved understanding of some of the complexities that exist within the non-safety I&C systems and provides more clarification overall. The applicant also proposed to modify DCD Tier 2 Section 7.7.1.1 to state that the UEL, LEL, and rod drop contacts signals from the RSPTs are interfaced to the DRCS via optical isolation to provide separation and independence. The staff finds the applicant's response to be adequate due to the reasons stated above. The incorporation of the proposed markups into the next revision of the CSCCF TeR and DCD Tier 2 Section 7.7.1.1 was a confirmatory item. The staff verified that the proposed markups have been incorporated into the Revision 1 of the FSAR, and Revision 1 of the CSCCF TeR. As such, this confirmatory item has been satisfied.

7.7.4.4 Remote control center

The DCD Tier 2 Section 7.7.1.1, Revision 0, the applicant states, in part, that the 7.7.4.4 Remote control center (RCC) is provided to address severe accident conditions. The applicant states the following.

> The RCC is designed against aircraft impact to meet the requirements of 10 CFR 50.150. The minimum equipment needed to maintain the reactor for 24 hours is provided to accomplish hot standby plant condition. The operator can shut down the reactor from the MCR 10 minutes before aircraft impact upon the MCR in the auxiliary building, and the control and monitoring is transferred to the RCC using a transfer switch located in the MCR. The RCC is located separately from the MCR so that aircraft impact to the MCR does not adversely affect the RCC operation integrity.
>
> The RCC panel consists of divisionalized safety control and non-safety controls to achieve plant hot shutdown. The signals from the RCC are routed from the RCC to the I&C equipment room as well as to the [motor control center] through multiplexers.

The RCC is not depicted on Figure 7.1-1, "APR1400 I&C System Overview Architecture," and therefore, there is no physical depiction of how the functionality of the RCC is taken into account with the overall I&C architecture, or how it's implemented. The acronym for the remote control center is also not defined in the Acronym and Abbreviation list in DCD Tier 2 Section 7.0. The staff cannot determine what the difference is between the RCC and the RSR as the applicant does not describe the design function of the RCC in DCD Tier 2 Section 7.7. The staff issued RAI 356-7881, Question 07-5, to request the applicant to provide more design detail on the RCC and its implementation per the requirements of 10 CFR 52.47(a)(2). The response will

facilitate the staff's determination on whether the requirements of 10 CFR Part 50, Appendix A, GDC 13, apply to the RCC.

In the October 24, 2016, response to RAI 356-7881, Question 07-5 (ML16336A827), and the December 19, 2016, response to RAI 522-8633, Question 07.07-19 (ML16354A501), the applicant provided more design detail on the RCC, summarized as follows from both responses:

Design Features of the Remote Control Center

The RCC provides manual control and monitoring means to bring the plant to hot standby operations under accident conditions. The RCC panel room is located on the opposite side of the plant from the MCR and the RSR so that an aircraft impact cannot affect all three rooms at the same time. The RCC is operated by one reactor operator who will monitor and control the plant. For control and monitoring, the RCC has four divisionalized ESCMs for safety component control and process monitoring and a dedicated control channel gateway. These ESCMs has the same design features as ESCMs located in the MCR and RSR. A communication interface does not exist between the safety-related system and non-safety systems in the RCC. The non-safety manual switches on the RCC and P-CCS loop controller are physically and electrically isolated from the ESCMs and the dedicated control channels gateways on the RCC. The MCR/RCC transfer switches consist of four safety division switches and one non-safety switch and these switches are physically separated and electrically isolated from each other. Conventional hardwired switches, indicators, and non-safety component control are also provided. The ESCMs and conventional switches in the RCC are physically separated from the MCR and RSR. The ESCMs are connected to the ESF-CCS loop controller in the remote multiplexer room through a dedicated route which is also separate from the MCR and RSR. The conventional switches are connected to the P-CCS cabinets in the remote multiplexer room through a dedicated route which is also separate from the MCR and RSR.

Differences between RSR and RCC

The RSR is designed to meet safe shutdown requirements as per GDC 19 in the case that the MCR becomes uninhabitable. The RCC is designed as a supplemental facility to accommodate aircraft impact event. The RSR and RCC are two distinct and different areas of the plant under different regulatory applications.

Design Requirements and Commitments in the RCC

The RCC is classified as non-safety. Controls and displays in the RCC have been designed according to NUREG-0700 and NUREG-0711. The ESCMs on the RCC are seismically and environmentally qualified as Class 1E. The applicant states that no single credible event that would require concurrent evacuation of the MCR and RSR (or fire damage to either room) would make the RCC inoperable.

With regard to verification of RCC equipment design requirements, the applicant stated the following, in part, the following:

- MCR/RCC transfer switches and transfer control function of the ESF-CCS are verified as described in DCD Tier 1 Table 2.5.4-4 Item 8 [Refer to the response to RAI 356-7881, Question 07-5].

- Testing for the MCR/RCC transfer switches and transfer control function of the P-CCS will be added to DCD Tier 1 Table 2.5.5-2, Item 3.

- The ESCMs located in the RCC are verified to meet independence, physical separation, and EMI/RFI requirements as described in DCD Tier 1 Table 2.5.4-1, Items 2 and 16.

Within the RAI responses, the applicant also included a new, detailed network diagram, showing the interconnections between the RCC and the MCR/RSR and included proposed markups for DCD Tier 2 Figure 7.1-1, to show the existence of the RCC and associated connections. The applicant also proposed similar updates to I&C architecture drawings in the Safety I&C System TeR and the D3 TeR.

Based upon the information presented by the applicant in both RAI responses, the staff finds the applicant had adequately addressed both of staff requests. The applicant has provided a sufficient level of information to permit understand of the design and regulatory basis for the RCC. The applicant has clarified that the RCC's main regulatory purpose is to supplement the aircraft impact analysis and that the RCC is a distinct area of the plant apart from both the MCR and RSR. The RCC also has relevant controls contained within to meet is intended design function. The applicant has also adequately addressed I&C-specific regulatory compliance in terms of demonstrating independence requirements for relevant safety-class controls in the RCC will be incorporated, verified and validated through associated ITAAC. The applicant has also provided enclosed markups with proposed changes to relevant licensing documents that adequately describe updates with new design information presented in these RAI responses. The staff considers the issues identified in both RAI 356-7881, Question 07-5, and RAI 522-8633, Question 07.07-19, are closed and resolved. The incorporation of the proposed markups into the next revision of relevant licensing documents was a confirmatory item. The staff verified that the proposed markups have been incorporated into Revision 1 of DCD Tier 2 Section 7.7 and related licensing documentation. As such, the confirmatory item has been satisfied.

7.7.4.5 Evaluation of Information Displays

In Section 7.7.1.4 of DCD Tier 2, regarding the IFPDs, the applicant states that, "If a data communication error occurs, an appropriate message is generated." For information displays, the applicant does not appear to state in the licensing documentation how an operator can determine whether a failure (e.g., CCF) has caused the display to fail (e.g., freezes or locks up). Therefore, it is not apparent that an appropriate error message would be generated to alert the operator(s) to a CCF, for non-safety or safety-displays. The staff issued RAI 356-7881, Question 07-18, to request the applicant to describe how operators can determine if failures have occurred in the non-safety MCR displays and controls such as the IFPDs and QIAS-N.

In the October 24, 2016, response to RAI 356-7881, Question 07-18 (ML16298A370), the applicant provided more information on the means by which operators can determine failure of the IFPDs have occurred. The applicant stated in its response that the March 15, 2016, response to RAI 323-821, Question 07.03-19 (ML16075A425), provides for mechanisms that will alerts operators to when the IFPDs are malfunctioning. The evaluation for this RAI response can be found in Section 7.3 of this SER regarding IFPDs.

Regarding the QIAS-N, the applicant states the following:

> The QIAS-N processor receives [safety-related] system signals via the ITP. The QIAS-N MTP receives non-safety system signals via the multi-channel gateway. Isolation devices are used between the ITP and QIAS-N processor, and between

the multi-channel gateway and QIAS-N MTP. The QIAS-N processor performs applicable calculations based on the data received from the [safety-related] systems and non-safety systems. The QIAS-N MTP provides maintenance and testing means of the QIAS-N, and a gateway function with the multi-channel gateway to provide communication from the non-safety P-CCS. The QIAS-N server contains the process database, updates the values and status of the database records, executes the alarm processing function, and functions as a gateway between the QIAS-N network and QIAS-N display network.

The data from the QIAS-N processor ([safety-related] system signals) and the data from the QIAS-N MTP (non-safety system signals) are broadcasted on the QIAS-N network. The QIAS-N server captures the data from the QIAS-N network and updates the QIAS-N process database. The QIAS-N server broadcasts them on the QIAS-N display network for indication on the QIAS-N displays (QIAS-N FPDs, mini-LDPs, and SODPs).

Internal self-diagnostic functions in place within the QIAS-N server to alert operators to potential failures include:

- Self-diagnostics monitoring of QIAS-N MTP, QIAS-N processor, QIAS-N network, QIAS-N display panels.
- The QIAS-N server generates and transmits trouble alarms and status indication to the IPS.
- Transfer the QIAS-N trouble status to the QIAS-N MTP via QIAS-N network for indication on the QIAS-N MTP displays.
- Transfer the QIAS-N trouble status to the QIAS-N FPDs, mini-LDPs, and SODPs via QIAS-N display network.

The staff finds the information provided in the response adequately demonstrates that operators will have adequate indication of trouble within QIAS-N through monitoring by the QIAS-N server so that corrective actions can be taken using means such as the QIAS-N MTP. Enclosed markups within the response to RAI 356-7881, Question 07-18, are also adequate and reflect the updated design information described above. The incorporation of these proposed markups into the next revision of relevant licensing documents was a confirmatory item. The staff verified that the proposed markups have been incorporated into Revision 1 of DCD Tier 2, Sections 7.5 and 7.9. As such, the confirmatory item has been satisfied.

The applicant also stated in the response that operator consoles (i.e., including IFPDs) are considered inoperable when one of the following occurs:

- Three IFPDs and each mouse are unavailable.
- Three ESCMs are unavailable.
- The workstation disable switch is switched to “disable mode.”

Regarding the workstation disable switch, the applicant states that it is a hardwired two-position type of cam rotational switch. This switch can disconnect the non-safety power to the IFPD and

peripheral devices while in “disable mode.” The applicant did not provide further design information as per the staff’s RAI to provide a complete set of design information on this mechanism. The applicant is not definitive that removing power from IFPDs and peripherals is the only design function of this switch. The applicant has not added this switch, and associated hardwired connections, to any system diagram presented in this RAI response so it is not apparent how the switch accomplishes its design function. All of the switch’s internal and external connections have not been identified. The response also does not account for the effects of a potential failure of this switch.

The applicant has provided a sufficient level of design detail in its response to RAI 323-7821, Question 07.03-19, to demonstrate that operators have adequate indication and design measures in place to be alerted of potential failures of QIAS-N and IFPDs as well as adequate means to compensate for IFPD failure (e.g., disabling problematic IFPDs through the disable switch as well as safety-related controls and displays available to operators). In addition, Section 4.4.4 of the CSCCF TeR provides information on design features in place to prevent spurious control actions from the IFPDs in case of failure. The applicant has not provided an adequate level of design detail on the disable switch itself, which was part of the staff’s RAI request. As such, the staff considered this portion of the RAI 356-7881, Question 07-18, an open item.

In the June 4, 2017, response to RAI 356-7881, Question 07-18 (ML17155A003), the applicant stated the following, in part,

- Addition of a new figure containing the configuration of the workstation disable switch (WDS).
- The WDS is to disconnect the signal interface of the IFPD and peripheral devices (e.g., mouse, keyboard) from the node of the DCN-I network should these non-safety devices generate spurious signals.
- The WDS is located on each operator console and is a hardwired two-position (enable/disable) type of cam switch.
- The WDS does not have any software and, therefore, is not subject to a software CCF.
- DCD Tier 2, Sections 7.5 and 7.7 will be updated with additional design information regarding the WDS.

The staff reviewed the RAI response and attached proposed FSAR revisions and found them acceptable. The applicant verified that the WDS is not a software-based device and specifically defined the design function of the WDS which is to disconnect the IFPDs from the DCN-I network when needed by the operator. The proposed changes and new figure of the WDS adequately describe the functionality of the WDS and permit understanding of how the WDS provides its design function. As such, the staff considers RAI 356-7881, Question 07-18, a confirmatory item pending incorporation of proposed FSAR revisions. The staff verified that the proposed markups have been incorporated into Revision 1 of DCD Tier 2 Section 7.5 and Section 7.7. As such, this confirmatory item has been satisfied.

In DCD Tier 2, Revision 3, Table 3.2-1, they identified the Mini LDP, QIAS-N, including its FPD, as associated circuits (see Note N-9). The applicant submitted a supplemental response to RAI 356-7881, Question 07-18 (ML18205A636), to clarify why the QIAS-N is considered an

associated circuit. This response states that although the QIAS-N is classified as a non-safety system because it performs no safety functions, the QIAS-N hardware is qualified as Class 1E and regarded as an associated circuit in accordance with IEEE Std 384. For the power supply design, the QIAS-N is powered form the Class 1E vital bus power supply system without isolation. A dedicated dcircuit breaker in the vital bus power supply system is provided for the feeder of QIAS-N. The staff finds the changes to the DCD is acceptable and does not change the staff's safety conclusions.

7.7.4.6 Core Operating Limit Supervisory System

The COLSS is described in Technical Report APR1400-F-C-NR-14002-, Revision 0, "Functional Design Requirements for a COLSS for APR1400" (hereafter referred to as COLSS TeR). According this technical report, the COLSS was designed to assist operators in implementing technical specification monitoring requirements for LCOs for the following plant parameters:

- DNBR Margin.
- LHR.
- Azimuthal Tilt.
- Axial Shape Index.

The applicant states in DCD Tier 2 Section 7.7.1.4 that the COLSS is an application program implemented within the IPS. The applicant states the following with regard to COLSS:

> The COLSS continuously calculates [DNBR] margin, linear heat rate margin, total core power, core average axial shape index, and azimuthal tilt magnitude and compares the calculated values to the LCO on the parameters. If a LCO is exceeded for any of these parameters, COLSS alarms are initiated and operator action is taken as required by the Technical Specifications.

The applicant also states the following with regard to a potential failure or unavailability of the COLSS:

> If the COLSS is not provided, maintenance of reactor core parameters within the LCOs, as defined by the Technical Specifications, would be accomplished by monitoring and alarming on the separate non-safety-related process parameters used in the COLSS calculations. Therefore, the essential difference in using COLSS in lieu of previous monitoring concepts is the integration of many separate process parameters into a few easily monitored parameters. The conciseness of the COLSS displays on the IPS has distinct operational advantages because the number of parameters that are monitored by the operator is reduced.

The COLSS program is mentioned throughout Chapter 15 and Chapter 16. It is referenced in several LCOs of the technical specifications in DCD Tier 2 Chapter 16. For example, LCO 3.1.7, "Regulating [CEA] Insertion Limits," a reduction in thermal power is a potential action that operators may take in the scenario of the COLSS being out of service (LCO Condition D). For LCO 3.2.1, "[LHR] shall not exceed the limit specified in the COLR," for Condition B, the technical specifications allow "One OPERABLE [CPC] calculated LHR not within region of acceptable operation when the COLSS is out of service."

If the COLSS is out of service, operators would appear to have to manually calculate the LHR trend every 15 minutes, which would present an additional burden to operators. In addition, B 3.2.1, the technical specification bases information for LHR states about COLSS, "The COLSS indicates continuously to the operator how far the core is from the operating limits and provides an audible alarm if an operating limit is exceeded. Such a condition signifies a reduction in the capability of the plant to withstand an anticipated transient, but does not necessarily imply an immediate violation of fuel design limits."

The regulations in 10 CFR Part 50, Appendix A, GDC 19, states in part, that a control room shall be provided with the capability to operate the plant safety under normal and abnormal conditions. The COLSS systems is specifically designed to help operators achieve safe plant operation. The COLSS does not appear to be referenced in DCD Tier 2 Chapter 18, "Human Factors Engineering." There also appears to be a lack of design detail in DCD Tier 2 Chapter 7 to demonstrate that the COLSS has been included as part of human factor analysis. The staff issued RAI 356-7881, Question 07-12, to request the applicant to address the functionality of COLSS in its HFE processes.

In the COLSS TeR, the applicant states that the COLSS is an application program implemented into the "plant monitoring system (PMS)." The PMS is not identified in any portion of DCD Tier 2 Chapter 7, nor anywhere in DCD Tier 1. The staff issued RAI 356-7881, Question 07-12, to request the applicant to describe the PMS and clarify whether this system is a separate system from the IPS or if it is a portion of the IPS.

In the February 18, 2016, response to RAI 356-7881, Question 07-12 (ML16049A328), the applicant provided more information regarding the COLSS. The information provided by the applicant is summarized as follows:

> The PMS, described in the COLSS TeR is a typographical error. In the referenced technical report, the acronym PMS is to be replaced by IPS. This error is corrected within the enclosed markups to this RAI response.

Information provided by the COLSS has been implemented and evaluated based on the HFE Guideline, as described in Technical Report APR1400-E-I-NR-14012, "Style Guide." In addition, information grouping, display format, display elements, and display coding which are described in the HFE Guideline is evaluated in Chapter 18 of this SER.

The staff's full evaluation of the APR1400 design against Technical Report APR1400-E-I-NR-14012 can be found in Chapter 18 of this SER. The applicant has adequately addressed RAI 356-7881, Question 07-12. The applicant has provided corrected design information and enclosed markups to correct the information in the licensing document. The incorporation of the proposed markup into the next revision of relevant licensing documents was a confirmatory item. The staff verified that the proposed markups have been incorporated into Revision 1 of the COLSS TeR. As such, this confirmatory item has been satisfied.

7.7.4.7 Design Basis Information

The SRP Section 7.7 states, in part, that control systems should include the necessary features for manual and automatic control of process variables within prescribed normal operating limits. DCD Tier 2 Section 7.7 describes the automatic and manual control features that allow the non-safety control systems to control process variables within prescribed normal operating limits. The APR1400 design provides controls systems to allow for control of operating

processes for both primary and secondary applications such as reactor power control, turbine control, etc. For example:

- Reactivity control systems – CEAs have both automatic control and manual control available to the operator to maintain reactor coolant temperature and power levels.
- The IFPDs provide soft-key manual controls for the non-safety control system components. Each operator console contains IFPDs and ESCMs.
- COLSS parameters can be accessed from the IFPDs.

7.7.4.8 Safety Classification

The DCD Tier 2 Section 15.0.0.5, "Non-safety-Related Systems Assumed in the Analysis," states, in part, that non-safety systems are not required to mitigate the consequences of events described in Chapter 15 and that only safety-related systems are credited in the APR1400 safety analyses. This is consistent with design information presented in DCD Tier 2 Section 7.7. The staff finds this design commitment adequate as the non-safety control system safety classification is appropriate due to the lack of crediting in Chapter 15 for accident mitigation.

7.7.4.9 Effects of Control System Operation Upon Accidents

The safety analysis considers the effects of control system actions or inactions when evaluating transient response. Manual control mode is assumed if the non-safety control system helps mitigate a given transient. Alternatively, the control system is assumed to be in automatic mode if that operating mode makes the consequences of a given transient worse. Refer to Chapter 15 and Section 7.7.4.17 of this SER for further information.

7.7.4.10 Effects of Control System Failures Caused by Accidents

The applicant states that due to their location in a mild environment, the controllers for the non-safety systems would not be affected by AOOs or PAs. Worst case single failure that would aggravate an accident condition is assumed within the safety analysis. Refer to Chapter 15 and Section 7.7.4.17 of this evaluation for further information.

7.7.4.11 Environmental control systems

The SRP Section 7.7 states, in part, that I&C systems include environmental controls as necessary to protect equipment from environmental extremes (e.g., cabinet cooling fans). The non-safety control system controllers are located in mild environment areas of the plant. The applicant also states in DCD Tier 2 Section 7.7 that environmental controls are provided to protect equipment from environmental conditions such as temperature, humidity, radiation, and ventilation conditions. For example, the IPS cabinets are designed with temperature switches and associated alarms in the MCR to alert operators if cabinet temperatures reach upper level temperature conditions. The applicant does not address specific high cabinet temperatures for other non-safety systems such as the PCS, P-CCS, and DAS. The staff issued RAI 356-7881, Question 07-13, to request the applicant to provide a description of the equipment cabinet environmental protection attributes for the PCS, P-CCS and DAS. Refer to Chapter 9 of this SER for further information on this portion of the review.

In the September 16, 2016, response to RAI 356-7881, Question 07-13 (ML16263A019), the applicant provided more information on the I&C equipment cabinet environmental. The information provided in the applicant's response is summarized in the three tables below.

Table 7.7-8: EQUIPMENT CABINET ENVIRONMENTAL PROTECTIONS – CLASS 1E I&C

Environmental Condition	Environmental Operating Limits Protection
Temperature (°F)	50-104 °F
Relative humidity (%)	7-90 %
Radiation (Gy)	≤ 10 Gy (Gamma)
Note: The Class 1E cabinets located in the MCR and safety-related I&C equipment rooms are designed and fabricated to operate without loss of function when exposed to the environmental design requirements specified in Table 6-1 of the Safety I&C System TeR. The Class 1E cabinets located in the auxiliary building area, except main control room and safety-related I&C equipment rooms, are designed and fabricated to operate without loss of function when exposed to the environmental conditions in this table. For these cabinets, the cooling and ventilation are provided by a fan mounted in the cabinet. Each cabinet contains a temperature sensor in the cabinet that is monitored. The fans are designed for continuous operation when the cabinet is powered. Though an alarm for loss of the fan is not provided, trouble alarms to indicate a high temperature in the cabinet are provided.	

Table 7.7-9: EQUIPMENT CABINET ENVIRONMENTAL PROTECTIONS – NON-CLASS 1E I&C

Environmental Condition	Environmental Operating Limits Protection
Temperature (°F)	50-104 °F in auxiliary building area 70-77 °F in non-safety I&C equipment rooms 65-85 °F for DRCS power cabinets of PCS
Relative humidity (%)	7-90 % in auxiliary building area 40-60 % in non-safety I&C equipment rooms 40-60 % for DRCS power cabinets of PCS
Radiation (Gy)	Negligible
Note: For these cabinets, the cooling and ventilation are provided by a fan mounted in the cabinet. Each cabinet contains a temperature sensor in the cabinet that is monitored. The fans are designed for continuous operation when the cabinet is powered. Though an alarm for loss of the fan is not provided, trouble alarms to indicate a high temperature in the cabinet are provided.	

Table 7.7-10: EQUIPMENT CABINET ENVIRONMENTAL PROTECTIONS – DIVERSE PROTECTION SYSTEM AND DIVERSE INDICATION SYSTEM

Environmental Condition	Environmental Operating Limits Protection
Temperature (°F)	70-77 °F
Relative humidity (%)	40-60 %
Radiation (Gy)	Negligible
Note: For these cabinets, the cooling and ventilation are provided by a fan mounted in the cabinet. Each cabinet contains a temperature sensor in the cabinet that is monitored. The fans are designed for continuous operation when the cabinet is powered. Though an alarm for loss of the fan is not provided, trouble alarms to indicate a high temperature in the cabinet are provided of the fan is not provided, trouble alarms to indicate a high temperature in the cabinet are provided.	

The evaluation in this section is only intended for non-safety control systems environmental protections. The information on environmental protections is for information purposes and is evaluated in other sections of this evaluation. There is no specific guidance or requirements on environmental protection for non-safety I&C systems. However, the applicant's response to the staff's RAI demonstrates that the non-safety I&C cabinets have a comparable level of environmental protection to the safety-related I&C cabinets. The applicant has described the exact operating range of environmental conditions for equipment, the physical methods of providing these protections (e.g., cooling fans, temperature sensors, and alarms) as well as provided information on the safety-related and non-safety systems by which the protections apply. The applicant included enclosed markups that depict proposed changes to relevant licensing documentation and the staff finds these changes, and the overall RAI response acceptable. The incorporation of the proposed markups into the relevant licensing documentation was a confirmatory item. The staff verified that the proposed markups have been incorporated into Revision 1 of the Safety I&C System TeR. As such, this confirmatory item has been satisfied.

7.7.4.12 Potential for inadvertent Actuation

Potential for inadvertent actuation will be addressed in Section 7.7.8.15 of this SER.

7.7.4.13 Independence

Refer to Sections 7.1 and 7.9 of this SER for details on the evaluation of independence.

7.7.4.14 Quality for Control and Diversity and Defense-in-Depth Systems

<u>Credited Diverse Controls</u>

Quality of equipment credited for diverse actions is discussed in DCD Tier 2 Section 7.8. This section also discusses the quality attributes for the various I&C systems and components as follows:

- DMA – The applicant states that the DMA design complies with GDC 1 of Appendix A to 10 CFR Part 50, 10 CFR 50.62, SRM to SECY-93-087, Item 18, II.Q and SRP BTP 7-19. The applicant also states that the DMAs are designed as augmented quality, defined by Generic Letter 85-06. The applicant states that the DMAs are implemented with Class 1E, seismically qualified hardware, in addition to being powered through Class 1E electrical sources.

- DIS – The applicant states that the DIS is designed to be in compliance with GDC 1. The applicant also states that the DIS is designed as augmented quality, as defined by input/output 85-06. DIS software is classified as ITS as per safety class designations in the SPM TeR.

- DPS – The DPS is designed as augmented quality, as defined by Generic Letter 85-06. The DPS software has been classified as ITS as described in the SPM TeR.

The D3 TeR, Revision 0, Section 5, "Diverse Actuation System," states the following with regard to quality:

> The DAS consists of the DPS, DIS, and the DMA switches. Each subsystem is described in the following [sections]. The DAS is implemented on a platform that is diverse from the common safety PLC platform. The DAS is designed to meet the quality assurance guidance of Generic Letter 85-06. Any software associated with the DAS is qualified as ITS.

The DPS, DIS, and DMAs each have an overall safety classification of non-safety and are not required to meet safety-related quality requirements, as described in 10 CFR Part 50, Appendix B. In lieu of Appendix B, the applicant has stated definitively that the quality attributes as defined by Generic Letter 85-06 have been used as a guideline to fulfill quality assurance guidelines for the DAS.

10 CFR 50.62, "Requirements for reduction of risk from [ATWS] events for light-water-cooled nuclear power plants." states in part, that, "…Each pressurized water reactor must have equipment from sensor output to final actuation device,…" and, that this diverse equipment credited to perform a reactor trip, automatic initiation of auxiliary feedwater, and initiation of a turbine trip under ATWS conditions, must be designed to perform its function in a reliable manner. This is applicable to the DAS which contains the DPS. The DPS initiates reactor trip, turbine trip, and auxiliary feedwater under ATWS conditions. Generic Letter 85-06 provides explicit quality assurance guidance as required by 10 CFR 50.62. Generic Letter 85-06 uses 10 CFR Part 50, Appendix B as a reference to provide a framework for non-safety ATWS equipment and compliance to Generic Letter 85-06 provides reasonable assurance of sufficient quality for this equipment. ATWS functions are performed by the DAS (via DPS) and, therefore, is subject to the design and quality requirements of 10 CFR 50.62.

The SRP BTP 7-19, Point 3 states, in part, 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. This information is also adapted from the SRM to SECY 93-087, Section 18, II.Q, Point 3, "Defense Against Common-Mode Failures in Digital Instrumentation and Control Systems." SRP BTP 7-19 goes on to state that:

> If a postulated common-cause failure could disable a safety function that is required to respond to the [DBE] being analyzed, a diverse means of effective

response (with documented basis) is necessary. The diverse means may be an automatic or manual non-safety system if the system is of sufficient quality to perform the necessary function under the associated event conditions and within the required time.

The DCD Tier 2 Table 15.0-13 lists various Generic Letters and bulletins and their disposition for the APR1400 design. Under Generic Letter 85-06, the applicant states that this Generic Letter is not applicant to the APR1400 and is not included with the APR1400 design requirements. This would appear to contradict design commitments made in both FSAR Section 7.8 and the D3 technical report. If Generic Letter 85-06 is not part of any design requirements in the APR1400 design, then it was not clear how the DAS has been design with sufficient quality in order to perform its design functions in a reliable manner. The staff issued RAI 356-7881, Question 07-11, to request the applicant to explain the apparent contradiction in design statements within the FSAR regarding usage of Generic Letter 85-06.

In the March 4, 2016, response to RAI 356-7881, Question 07-11 (ML16064A371), the applicant provided supporting information to resolve the staff's inquiries.

The following was stated, in part, with regard to the design quality of the DAS as well as associated components (i.e., DMA switches):

- The applicant confirms and commits to the DAS being designed with augmented quality as defined by Generic Letter 85-06.

- The DMAs are conventional hardwired switches and classified non-safety. They are implemented by Class 1E devices with environmental qualification in accordance to IEEE Std 323-2003 as endorsed by RG 1.209, Revision 0, and seismic qualification in accordance IEEE Std 344-2004 as endorsed by RG 1.100, Revision 3.

The enclosed markups with proposed changes to the licensing documents reflect the design commitments stated above. Based upon this information, the staff finds that the applicant has adequately addressed RAI 356-7881, Question 07-11. The applicant has confirmed the level of quality design imposed upon the DAS and DMAs by citing NRC-endorsed commensurate to the safety designation of these items. The enclosed markups demonstrate adequate changes to reflect the design commitments to quality design. The incorporation of the proposed changes into relevant licensing documentation was a confirmatory item. The staff verified that the proposed markups have no specific effect on the evaluation content for Section 7.7 and as such, this confirmatory item has been satisfied. Further information can be found in Section 7.8 of this SER.

7.7.4.15 Use of Digital Systems

The SPM TeR describes the design processes the applicant applies to software to ensure quality and reliability. The SPM TeR also describes conformance of the software lifecycle activities to NRC-endorsed standards such as IEEE Std 603-1991, IEEE Std 1074-2006, and IEEE Std 1012-2004 as well as the overall software quality assurance process to meet the requirements of 10 CFR Part 50, Appendix B, which is the safety-related quality assurance criteria. Safety-related software that is developed using a structured design process based on the guidelines described in the SPM TeR would conform to these requirements. The evaluation of the SPM TeR can be found in Section 7.1.4.7 of this SER.

The SPM TeR defines the software lifecycle activities that are applied to software of differing safety class. The activity designations can be found on Table 4-3 of the SPM TeR. Section 2.1 of the SPM TeR defines "ITS" as software whose function is necessary to directly perform DPS control actions, software that is relied on to monitor or test safety critical functions, or software that monitors plant critical safety functions. In a review of the software lifecycle activities and outputs from those activities, the differences between safety critical and ITS amount to the following:

- ITS class software will not have a software safety plan from the software planning phase.
- ITS class software will not have a Module Test (including procedure and report generation) during the implementation phase.

Based upon this table it is clear that safety critical software has the highest level of requirements to be met although ITS software is nearly identical in its requirements. The SPM TeR, Section 5.2, "Verification and Validation Overview," states that for safety critical and ITS class software, the V&V team is organized independently of the design team and that V&V team members shall not have been directly involved in the design of the project. The SPM TeR, Table 5-1 describes the V&V tasks required for software of differing safety class. The differences between safety critical and ITS software includes the following:

- For ITS software, each V&V task for ITS class software shall be performed by the IV&V team, or by the member of the design team who is not directly involved in the software design.
- For ITS software, module testing (including case/procedure/report generation) is not required.
- Unit testing is performed by the design team for ITS software.
- Hazard analysis is not required for ITS software.

The software lifecycle development processes (including V&V activities) for safety critical and ITS software are very similar overall, and in terms of the software design and implementation, nearly identical as described in the SPM TeR. Therefore, if ITS software (e.g., DPS software and DIS software) is developed as per guidance in the SPM TeR, ITS-level software would be developed in a structured process similar to processes applied to safety-related system software. The software portions of both DPS and DIS are designated as ITS.

<u>Credited Diverse Controls</u>

The DCD Tier 1 Section 2.5.2, "Diverse Actuation System," states that the DPS software is implemented according to the software lifecycle process and ITAAC Item 6 under Table 2.5.2-5 captures this design commitment. Section 2.5.2 does not state that for the DIS, its software is implemented according to a software lifecycle process and Table 2.5.2-5 does not contain a commitment to software lifecycle development for the DIS software. The applicant committed to the DIS software being developed under the software lifecycle process documented in the SPM TeR for ITS-grade software, however this commitment has not been captured in DCD Tier 1 and the staff would not have reasonable assurance that this commitment has been met. This issue is covered in Section 14.3.5 of this SER.

Control System Software

The applicant states that the non-safety control system application software is developed using a structured process similar to that applied to the development of the safety-related system software. This quality program, according to the applicant also includes software verification and validation commensurate to the safety class of the control system. Appendix A, Table A-1 of the SPM TeR designates the safety class for the software portions of the following control systems:

- PCS is designated as ITA.
- P-CCS is designated as ITA.

Similar to the software safety classification, ITS, the ITA-level software lifecycle tasks and responsibilities is very similar to that of safety grade software. For ITA software, the applicant does not require a software safety plan, or independence between organizations to perform integration/system testing. Likewise for the V&V specific tasks, there's no requirement for a hazard analysis and strict independence between organizations for specific tasks for ITA software. The SPM TeR defines ITA software as software that is relied upon to maintain operation of plant systems and equipment that are critical to operate the plant. The PCS and P-CCS are non-safety and are not specifically designated for diverse control functionality and the differences between the software development process used to between the control systems, diverse systems and safety-related systems is reasonable given the safety significance between each system. Based upon a comparison of the software lifecycle development process between different software safety classes, the software that comprises both the PCS and P-CCS will be developed in a structured process similar to safety-related system software, which supports the applicant's original assertion.

The software package, COLSS, is not listed on this table for software components that are part of the IPS in Appendix A, Table A-1 of the SPM TeR. The COLSS is listed under the section "Application programs" in DCD Tier 2 Section 7.7. Application programs (i.e., nuclear application programs) are classified as ITA safety class.

Control System Fault Detection Features

Section 4.4.2, "Redundancy," of the CSCCF TeR, states, in part, that the control systems have a comprehensive set of diagnostic features to aid in fault detection as well as locating a repairing technical issues before operational difficulties occur. Controllers that comprise the control system are configured into a "primary/standby" mode of operation. The primary controller is the device that performs normal operational controls. The standby controller would resume control of operational actions in the event of a failure of the primary controller, as well as an alarm. Failure of the standby controller would result in an alarm only. This section did not provide any specific details on the set of diagnostics, nor any design details on the types of failures that would result in a controller swap-over. This section did not provide the general operational aspects of the controllers. Another concern is that, upon a failure of the primary controller, there does not appear to be information in the CSCCF TeR that describes how a faulted controller is prevented from sending potentially erroneous signals onto the communications network. The operational aspects of the non-safety DCS controllers is essential to how the control architecture is implemented, how control functions are performed, and ensuring that design properties support the over CCF Analysis methodology provided in the CSCCF TeR.

The staff issued RAI 68-7892, Question 07.07-4, to request the applicant provide clarification on these topics. In the October 21, 2016, response to RAI 68-7892, Question 07.07-04 (ML16295A268), the applicant provided information regarding the fault detection features. Those features include:

- Status checking of nodes on the control system network (e.g., controllers) – This algorithm access and outputs the contents of any record field in a controller. If an invalid field number is entered, a zero is written to the output points. The date in the record field is then output as a packed point.

- Heartbeat algorithm – Used to monitor heartbeat signals from various controllers. The heartbeat signal is a continuously changing signal, generated and broadcast from each controller. If a heartbeat signal from a particular controller ceases, it sets the corresponding output to one. The monitored heartbeat signal has a value of zero when it's communicating.

- Point Status – This algorithm checks the output state of a point depending upon the point's input state. It compares the state of the input bit and state of the output bit in the "enable mode" of the function block.

Each of these algorithms reside on the individual DCS controllers, but are not specifically credited towards failure types 1, 2, 3 or 4 analyses, discussed later in this evaluation report.

<u>DCS Controller Operation and Redundancy</u>

In the October 21, 2016, response to RAI 68-7892, Question 07.07-04 (ML16295A272), the applicant provided more detail regarding DCS controller operations and implementation. The primary and standby controllers (redundant) are connected by a direct wired connection, which allows for periodic system data updates between the paired controllers. A loss of this connection does not affect the operation of either paired controller or will continued to operate over the DCN-I network but will not be synchronized. The controller that is powered up first becomes the primary controller.

If the primary controller fails, the watchdog detection circuitry disables the input/output interface of the primary controller. The watchdog alerts the backup controller of this operation, wherein the backup controller proceeds to take control of the input/output bus interface and begins to execute the process control program and broadcasts over the DCN-I network. The faulted controller will also enter into a state where all its operations are ceased and can only responds to diagnostic inquiries. This failure behavior ensures data network is protected as the faulted controller has its input/output interface disabled such that no potential erroneous data is passed onto the network. Events that can trigger an automatic swap-over between redundant controllers include the following.

- Internal check failure,

- Loss of network communication,

- Spurious reboot, and

- Watchdog timer overrun.

Alarms for faulted controllers are displayed on the IFPDs. Based upon the applicant's response, the staff finds the applicant's response adequate. The applicant has provided a sufficient level of design detail on the existing fault detection features of the DCS so as to ensure that fault detection for the various portions of the non-safety I&C will be alerted to operators. The response also provides an adequate level of detail to ensure that the fault detection feature described in the response are germane to its operation and adequately support the CCF analysis documented in the CSCCF TeR, Section 4.4.2. The enclosed markups contain proposed changes to relevant licensing documentation to describe the key features in the design that address fault detection in the DCS. The incorporation of the proposed changes to the next revisions of the relevant licensing documentation was a confirmatory item. The staff verified that the proposed markups have been incorporated into the CSCCF TeR, Revision 1. As such, this confirmatory item has been satisfied.

Broadcast Storms (Data Storms) CCF

Broadcast Storms on DCN-I Network

Section 4.4.5 of the CSCCF TeR describes design features and measures that protect against CCF affecting the DCN-I due to data storms. The applicant states that a data storm can originate from any controller, IFPD, or server on the network. Should a data storm occur over the DCN-I network, operators will be able to use the divisionalized ESCMs on the safety console that do not have IFPD connections.

Broadcast Storms on IFPD/ESCM Ethernet Networks

Ethernet protocol is used to connect IFPDs to the ESCMs. Each operator console has a separate Ethernet network. According to the applicant, the interconnected IFPDs and ESCMs could become unstable, displaying erratic behavior on screen. CPU capacity for the IFPDs/ESCMs may be stressed due to overload of data, leaving insufficient capacity to execute selected functions by operators. Due to operator consoles having separate Ethernet networks with associated IFPDs/ESCMs, this failure is limited to the affected equipment.

The applicant did not appear to address other design attributes in place to cope with, mitigate, or prevent excessive network traffic. The applicant also did not appear to describe the adequacy of operator actions to address loss of functionality at the consoles. The staff issued RAI 68-7892, Question 07.07-6, to request clarification on these topics. In the October 18, 2016, response to RAI 68-7892, Question 07.07-6 (ML16292A478), the applicant stated, that the DCN-I is designed such that network traffic cannot exceed more than 60 percent of bandwidth in order to ensure minimal delays in message delivery. Operational procedures will also be in place to guide operator actions in the instance that a connected IFPD/ESCM network is malfunctioning.

Table 07.07-4: Protective Features of the DCN-I Network against Data Storms[5]

Equipment	Protective Feature
DCN-I Network Switches	Rapid spanning tree protocol – If more than one path occurs between two ports on a network, this creates a potential vector to data storms as these redundant paths between ports can loop infinitely, creating data storm.

[5] Source: CSCCF TeR

Equipment	Protective Feature
	The rapid spanning tree protocol blocks communications on redundant network switch paths (ports), thus eliminating network loops (bridge loops) until the active link loses connectivity, and reconfigures the network to use the redundant path.
DCN-I Network Switches	Automatic disabling of packet-forwarding – If a port experiences a higher than expected amount of network traffic, its packet-forwarding functionality is disabled until traffic falls below desired threshold.
DCN-I Network Switches	CRCs – Verifies data integrity for received data packets. If a networked device (e.g., controller) transmits erroneous data, the network switch disables the port for which the failed device is connected to the network.
DCS Controllers	”Quiet Mode” – When a controller detects excess network traffic, it enters this mode of operation, which prioritizes essential network communications to ensure control software functions is properly achieved. Not specifically credited towards broadcast storm mitigation to support CCF analysis.

In addition to the information provided in Table 07.07-4, above, the applicant also stated in its response to RAI 68-7892, Question 07.07-6, that the worst case non-safety I&C equipment failure due to excessive network traffic is bounded within Failure Type 3, analyzed in Section 5.3 of the CSCCF TeR. A failure of the DCN-I network by itself, is considered a single failure of the non-safety I&C components. Regarding operator actions in the presence of a CCF affecting non-safety networks, the applicant states that systemic failure and degraded conditions will be included in HFE V&V scenarios to evaluate the integrated design to determine whether it conforms to accepted human factors design principles such that personnel can successfully perform their tasks. Refer to Section 4.1.1, “Sampling Dimension,” of the Human Factors V&V Plan TeR.

The staff finds the applicant’s response to RAI 68-7892, Question 07.07-6, is adequate because the applicant provided sufficient design information to demonstrate that there are adequate protections built into the non-safety network apparatus and equipment, as well as ensuring that operators are alerted to failures in this area and have alternative options to control the plant. There is redundancy in non-safety operation control as well as independent, safety-related control capability available to operators. The enclosed markups are also acceptable as they adequately depict the updated design information presented in the applicant’s response. The incorporation of the proposed changes into the relevant licensing documents was a confirmatory item. The staff verified that the proposed markups have been incorporated into Revision 1 of the CSCCF TeR and the Safety I&C System TeR. As such, this confirmatory item has been satisfied.

Control of Safety Components from the Non-Safety DCS

Section 4.9 of the CSCCF TeR describes non-safety control signals that are sent to ESF-CCS. Table 4.9-1, “Non-safety Control Signals sent from P-CCS to ESF-CCS,” of the CSCCF TeR, also purports to show the non-safety control signals sent from P-CCS to ESF-CCS. These non-safety signals are used to control safety components during normal operations. The

applicant states in Section 4.9 of the CSCCF TeR that the P-CCS only sends a few signals. However, it was not clear to the staff if these non-safety control signals sent to ESF-CCS, described in Section 4.9 are the only signals that are sent. Figure 4.1-1, "Credible Failure Boundary of Control System CCF," shows network connectivity between the IFPDs/ESCMs to the safety data network, with no apparent restrictions on the amount of safety components 'controlled' by IFPDs. The staff issued RAI 68-7892, Question 07.07-8 to clarify what is the level of control enabled in the non-safety DCS to control safety-related I&C components.

In the September 20, 2016, response to RAI 68-7892, Question 07.07-8 (ML16264A400), the applicant provided more information on what control of safety-related I&C equipment is enabled within the non-safety I&C systems.

- The applicant affirms that Table 4.9-1 of the CSCCF TeR contains a list of all safety functions and safety related devices that can be controlled from non-safety controllers via the P-CCS. However, the revised version of this table, as enclosed in this RAI response, added a significant number of components such as class 1E 4.16kV system unit auxiliary transformer and standby auxiliary transformer circuit breakers.

- The manual control signals from the IFPDs are sent to the DCS controllers to control non-safety components but these signals do not affect safety components.

- The IFPDs do not directly or indirectly control safety-related components/functions except for those defined in Section 4.9 of the CSCCF TeR. This would not include those components described on Table 4.9-1.

The CCF analysis as documented in the CSCCF TeR includes as part of its scope, the potential failures that could be induced into the safety class systems due to failure of non-safety systems or devices. Control signals documented in Section 4.9 of the CSCCF TeR are accounted for in this analysis. This portion of the evaluation does not consider the efficacy of the ability of control of safety functions and devices from non-safety devices. Rather, this portion of the evaluation determines whether this control configuration has been evaluated for potential failure effects and how this configuration is implemented. Based upon this RAI response, the applicant has adequately demonstrated this control configuration is evaluated in the CCF analysis as described in the CSCCF TeR and how this configuration is implemented. Based upon the clarifications provided in the applicant's response to the staff's request, in addition to the enclosed markups, the staff finds the applicant has adequately addressed RAI 68-7892, Question 07.07-8. The incorporation of the proposed markups into to the next revision of relevant licensing documentation was a confirmatory item. The staff verified that the proposed markups have been incorporated into Revision 1 of the CSCCF TeR specific to this RAI response. As such, this confirmatory item has been satisfied.

7.7.4.16 Control of Access

Refer to Section 7.1.4.13 of this SER for information on this topic.

7.7.4.17 Effects of Control System Failures

IEEE Std 603-1991, Clause 5.6.3 states, in part, that the safety system design shall be such that credible failures in and consequential actions by other systems, as documented in Clause 4.8 of the design basis section of this standard, shall not prevent the safety-related systems from meeting the requirements of this standard. One of the other systems documented

in Clause 4.8 is non-safety systems. The failure(s) of non-safety control systems or components have the potential to challenge safety-related systems and overall plant safety, as demonstrated by the various non-safety system or component failures that are analyzed in the Chapter 15 safety Analyses (e.g., loss of feedwater, rod ejection). Failure(s) of non-safety systems or components, when taken individually, are typically addressed by automated safety system actuation such as reactor trips or ESFAS actuations, or in other cases, by operator actions.

Modern I&C systems challenge the appropriateness of these traditional measures due to way these modern systems are designed and configured. For the APR1400 design, the non-safety control systems, like other modern I&C systems, has a common software platform by which all of the non-safety controls and indications, are implemented. The common software platform, along with other commonalities and dependencies (due to common software platform being part of a [DCS]) suggests that a postulated failures within the non-safety control systems may not necessarily be limited to a single function or component. In this scenario, CCFs takes on added significance as a common trigger has a greater potential for propagation. In addition, there is no presumption of high quality design, testing, V&V for the non-safety control systems.

The CSCCF TeR provides information to demonstrate that the APR1400 design adequately accounts for postulated failures in the non-safety I&C systems and component and the potential effects on plant safety. The report provides a comprehensive methodology to address postulated CCF in non-safety I&C systems and components. The methodology incorporates quantitative and qualitative analytical techniques in order to provide full coverage to the entirety of the non-safety I&C systems. The methodology is intended to cover the postulated failure effects of both functions and components.

7.7.4.17.1 Scope of Analysis

According to the applicant, both the primary and secondary non-safety systems are addressed by the CCF analysis. The applicant states the following with regard to non-safety systems that are not considered within the scope of the evaluation.

> Monitoring systems such as [NIMS] and [RMS] which are not used for maintaining controlled variables within prescribed operating ranges of the plant are not considered for evaluation.

The applicant does not specifically call out the exact number and/or types of systems that are considered for this evaluation. It must be assumed that, based upon this quote, the only criterion used to determine whether a system is included in the scope of this evaluation is if the system is responsible for controlling variables within pre-defined operational ranges. This criterion would appear to be arbitrary as the applicant does not provide any further evidence to support this criterion. The staff issued RAI 356-7881, Question 07-09, to gain further clarity on the process the applicant used to determine the evaluation scope.

In the April 7, 2016, response to RAI 356-7881, Question 07-09 (ML16098A336), the applicant provided information to resolve the staff request.

The applicant stated, in part, the following, within the RAI response.

- All control systems of the primary and secondary systems of the APR1400 design are included in the evaluation for CCF.

- Control systems are included in the evaluation (scope) if their failures can affect critical safety functions. The critical safety functions are based upon the whether the system can affect the following:
    - Reactivity,
    - RCS pressure,
    - RCS temperature,
    - RCS flow, and
    - RCS inventory or integrity (fuel cladding).
- The evaluation acceptance criteria based upon the critical safety functions, as presented in DCD Tier 2 Section 15.0 are considered to determine the limiting initiating events for the control system CCF analysis:
    - Challenge to fuel cladding integrity,
    - Challenge to primary system integrity,
    - Challenge to offsite dose limit, and
    - Challenge to containment integrity.
- Monitoring systems such as NIMS and RMS are not included in the evaluation (scope) because their failures cannot challenge fuel cladding integrity or primary system integrity.

The applicant clarified that all I&C systems are considered within the evaluation scope but only those I&C systems that can affect critical safety functions will be within the scope of the CCF evaluation. The applicant provided "Table 1" within its response to RAI 356-7881, Question 07-09, which describes the process for how the applicant screens I&C systems based upon if its operation affects a critical safety function. In the December 2, 2016, response to RAI 522-8633, Question 07.07-20 (ML16098A336), the applicant committed to the following in support of its response to RAI 352-7881, Question 07-09:

- "Table 1" screening results table will be included in the CSCCF TeR.
- The applicant committed that there are no failures among the non-safety controllers that could block or inhibit any safety function.

The enclosed attachments to the responses to both RAI 352-7881, Question 07-09; and RAI 522-8633, Question 07.07-20, adequately describe the inclusion of proposed revisions and corrections to the relevant licensing documents based upon the information provided by the applicant in these RAI responses. Based upon this, the staff finds the applicant has adequately addressed RAI 352-7881, Question 07-09; and RAI 522-8633, Question 07.07-20. The applicant has adequately described how various I&C systems are directly included within the scope of the CCF analysis based upon critical safety function applicability and the acceptance criteria based on this applicability. As stated above, the applicant provided markups in both

RAI responses that demonstrate inclusion of new design information into the relevant affected licensing documents. The incorporation of the proposed markups into the next revision of relevant licensing documentation was a confirmatory item. The staff verified that the proposed markups have been incorporated into Revision 1 of the CSCCF TeR. As such, this confirmatory item has been satisfied.

The applicant provides four groupings and associated acceptance criteria for its evaluation of control system CCF (CSCCF).

Table 7.7-5: Failure Groupings and Acceptance Criteria for CCF Evaluation

Failures	Failure Scope	Acceptance Criteria for Evaluation
Type 1	Multiple function failures due to a single failure of a shared signal	AOOs as evaluated in FSAR Chapter 15 Safety Analysis
Type 2	Multiple failures of a single control group due to CSCCF	AOOs as evaluated in FSAR Chapter 15 Safety Analysis
Type 3	Multiple failures of more than one control group due to CSCCF	PAs as evaluated in FSAR Chapter 15 Safety Analysis
Type 4	Multiple failures of IFPD control commands due to CSCCF	PAs as evaluated in FSAR Chapter 15 Safety Analysis

In addition, Table 5.1-1, "Shared Signals," presents a list of common signals from specific primary/secondary controls systems and interfacing systems that receive the common shared signal. The entirety of the analysis, the applicant's basis appears to limit initiators of CCFs to that of shared signals. The applicant does not provide a basis as to why this failure mode is the sole means to cause a CCF. For example, upon reviewing the technical report, the applicant does not appear to consider other potential failure modes such as EMI/RFI, seismic movement, etc. It is possible that the four failure categories, supporting design constraints, and analysis bound all failure modes beyond that of shared signals but the applicant does not make this claim or any arguments to support this premise within the CSCCF TeR. The staff issued RAI 356-7881, Question 07-10, request the applicant justify why shared signals are the only failure mechanism considered when determining the above four failure categories.

In the October 12, 2016, response to RAI 356-7881, Question 07-10 (ML16286A678), the applicant provided information to resolve the staff request.

The following information summarizes the applicant's response:

- The EMI/RFI qualifications of all DCS controllers are considered in the design, however, specific conformance of the non-safety systems to any endorsed guidance such as SRP BTP 7-18, "Guidance on the Use of Programmable Logic Controllers in Digital Computer-Based Instrumentation and Control Systems," and RG 1.180, Revision 1, is not required. This is augmented by the consideration that non-safety systems are not credited in the Chapter 15 safety analysis if the control system failure does not make the consequences of a transient worse.

- If EMI/RFI affects a single control group, this is considered bounded by Failure Type 2. Failure Type 2 considers failures of multiple digital and analog output modules which can all be affected by software CCF. Therefore, Failure Type 2 is considered equivalent to failure of multiple hardware failures in a control group as it would then be bounded by the evaluation of a software CCF of the single control group. This also means that malfunctions as a result of EMI/RFI will be bounded by the criterion that is already established for this failure type if EMI/RFI effects are limited to a single control group.

- If EMI/RFI affects multiple control groups, this is considered bounded by Failure Type 3. This also means that malfunctions as a result of EMI/RFI will be bounded by the criterion that is already established for this failure type.

- Non-safety controllers are not required to be seismically qualified, however a seismic event can cause multiple failures in all control groups. Based upon the effects of seismic failure, the applicant states that Failure type 3 is bounding. Seismically-induced failures would essentially be another type of causal factor for multiple controller failures across multiple control groups, thereby being enveloped by the failure type 3 pre-established evaluation criteria.

The enclosed markups also include proposed changes to the CSCCF TeR. The applicant proposed to add information that confirms that EMI/RFI and seismic effects are considered in the analysis and enveloped by the analysis even though specific conformance to guidance on these topics is not required for non-safety systems. Based upon the above information, the staff finds the applicant has adequately addressed RAI 356-7881, Question 07-10. The applicant has adequately demonstrated how different types of causal factors for failure such as hardware failures, EMI/RFI effects, and seismic effects are enveloped by the pre-established failure types. The incorporation of the proposed markups into the next revision of relevant licensing documentation was a confirmatory item. The staff verified that the proposed markups have been incorporated into Revision 1 of the CSCCF TeR. As such, this confirmatory item has been satisfied.

7.7.4.17.2 Design Features

As described in the CSCCF TeR, the non-safety systems include a number of inherent design features to reduce the likelihood of a CSCCF or to reduce potential fault propagation in the event of a CSCCF.

<u>Segmentation</u>

The applicant defines segmentation as a process that separates and groups components, including instruments and control functionality in a non-safety DCS controller. This definition describes the allocation of functions to various controllers in a systematic way, within a DCS. The allocation includes the allocation of functions (e.g., monitoring, control) as well as specific input/output modules (e.g., boards, base modules). The applicant credits the segmentation arrangement to limit the effects of failures due to a software defect to a single controller, regardless of the defect existing in other controllers through demonstrating differences in controller inputs and native application programs. From this, the applicant states that it is unlikely that a common trigger, such as a shared signal input, would affect multiple controllers concurrently.

The applicant appears to be making the argument that the segmentation arrangement adds or enhances the amount of diversity between controllers or controller groups, but does not state this explicitly. The applicant also does not cite any probabilistic data that could supplement design claims when using terms such as “likelihood” or “highly unlikely.” This portion of the evaluation will not address the veracity of terminology germane to probabilities as they do not necessarily affect or invalidate the applicant’s design claims regarding the physical arrangements and attributes of the non-safety DCS to provide barriers against CCF.

The staff issued RAI 68-7892, Question 07.07-2, to request the applicant to explain why there are the differences in controller group arrangements between DCD Tier 1 Table 2.5.5-1, and Table 5.2-1 of the CSCCF TeR. In the November 3, 2015, response to RAI 68-7892, Question 07.07-02 (ML15307A683), the applicant addressed the staff’s concern regarding why the content of DCD Tier 1 Table 2.5.5-1, “Controller Group Arrangement of the PCS and NPCS,” did not appear to align with Table 5.2-1, “Control Group Segmentation,” of the CSCCF TeR. Specifically, the control systems detailed in Table 5.2-1 appears to have a wider range of systems as compared to Table 2.5.5-1. It appears that Tier 1 content is not reflective of the basic design of the overall control system physical arrangement and doesn’t include all control systems, with no explanation as to why this is the case. In the RAI response, the applicant stated that DCD Tier 1 Table 2.5.5-1 only showed the ‘major’ controllers groups and not the entirety and this appears to be an oversight on the part of the applicant. The applicant stated that DCD Tier 1 Table 2.5.5-1 will be revised to align with Table 5.2-1 to accurately describe all non-safety control system groups. The staff finds this change adequate. The incorporation of the proposed markups into the next revision to DCD Tier 1 was a confirmatory item. The staff verified that the proposed markups have been incorporated into Revision 1 of the CSCCF TeR and DCD Tier 2 Section 7.7. As such, this confirmatory item has been satisfied.

<u>Functional and Component Grouping</u>

The segmentation arrangement has two specific designations:

- Functional grouping – Establishes groupings consistent with the functional boundaries of the systems.

- Component groupings – This is a secondary grouping designed to further pair group components consistent with functional plant processes.

Both functional and component groupings are not credited in the analyses germane to Failure types one through four, as shown on Table 7.7-5 of this safety evaluation. The functional and component groupings are distinct from functional and component segmentation as well as addition segregation of components. According to the applicant, functional and component segmentation are credited towards the analysis for Failure Types 1 and 2.

Power Source Segregation

Table 7.7-6: Power Source Allocation for non-safety systems[6]

Division of Power	Channel Designation
Non-Safety 'A'	AB (N1)
Non-Safety 'B'	BB (N2)

The applicant states that all controllers are redundant and powered from two separate power sources within the same electrical division, thereby ensuring a failure of one power source does not have an adverse effect on any control functions. As these are non-safety control functions and applications, they are not required from a safety standpoint. This power source arrangement is beneficial as it provides some protection in the event that potential loss of power scenario causing an unintended control system action but is more likely the case that this arrangement provides enhanced availability which is in alignment with the software safety class designation (important to availability as defined by the software program manual).

Functional and Component Segmentation

The TCS would comprise a control group or 'segment' within the DCS. This would appear to be specific to the application software of the TCS being distributed to a specified segment of the DCS. Component segmentation goes further by designating connections from the physical portions of the control systems (e.g., sensors) to different control groups. Figure 4.5-5 of the CSCCF TeR shows a type of signal transmission between various controllers for a sample type of component segmentation. The applicant's description of this communication path was not clear compared to design descriptions in other portion of the technical report with regard to the controllers. The staff issued RAI 356-7881, Question 07-15, to gain clarity on this point and request the applicant provide more information on how interlocks/permissives are accounted for within the segmentation arrangements. The staff issued RAI 356-7881, Question 07-16, to request the applicant to provide more clarity on how component segmentation is applied after functional segmentation is completed.

In the March 4, 2016, response to RAI 356-7881, Question 07-15 (ML16064A371), the applicant provided more information on controller communications as well as interlock implementation within the segmentation arrangements.

The applicant states, in part, the following in the response:

- The dotted line between control groups in Figures 4.5-5 and 4.5-6 of the CSCCF TeR is only intended to show signal transmission and does not mean a bi-directional communication path. Hardwired interface and communication path between control groups are possible, however, communication between the controllers take place over the DCN-I.

- As identified in Table 5.1-1, Note 2 of Technical Report the CSCCF TeR, data communications are not used for signal transmission between control groups of the PCS and NPCS. The SBCS main and permissive control groups are a subset of NPCS, as

[6] Source: CSCCF TeR

identified in Section 4.2 of the CSCCF TeR. Therefore, the signals between SBCS main and permissive/interlock controllers are hardwired.

- There are three control groups for the high pressure feedwater heaters. One control group of the high pressure feedwater heater has no signal transmission with the other control groups as identified in Table 5.2-1 of the CSCCF TeR.

The applicant also stated the following:

> The permissive/interlocks related to the SBCS are on separate controllers from the SBCS main functions. Conversely other system interlocks such as CEA withdrawal prohibit are provided from separate safety/non-safety controllers and are generated through the DRCS controllers for which the functions reside. Because interlocks in the CSCCF TeR, Table 4.7-1 are generated by the DRCS and because they can be affected by a software CCF (because the interlocks reside on the same controllers as the main functions) they are not credited for the evaluation of DRCS control group failure.

Based upon the design detail provided in the applicant's response, as well as the enclosed markups in the response, the staff finds the applicant has adequately addressed the staff's request. The applicant has adequately clarified the types of communications taking place, if any, between controllers in the DCS and how permissive/interlocks signals are transmitted between controllers. The applicant has also adequately clarified that for the subsystems with specific permissives/interlocks the segmentation arrangements, and associated evaluation crediting are different between the SBCS and DRCS. A review of the enclosed markups demonstrates that proposed changes to the CSCCF TeR are adequate. The incorporation of the proposed markups into the next revision to the CSCCF TeR was a confirmatory item. The staff verified that the proposed markups have been incorporated into Revision 1 of the CSCCF TeR. As such, this confirmatory item has been satisfied.

In March 4, 2016, response to RAI 356-7881, Question 07-17 (ML16064A371), the applicant provided more information on its component segmentation application. Regarding component segmentation the applicant stated, in part, that additional component segmentation is applied to reduce the likelihood of potential failures, based on the evaluation results of Failure Types 1 and 2, as described in the CSCCF TeR, Section 2, Revision 0, and after functional segmentation is applied. As described in the CSCCF TeR, Section 4.5, "Segmentation," there are two types of component segmentation, denoted simply as 'Component Segmentation 1' and 'Component Segmentation 2'. The additional application of component segmentation (after functional segmentation is applied) ensure that the evaluation results of Failure Types 1 and 2 are bounded by DCD Tier 2 Chapter 15 acceptance criterion. The significance of this application is that:

- Component segmentation 1 is applied in addition to functional segmentation if Failure Types 1 and 2 results are NOT bounded by Chapter 15 acceptance criteria

- Component segmentation 2 is applied within the control function itself, and is not necessary to bound evaluation results but adds additional conservatism to the analysis as well as support limitation of the effects of postulated control group failure, as described in Section 4.5.5 of the CSCCF TeR.

The applicant also clarified what forms of segmentation would be appropriate to apply to Failure Types 1 and 2:

- Failure Type 1 evaluates the effects of shared signal failure (i.e., erroneous signal) within a control group(s). Functional and component segmentation are credited in limiting the effects the failure to the functions existing on the affected controller. This is not specific to a software defect being the causal factor.

- Failure Type 2 evaluates the effect of a software defect or software CCF of a single control group. Both types of segmentation are also credited here to limit the effects of the software defect by virtue of the segmentation types providing controllers with different inputs and application software configuration such that the potential for a common trigger affecting a software defect on multiple controllers concurrently is reduced.

Both types of segmentation can be applied depending on the results of the evaluation for both Failure Types 1 and 2. Based upon the applicant's response, and the attached markups, the staff finds the applicant has adequately addressed RAI 356-7881, Question 07-17. The applicant has adequately clarified what specific criterion is used to determine whether component segmentation is needed or not, which is based upon evaluation results after the application of functional segmentation. The applicant has also adequately clarified how segmentation is applied while performing evaluations for both Failure Types 1 and 2. The attached technical report markups adequately represent the applicant's clarifications. The incorporation of the proposed markups into the next revision of the CSCCF TeR was a confirmatory item. The staff verified that the proposed markups have been incorporated into Revision 1 of the CSCCF TeR. As such, this confirmatory item has been satisfied.

The CSCCF TeR, Section 4.5, "Segmentation," describes the grouping of control functions and components into segmented arrangements that directly support the quantitative and qualitative analysis provided in this report to address the safety issue of postulated failure(s). DCD Tier 1 Table 2.5.5-2, "Control System Not Required for Safety ITAAC," of DCD Tier 1, ITAAC Section 2.5.5, "Control System Not Required for Safety," did not provide an ITAAC item that verifies that these segmentation arrangements have been adequately implemented to support the safety case made within the CSCCF TeR. The verification of the segmentation arrangements are essential to ensure the programming and implementation of the functional and component segmentation as shown in the technical report be verified in order in order to maintain the validity of the CCF quantitative and qualitative analysis. In RAI 68-7892, Question 07.07-3, the staff requested the applicant provide an ITAAC that verifies the segmentation arrangements for the non-safety system as described in the CSCCF TeR, Section 4.5.

In the October 11, 2016, response to RAI 68-7892, Question 07.07-3 (ML16285A534), the applicant stated:

> To verify that the implementation of functional segmentation and component segmentation arrangements have been performed according to the CSCCF TeR, DCD Tier 1, Section 2.5.5.1 and Table 2.5.5-1 will be revised as shown in the attachment associated with the response to RAI 68-7892, Question 07.07-2.

The staff reviewed the applicant's November 3, 2015, response to RAI 68-7892, question 07.07-02 (ML15307A683), and found it acceptable for RAI 68-7892, Question 07.07-3, because

the response to RAI 68-7892, Question 07.07-2, contained the requested ITAAC. In the response to RAI 68-7892, Question 07.07-2, the applicant provided updates for both DCD Tier 1 Table 2.5.5-1 and Table 2.5.5-2 that demonstrate that the separate control groups as described in the CSCCF TeR, Section 4.5 are adequately described in DCD Tier 1 as well as verification of the controller arrangement by revision of ITAAC related to segmentation on Table 2.5.5-2. The staff finds the applicant's response to RAI 68-7892, Question 07.07-3 adequate and considers this RAI a confirmatory item pending inclusion of proposed changes into applicable licensing documentation. The staff verified that the proposed markups have been incorporated into Revision 1 of DCD Tier 1 Section 2.5.5. As such, this confirmatory item has been satisfied.

Additional Design Features

The non-safety control system DCS, in addition to the segmentation arrangement, also comes with some of the following design features:

- Redundant controllers (for increased availability),
- Interlock/permissives on separate control groups,
- Control signal validation,
- Redundant analog input with auto signal selection algorithms,
- Hardwired signal interface between control group within PCS and NPCS, and
- Diagnostic and alarming functions.

Section 4.6 of the CSCCF TeR, the applicant identifies the following functions as having completely redundant control loops with redundant controllers and two input/output modules, with the input/output modules operating concurrently for each control loop:

- Control logic for RCPs,
- Control logic for non-Class 1E 13.8 kV switchgear power circuit breakers, and
- Control logic for non-Class 1E 4.16 kV switchgear power circuit breakers.

The applicant does not explain why these specific control functions were described in this way, considering this type of control loop configuration would appear to be applicable to the entirety of the DCS, based upon design descriptions of the DCS in other areas of the licensing documentation. The staff issued RAI 356-7881, Question 07-16, to request the applicant to clarify if the input/output configuration for the above-mentioned functions is only applicable to those functions, and why is that the case. In the May 5, 2016, response to RAI 356-7881, Question 07-16 (ML16126A066), the applicant provided the referenced control logic configurations.

The applicant states, in part, the following regarding control loop configurations:

- Each controller for the PCS and P-CCS is provided a redundant processor, power supply and data communication network.

- For the NSSS, PCS and NPCS, and associated subsystems, a redundant control loop and control signal validation design is used as identified in Section 4.8, 5.1.1 and Figure 4.1-3 of the CSCCF TeR.

- For the RCP and BOP control functions, the completely redundant control loop design is applicable to only three control logics mentioned in Section 4.6 of the CSCCF TeR. In this case, each redundant controllers is provided with redundant input/output modules to enhance availability. The other BOP control loops do not have redundant input/output modules.

The applicant also clarified the reasoning behind the RCP and specific BOP control function loop configurations with the following explanations:

- Control logic for RCPs – RCPs are essential non-safety components that may significantly affect plant availability.

- Control logic for non-Class 1E 13.8 kV and 4.16 kV switchgear power circuit breakers – The failure these control loops can lead to the loss of non-safety main power.

Based upon the information the applicant provided in its RAI response, as well as attached markup revisions to the CSCCF TeR, the staff finds that the applicant has adequately addressed RAI 356-7881, Question 07-16. The applicant provided an adequate summary of the differences in control loop configurations for non-safety systems. In addition, the applicant has provided an adequate explanation of why RCP control loops and switchgear control loops have full redundancy versus other non-safety functions. The applicant cited plant availability and the potential for plant-wide perturbations based on failure for those particular non-safety systems as basis for why redundant control loops are implemented for provision of additional protections. The enclosed markups with the design information provided in the response are also adequate. The staff incorporation of the proposed markups into the next revision of the CSCCF TeR was a confirmatory item. The staff verified that the proposed markups have been incorporated into Revision 1 of the CSCCF TeR. As such, this confirmatory item has been satisfied.

Non-Safety Control Signals Sent to ESF-CCS

Section 4.9 of the CSCCF TeR describes non-safety control signals that are sent to the ESF-CCS. This is done because there are safety components that are used by the control system during normal operations. The evaluation of the spurious operations of these safety components due to control system failure, refer to Section 7.7.4.14.1 of this SER. Also refer to Section 7.9 of this SER for the review on independence.

CCF Analysis of Embedded Devices in Field Equipment

The applicant provided an evaluation of potential consequences of a CCF of field equipment that uses embedded digital technology. The applicant asserts that the quantitative analysis provided in Section 5 of the CSCCF TeR is bounding for postulated failure modes due to embedded digital technology. The evaluation of the quantitative analysis provided in the CSCCF TeR can be found in Section 7.7.4.14.1 of this SER.

Embedded Digital Devices

In Section 4.10 of the CSCCF TeR, the applicant addresses embedded digital technology as part of the overall evaluation of CCF for the non-safety control systems design. In this section, the applicant states, in part, that Embedded Digital Devices (EDD) in non-safety field devices have no potential to cause CCF of both safety-related and non-safety systems. The applicant states that EDDs used in non-safety field devices are different from those used in safety-related systems or safety-related system field components. The applicant did not provide specific evidence to support this claim as this design claims implied that EDDs that exist in both non-safety and safety field components are diverse from one another. The staff issued RAI 522-8633, Question 07.07-18, to request the applicant to provide more evidence to support its claims regarding EDDs in the APR1400 design.

In the December 1, 2016, response to RAI 522-8633, Question 07.07-18 (ML16336A827) [a follow up to RAI 352-7881, Question 07-08 (ML16342A998)], the applicant provided the following commitments and clarifying information:

- EDDs contained within field devices in non-safety applications are diverse from EDDs contained in field devices for safety-related applications.
- The PCS and NPCS, which have major control functions of the NSSS do not have EDDs in the field.

The table below provides specific information on the types of EDDs used and what types are common between safety-related and non-safety systems and how the applicant intends to prevent the potential for CCF between the devices:

Table 7.7-7: Embedded Digital Device Diversity Application for Non-Safety Field Components[7]

Device Type use in Non-Safety System	Also Used in Safety Systems?	Diversity Attribute
SMART Transmitter	No	Diversity does not need to be considered
Ultrasonic Level Transmitter	Yes	Diversity is achieved by using different and diverse manufacture's designs for safety-related and non-safety applications
Ultrasonic Flow Transmitter	No	Diversity does not need to be considered
RMS Computer and Interface portion within local unit	No	Diversity does not need to be considered

[7] Source: Response to RAI 522-8633 Question 07.07-18 (ML16336A827)

Note that the full evaluation of diversity in the APR1400 design is located in Section 7.8 of the SER. Based upon a review of the RAI responses as well as enclosed markups of proposed revisions to relevant licensing documentation, the staff finds the applicant has adequately addressed the staff's requests. The applicant has committed that EDD types that are common to both safety-related and non-safety applications are diverse from one another so as to eliminate a potential CCF from affecting both. The applicant has also provided evidence to support this claim, but the applicant did not provide a Tier 1 ITAAC item to verify the design commitment of EDDs used in non-safety applications will be diverse from EDDs used in safety applications. The applicant also did not provide revised markups of the D3 TeR for the inclusion of this design commitment. This would appear to suggest that the applicant has not incorporated EDDs into its overall diversity analysis considerations in order to demonstrate to staff that EDD usage complies with applicable requirements and guidance. This correlates with the lack of any specific information in the licensing basis that describes how EDD usage complies with applicable diversity rules and guidance. The enclosed markups provided in the response to RAI 352-7881, Question 07-08, demonstrate that the applicant has proposed updates to the relevant licensing documentation to reflect the design commitments made in this RAI response as well as the inclusion of supporting evidence for the design commitments but do not describe an ITAAC to verify design commitments or how EDDs comply with applicable diversity guidance. The inclusion of the proposed markups provided in the response to RAI 356-7881, Question 07-08, into the next revision of relevant licensing documentation was a confirmatory item. The staff verified that the December 7, 2016, RAI 356-7881, Question 07-08 (ML16342B001), response markups have been incorporated into Revision 1, Section 4.10, of the CSCCF TeR. As such, this confirmatory item has been satisfied. However, because the applicant did not provide a Tier 1 ITAAC item to verify the design commitment of EDDs used in non-safety applications will be diverse from EDDs used in safety applications and include supporting design descriptions in the D3 TeR, RAI 522-8633, Question 07.07-18, was tracked as an open item.

In the July 27, 2017, response to RAI 522-8633, Question 07.07-18 (ML17208B026), the applicant provided the following commitments, in part:

- Section 4.10 of the CSCCF TeR has been revised as indicated in the attachment to the Revision 0 response to specifically state the embedded technology used in safety-related and non-safety applications are diverse from each other and to add the table that lists the different types of EDDs and their functions.

- Design commitment that EDDs used in non-safety applications will be diverse from EDDs used in safety applications will be added as an ITACC item in the FSAR. DCD Tier 1, Section 2.5.5, will be revised as indicated in the attachment 1 associated with this response.

- The explanation regarding Class 1E devices with embedded technology that is included in part 4 of the response to RAI 356-7881, Question 07-08, will be moved into Section 6.2.5 of the D3 TeR, Revision 1 from Section 4.10 of the CSCCF TeR to provide an overall diversity analysis of APR1400 as indicated in attachments 2 and 3 associated with this response.

The staff finds this response adequately addressed the staff's specific requests for clarification in terms of providing clear statements on diversity between safety-related and non-safety devices with embedded technology as well as the addition of an ITAAC to verify this commitment. The staff finds the RAI responses' attached revisions to Section 4.10 of the

CSCCF TeR and DCD Tier 1 Section 2.5.5, based on the commitments in bullets #1 and #2 to be acceptable. The commitment for inclusion of design information for the D3 TeR, Revision 1 under bullet #3 above will be reviewed in Section 7.8 of this evaluation. However, since the applicant stated that in addition to having different manufacturer software and hardware designs, there is also functional diversity between the two ultrasonic level transmitters used, the staff requested the applicant to include functional diversity as an acceptance criterion to ITAAC Table 2.5.5-2, Item 8. In the August 14, 2017, response to this RAI (ML17226A285), the applicant added design descriptions and corresponding acceptance criterion to include functional diversity for the two level transmitters. Based on this addition, the staff finds that the proposed design description and ITAAC item will adequately verify the as-built I&C systems will use sufficiently diverse transmitters such that a software CCF will not cause the loss of function for both level transmitters. The incorporation of the proposed markup in the next revision of the DCD Tier 1, Section 2.5.5 and the D3 TeR was a confirmatory item. The staff verified the proposed markups have been incorporated into Revision 2 of the DCD Tier 1, Section 2.5.5 and the D3 TeR, Revision 2. As such this confirmatory item has been satisfied.

Evaluation Methodology for CCF Analysis

Section 7.7.2.3 of the FSAR refers to the CSCCF TeR for the analysis of postulated CSCCFs. The subject technical report describes the non-safety primary and secondary side control system design, and provides the evaluation method and results of the evaluation of postulated CSCCFs that could potentially affect plant critical safety functions.

The staff reviewed Sections 4.9, 4.10, and 5 of the CSCCF TeR. The staff reviewed the evaluation methods and the reported results for the CCF described in this technical report to assess whether the consequences are bounded by the DCD Tier 2 Chapter 15 safety analyses. The control system architecture and design features described in the subject technical report, up to and including failure mode definition, are outside the scope of this review.

The CSCCF TeR uses the term, “disappeared” in multiple places in Section 5, “Evaluation Method and Results,” which is confusing since it would not seem to convey the technical idea that is appropriate for the context in which the term is used. For example, in Sheet 9 of 18 of Table 5.1-10, “Multiple Failure due to a Single Failure of Shared Signals,” of the technical report, it states the following, “The above temporary excessive feedwater by ... is disappeared by ....” The staff issued RAI 68-7892, Question 07.07-7, to the applicant to clarify the use of the term “disappeared.”

In the October 14, 2016, response to RAI 68-7892, Question 07.07-7 (ML16288A859), the applicant clarified that, in part, the term “disappeared” is used to mean that an abnormal state of the feedwater flow due to a shared signal failure is recovered or cleared by a high pass filter function of the FWCS, because the high pass filter has a steady-state gain equal to zero. For clarification, the term “disappeared” will be changed to “recovered” in the CSCCF TeR. The applicant also proposed changes to Sections 5.1.4.7 and 5.1.4.8, and Tables 5.1-9, 5.1-10, and 5.2-9, of the CSCCF TeR to clarify operation of the FWCS. The staff reviewed the applicant’s response and proposed updates and found them acceptable. The applicant adequately removed the use of the term “disappeared” and provided sufficient clarifying language that permits better understanding of the failure modes of the FWCS and other associated functions in lieu of using the term “disappeared.” The incorporation of the proposed changes in the next revision of the CSCCF TeR was a confirmatory item. The staff verified that the proposed markups have been incorporated into Revision 1 of the CSCCF TeR. As such, this confirmatory item has been satisfied.

Regulatory Evaluation

The acceptance criteria applicable to the evaluation of CSCCFs presented in Section 5 of the CSCCF TeR are based on meeting the applicable requirements of 10 CFR Part 50, Appendix A, GDCs. The pertinent GDC are summarized below.

- GDC 10, “Reactor Design,” requires that the reactor be designed with sufficient margin to assure that specified acceptable fuel design limits are not exceeded during any condition of normal operation, including the effects of AOOs.

- GDC 15, “Reactor Coolant System Design,” requires that the RCS be designed with sufficient margin to assure that the design conditions of the reactor coolant pressure boundary are not exceeded during any condition of normal operation, including the effects of AOOs.

- GDC 28, “Reactivity Limits,” require that the reactivity control systems be designed with appropriate limits on the potential amount and rate of reactivity increase to assure that the effects of postulated reactivity accidents can neither (1) result in damage to the reactor coolant pressure boundary greater than limited local yielding nor (2) sufficiently disturb the core, its support structures or other reactor pressure vessel internals to impair significantly the capability to cool the core. These postulated reactivity accidents shall include consideration of rod ejection (unless prevented by positive means), rod dropout, steam line rupture, changes in reactor coolant temperature and pressure, and cold water addition.

In addition to the above design criteria, the acceptance criteria for radiation exposure as stipulated in 10 CFR 50.34 is applicable to the evaluation of CSCCFs presented in Section 5 of the CSCCF TeR.

The review guidance provided in the SRP was utilized in the review of Section 5 of the CSCCF TeR. The SRP sections particularly relevant to the review and evaluation are summarized below:

- SRP Section 7.7, “Control Systems,” to confirm that the effects of failures of control systems do not cause plant conditions more severe than those described in the analysis of design basis accidents and AOOs in Chapter 15.

- SRP BTP 7-19 provides guidance for the analysis of CCFs.

- SRP Chapter 15, “Introduction-Transient and Accident Analyses,” provides the acceptance criteria applicable to the CSCCF events evaluated in Section 5 of the CSCCF TeR.

In addition to the SRP sections listed above, each of the relevant sections under SRP Chapter 15 are applicable according to the event being evaluated.

7.7.4.17.3 Technical Evaluation

<u>The CSCCF TeR, Section 4.9, “Non-Safety Control Signals Sent to ESF-CCS”</u>

This section of the CSCCF TeR describes the design features of safety-related system instrumentation that prevent adverse protection system action resulting from signals originating from non-safety control systems (used to control safety components during normal operation) to the ESF-CCS.

The CSCCF TeR, Section 4.9.1 addresses the non-safety P-CCS signal for CVCS, and Section 4.9.2 addresses the non-safety P-CCS for the safety smoke damper control.

Table 4.9-1 of the CSCCF TeR identifies each of the non-safety signals sent to the CVCS safety-related components, and provides an evaluation of its effect on safety function.

Valves CV-515 and CV-560 are CVCS letdown and reactor drain tank isolation valves that interface with a non-safety P-CCS. While CV-515 is designed to close on a non-safety P-CCS signal resulting from letdown heat exchanger high temperature, its closure is a fail-safe position; further, CV-515 and downstream CV-516 both close on a SIAS.

The CV-560 is designed to close on a non-safety P-CCS signal resulting from reactor drain tank high pressure. Similar to CV-515, CV-560 is aligned in series with CV-561, both of which are closed upon receipt of a CIAS. Inadvertent closure of CV-560 is also a fail-safe position.

The volume control tank discharge isolation valve CV-504 receives a non-safety P-CCS signal to close resulting from the boration control valve CV-514 being not fully open. Either CV-504 or in-series valve CV-501 are manually closed during boration to cold shutdown conditions. Inadvertent closure of CV-504 is a fail-safe position.

Closure of either CV-515, CV-560, or CV-504 following a spurious non-safety P-CCS signal does not cause a plant transient that directly challenges plant safety. The failure effects of these valves opening resulting from spurious non-safety P-CCS signals is covered by the evaluations under the CSCCF TeR, Section 5.2.4.7.

Table 4.9-1 of the CSCCF TeR identifies the non-safety signal sent to the components of the safety-related smoke damper control system, and provides an evaluation of its effect on safety function.

The MCR HVAC system consists of two redundant divisions of outside air intake, each division including a smoke detector and a smoke damper, plus two in-series outside air intake isolation dampers. Therefore, a spurious P-CCS signal will close one of the smoke dampers, but the other division will continue to supply fresh air to the MCR. In addition, the intake isolation dampers will close upon receipt of an SIAS or CREVAS. Therefore, spurious closure of a smoke damper does not affect a plant safety function.

The staff finds that there is reasonable assurance that spurious non-safety control system signals sent to ESF functions of the CVCS and the MCR HVAC system will not pose a threat to plant safety functions worse than those described and evaluated in Section 5 of the CSCCF TeR. The staff’s review consisted of evaluating Section 5 of the CSCCF TeR against the regulatory criteria, and review of the applicant’s analysis input assumptions. The evaluations were performed by direct comparison of the postulated CSCCF events to applicable DCD Tier 2 Chapter 15 DBEs, supplemented as necessary by verification of key design information from

other chapters of the FSAR. Where explicit analyses have been performed by the applicant and reported in the CSCCF TeR, the analysis results were similarly reviewed by the staff and evaluated for compliance.

CSCCF TeR, Section 4.10, "CCF Analysis of Embedded Digital Devices in Field Equipment"

This section of the CSCCF TeR describes the potential for CCF of EDDs in field equipment, and evaluates the resulting multiple function failures due to both a single failure and a CCF of an embedded device. The applicant states that because embedded devices used in non-safety field equipment are not used in safety-related systems, there is no potential for a design defect in an embedded device to result in a CCF in both safety-related and non-safety equipment.

Section 4.10.1, "Evaluation for the CCF of No-safety Field Instruments," of the CSCCF TeR addresses the single failure of a non-safety field instrument with an EDD through reference to the evaluation of Failure Type 1 provided under Section 5.1 of the CSCCF TeR which considers the failure of any shared instrument signal regardless of implementation technology. Similarly, CCFs affecting all non-safety controllers are evaluated below as a Failure Type 3 occurrence under Section 5.3 of the CSCCF TeR, which covers spurious signals from the non-safety controllers regardless of failure source.

Section 4.10.2, "Evaluation for the CCF of Non-safety Field Actuators," of the CSCCF TeR provides an evaluation of failures of non-safety field actuators, stating that a failure of a single embedded device in a single field actuator is already covered by the FSAR Chapter 15 analysis of AOOs, and that a CCF of multiple non-safety controllers is covered by the analysis of Failure Type 3 occurrences that are evaluated below under Section 5.3 of the CSCCF TeR.

Section 4.10.3, "Evaluation for the Effect on Field Instruments due to Controller Failures," of the CSCCF TeR provides an evaluation of non-safety controller failures on field instruments, that is, failure of a non-safety controller that can potentially affect the instrument signal it's receiving. The applicant refers to the Failure Type 2 occurrences evaluated in Section 5.2 of the CSCCF TeR, which considers the effect of a failure of a single control group on all signals shared by that control group and other control groups via input/output modules. Failure of all field instruments resulting from failure of all control groups is already covered by Failure Type 3 evaluated below under Section 5.3 of the CSCCF TeR.

Section 4.10.4, "Evaluation for the Effect on Field Actuators due to Controller Failures," of the CSCCF TeR provides an evaluation of the effect of controller failures on field actuators, which interface with non-safety control systems via an output module. The effects of a failure of a single control group on all components controlled by that control group are already covered by the evaluation of Failure Type 2 occurrences in Section 5.2 of the CSCCF TeR. The failure of all control groups, evaluated below as Failure Type 3 occurrences under Section 5.3 of the CSCCF TeR, covers failure of all field actuators.

The staff finds that there is reasonable assurance, therefore, that single and CCFs of embedded devices in field equipment will not pose a threat to plant safety functions worse than those described and evaluated in Section 5 of the CSCCF TeR. The staff's review consisted of evaluating Section 5 of the CSCCF TeR against the regulatory criteria, and review of the applicant's analysis input assumptions. The evaluations were performed by direct comparison of the postulated CSCCF events to applicable DCD Tier 2 Chapter 15 DBEs, supplemented as necessary by verification of key design information from other chapters of the FSAR. Where

explicit analyses have been performed by the applicant and reported in the CSCCF TeR, the analysis results were similarly reviewed by the staff and evaluated for compliance.

Technical Report Section 5, "CSCCF Evaluation Methods and Results"

The initiating events postulated to occur as a result of credible control system failures are defined according to type of failure, as follows:

- Failure Type 1: multiple failures due to a single failure of a shared input signal.
- Failure Type 2: multiple failures of a single control group due to CSCCF.
- Failure Type 3: multiple failures of more than one control group due to CSCCF.
- Failure Type 4: multiple failures of Information FPD control commands due to CSCCF.

One or more control groups are designated to achieve each NSSS control function, as described in DCD Tier 2 Section 7.7 and as presented in Table 4.5-2, "Control Group," of the CSCCF TeR.

Control groups include the following:

- Steam Bypass Control System,
- FWCS,
- Main Feedwater Pump Control,
- Pressurizer Pressure Control System,
- Pressurizer Level Control System,
- CVCS,
- Reactor Regulating System / Reactor Power Cutback System,
- Digital Rod Control System,
- RCP Control,
- Non-1E alternating current Power Control,
- Condenser Vacuum Control,
- Turbine Control, and
- High Pressure Feedwater Heater Control.

The evaluations documented in Section 5, "Evaluation Method and Results," of the CSCCF TeR address each of the above failure types relative to its challenge to the plant critical safety functions, including fuel cladding integrity, primary system integrity, and offsite dose. Because

the postulated CSCCFs cannot result in a pipe break inside containment, challenge to containment integrity is not considered.

The evaluations provided in the CSCCF TeR are presented principally as qualitative assessments through comparison of the postulated transient event against the applicable DCD Tier 2 Chapter 15 safety analysis to demonstrate the CSCCF initiating events are bounded by the same acceptance criteria as the Chapter 15 DBEs.

Section 5 of the CSCCF TeR was reviewed and evaluated to confirm with reasonable assurance that CSCCF events will not result in consequences that exceed the acceptance criteria of DCD Tier 2 Chapter 15. The review consisted of evaluating Section 5 of the CSCCF TeR against the regulatory criteria, and review of the applicant's analysis input assumptions. The evaluations were performed by direct comparison of the postulated CSCCF events to applicable DCD Tier 2 Chapter 15 DBEs, supplemented as necessary by verification of key design information from other chapters of the FSAR. Where explicit analyses have been performed by the applicant and reported in the CSCCF TeR, the analysis results were similarly reviewed by the staff and evaluated for compliance.

Failure Type 1: Multiple Failures due to a Single Failure of a Shared Input Signal

The applicant used initial conditions that are the same as those used in the DCD Tier 2 Chapter 15 events. Similarly, the applicant assumed operator action is not credited during the first 30 minutes of the event and used engineering judgement to determine if similar Tier 2 Chapter 15 events bound the failures.

Process instrumentation signals may be shared among multiple control groups; therefore, loss of a process signal can affect multiple control groups. Shared signals include, for example, reactor power, pressurizer pressure and pressurizer level, RCS temperature, and steam generator steam flow.

Reactor Power Fails Low (as addressed in Section 5.1.4.1 of the CSCCF TeR): The primary response of the control system to this signal failure is CEA withdrawal, resulting in an increase in core power level, reactor coolant temperature, and pressure, accompanied by a decrease in heat removal due to feedwater flow reduction response to the erroneous low reactor power signal. The design basis for the CPC system includes consideration of a CEA withdrawal as well as a decrease in heat removal by the secondary system (Reference 1). The fuel is therefore protected by response of the CPC system to the DNBR transient. The main steam safety valves (MSSVs) and power operated safety relief valves (POSRVs) do not open for this event as they do for the Loss of Condenser Vacuum event analyzed in DCD Tier 2 Section 15.2.3, "Loss of Condenser Vacuum." The results for this event are therefore bounded by the DCD Tier 2 Section 15.2.3 event.

Reactor Power Fails High (as addressed in Section 5.1.4.2, of the CSCCF TeR): CEA insertion occurs as a result of this signal failure, resulting in a decrease in reactor T_{avg} subsequently followed by CEA withdrawal by T_{avg} program control. At high power conditions, normal plant conditions are restored with no challenge to plant critical safety functions. During low power operation, a temporary increase in feedwater flow occurs due to transfer from downcomer to economizer control valve, resulting in an increase in core reactivity due to moderator temperature feedback. The feedwater level control is eventually recovered through steam generator level control, though a reactor trip on steam generator high level may occur.

Pressurizer Pressure Fails Low (as addressed in Section 5.1.4.3 of the CSCCF TeR): As a result of this initiating event, the pressurizer heaters actuate without pressurizer spray, resulting in an increase in system pressure. The reactor is tripped on high pressurizer pressure, and the heaters turn off by low pressurizer level. This event is bounded by the DCD Tier 2 Section 15.2.3 event which also results in reactor trip on high pressurizer pressure but also results in opening of POSRVs and MSSVs which are not expected to open for the postulated event.

Pressurizer Pressure Fails High (as addressed in Section 5.1.4.4 of the CSCCF TeR): Excessive pressurizer spray without heater actuation occurs, resulting in a decrease in system pressure with the pressurizer level control system controlling pressurizer level. Inadvertent depressurization of the RCS by actuation of full spray flow without pressurizer heater operation is included in the design basis of the CPC system. A CPC trip on low DNBR may occur as a result of the low reactor pressure effect on fuel thermal margin, however a reactor trip will also occur on low pressurizer pressure accompanied by safety injection into the reactor system. The event does not pose a challenge to any critical safety function.

RCS Temperature Fails Low (as addressed in Section 5.1.4.5 of the CSCCF TeR): This initiating event causes an inadvertent withdrawal of CEAs, resulting in an increase in reactor power, pressure, and T_{avg} and eventually an automatic withdrawal prohibit actuated by the SBCS high pressurizer pressure signal (via SBCS demand for turbine bypass valve open). Uncontrolled CEA withdrawal is considered in the design of the CPC system. The postulated event is less severe than the DCD Tier 2 Section 15.4.2, “Uncontrolled CEA Withdrawal,” event which is characterized by a longer CEA withdrawal time.

RCS Temperature Fails High (as addressed in Section 5.1.4.6 of the CSCCF TeR): This initiating event causes an inadvertent insertion of CEAs, resulting in a decrease in reactor power, reactor pressure, and steam generator pressure, causing a reactor trip on low pressurizer pressure or low stream generator pressure. The uncontrolled insertion of CEAs is included in the design basis of the CPC system which ensures that specified acceptable fuel design limit (SAFDLs) are not violated. Furthermore, the postulated event is bounded by the more rapid insertion of a dropped CEA event as analyzed in DCD Tier 2 Section 15.4.3. The Dropped CEA event also results in a distortion of the core radial power distribution and no reactor trip occurs; fuel integrity is protected through Technical Specification LCO to ensure adequate margin to the SAFDL.

Turbine Load Index Fails Low (as addressed in Section 5.1.4.7 of the CSCCF TeR): This event causes the inadvertent insertion of CEAs, with results similar to the Reactor Coolant System Temperature Fails High. The reactor core is protected by the CPC system which includes an uncontrolled insertion of CEAs in its design basis.

Turbine Load Index Fails High (as addressed in Section 5.1.4.8 of the CSCCF TeR): As a result of this initiating event, a CEA withdrawal signal is generated when operating at less than full power and subsequently cleared by the RRS high pass filter, thus terminating the CEA withdrawal; feedwater is also temporarily increased due to the erroneous steam flow signal, but then cleared by the FWCS high pass filter. This event is bounded by the “Uncontrolled CEA Withdrawal” event analyzed in DCD Tier 2 Section 15.4.1 which involves a longer uncontrolled withdrawal of CEAs.

Pressurizer Level Fails Low (as addressed in Section 5.1.4.9 of the CSCCF TeR): As a result of the erroneous low pressurizer level signal, excessive CVCS charging flow and insufficient

letdown flow occurs, which is similar to the CVCS Malfunction that Increases Reactor Coolant Inventory as analyzed in DCD Tier 2 Section 15.5.2. This event does not challenge a plant critical safety function.

Pressurizer Level Fails High (as addressed in Section 5.1.4.10 of the CSCCF TeR): This initiating event causes excessive CVCS letdown and insufficient charging flow resulting in a decrease in pressurizer pressure, level, and reactor trip on low pressurizer pressure accompanied by safety injection into the reactor. The DNBR SAFDL is protected by the CPC system if a reactor trip on low pressurizer pressure does not occur first. The event is bounded by the Failure of Small Line Break Outside Containment analyzed in DCD Tier 2 Section 15.6.2 for which the letdown flow is limited only by the letdown orifices inside containment and a reactor trip is prevented in order to maximize the break flow. The design basis of the CPC system includes the letdown line break outside containment to ensure protection of the SAFDLs.

Steam Generator Steam Flow Fails Low (as addressed in Sections 5.1.4.11 and 5.1.4.12 of the CSCCF TeR): This initiating event affects the Steam Bypass Control System (Main and Permissive) and the Feedwater Control System control groups. For a low steam flow in either of the two steam generators, neither the turbine bypass nor the reactor power cutback will actuate because either the SBCS main or permissive signal is unavailable (depending on which steam generator has the spurious low flow signal). The feedwater flow will decrease but the decrease will be terminated by the FWCS high pass filter function which clears the signal failure, and normal operation is maintained.

Steam Generator No. 1 Steam Flow Fails High(as addressed in Section 5.1.4.13 of the CSCCF TeR): The worst case evaluated is an erroneous high steam flow signal in steam generator no. 1 prior to turbine synchronization, which causes turbine bypass valves to open (assuming manual permissive prior to turbine synchronization) and a variable overpower reactor trip may occur. In addition, the CPC system is designed to protect the fuel against excessive heat removal caused by inadvertent opening of turbine bypass valves (Reference 1). During turbine synchronization, an increase in feedwater will occur, but will be recovered by action of the high pass filter function. Relative to the heat removal transient, the postulated erroneous steam generator high steam flow signal is not more limiting than the DCD Tier 2 Section 15.1.4 Inadvertent Opening of a Steam Generator Relief or Safety Valve which results in a new stabilized power level of 113 percent.

Steam Generator No. 2 Steam Flow Fails High (as addressed in Section 5.1.4.14 of the CSCCF TeR): In the case of an erroneous high steam flow signal steam generator no. 2, a steam bypass control system permissive is generated without a steam bypass control system main signal and the turbine bypass valves do not open. The increase in feedwater flow in steam generator no. 2 is terminated by the high pass filter and normal operation is maintained.

Steam Header Pressure Fails Low (as addressed in Section 5.1.4.15 of the CSCCF TeR): During power operation following turbine synchronization, this initiating event causes a reduction in feedwater flow (due to decreased feedwater pump speed control bias), resulting in steam generator low level and possibly a reactor trip on steam generator low level. This event is bounded by the DCD Tier 2 Section 15.2.7, “Loss of Normal Feedwater Flow,” analysis because the DCD Tier 2 Section 15.2.7 analysis assumes a loss of all normal feedwater flow. At lower power conditions, before turbine synchronization, in addition to the reduction of feedwater flow, turbine bypass valves are assumed to close, resulting in an increase in both secondary and primary system pressure and reactor trip on either low steam generator level or high pressurizer pressure. In comparison to DCD Tier 2 Section 15.2.3, “Loss of Condenser

Vacuum," event, the transient resulting from a postulated steam header pressure fails low signal is less severe in terms of decreased heat removal because the "Loss of Condenser Vacuum" event assumes an immediate and complete loss of feedwater flow and a turbine trip.

Steam Header Pressure Fails High (as addressed in Section 5.1.4.16 of the CSCCF TeR): This event causes an increase in feedwater flow (due to increased feedwater pump speed control bias). The increase in feedwater flow is bounded by the "Increase in Feedwater Flow" event analyzed in DCD Tier 2 Section 15.1.2 which assumes the maximum increase in feedwater flow. The fuel is protected by the CPC system which is designed to take into account an excess feedwater flow event (Reference 1).

Non-Class 1E 13.8 kV low-low Signal (as addressed in Section 5.1.4.17 of the CSCCF TeR): An erroneous low-low signal from the non-Class 1E 13.8 kV power system control group will send a stop-pump signal to the RCP control group, Condenser Vacuum control group, Main Feedwater Pump control group, and the miscellaneous BOP control group for pump protection purposes.

In the case where an inadvertent low-low signal is sent to the aforementioned control groups, reactor trips will be actuated as a result of: CPC RCP shaft low speed, which is bounded by the DCD Tier 2 Section 15.2.6, "Loss of Non-emergency Alternating Current Power Event"; low steam generator level, which is bounded by DCD Tier 2 Section 15.2.7, "Loss of Normal Feedwater Flow"; and turbine trip (due to loss of condenser vacuum), bounded by DCD Tier 2 Section 15.2.3, "Loss of Condenser Vacuum."

In the case where there is a failure of the low-low signal to be sent, the loss of electrical power to the RCPs will result in a reactor trip on CPC RCP shaft low speed. This event is bounded by the DCD Tier 2 Section 15.2.6, "Loss of Non-Emergency Alternating Current Power," analysis.

The staff reviewed the applicant's evaluation of a failed share signal effecting potentially multiple control groups (i.e., Type 1 failures) as given in Tables 5.1-2 through 5.1-19. Tables 5.1.2 through 5.1-19 evaluate the failure of the shared signals, as given in Table 5.1-1, at both the high or low signal range. Consistent with the guidance given in Standard Review Plan 7.7, "Control System," the staff agrees that a failure of a shared signal affecting the multiple control groups is bounded by a Tier 2 Chapter 15 FSAR analysis.

<u>Failure Type 2: Multiple Failures due to a Single Control Group</u>

This evaluation addresses multiple spurious output failures of a single control group as an initiating event.

The applicant used initial conditions that are the same as those used in the DCD Tier 2 Chapter 15 events, and operator action is not credited during the first 30 minutes of the event.

Steam Bypass Control-Main / Permissive System Control Groups (as addressed in Sections 5.2.4.1 and 5.2.4.2 the CSCCF TeR): A spurious signal to open turbine bypass valves (either quick open or modulation mode) would have no effect because a Steam Bypass Control-Permissive signal, which is controlled by another Control Group, would not be present to permit valve opening. Erroneous outputs that would prevent turbine bypass valve opening, automatic withdrawal prohibit, automatic motion inhibit, and reactor power cutback also do not result in any event because there is no demand for such control system actions.

Therefore, the staff agrees that multiple failures of the Steam Bypass Control System-Main control group has no effect on the plant. Similarly, the staff agrees that multiple failures of the Steam Bypass Control System-Permissive control group have no effect on the plant.

Steam Generator No.1 /No. 2 Feedwater Control System Control Groups (as addressed in Sections 5.2.4.3 and 5.2.4.4 of the CSCCF TeR): The multiple failures of either the Steam Generator No. 1 or Steam Generator No. 2 control group can cause erroneous feedwater valve opening/closing (downcomer or economizer inlets), and feedwater pump speed increase/decrease. These erroneous feedwater control valve opening/closing and pump speed increase/decrease scenarios are already considered in DCD Tier 2 Section 15.1.2 Increase in Feedwater Flow and Section 15.2.7, "Loss of Normal Feedwater Flow," and are therefore bounded by the DCD Tier 2 Chapter 15 safety analysis. The fuel is protected by the CPC system which is designed to take into account either an increase or a decrease of feedwater flow transient.

Pressurizer Pressure Control System Control Group (as addressed in Section 5.2.4.5 of the CSCCF TeR): Multiple failures of the pressurizer pressure control system control group can either cause excessive pressurizer spray/insufficient heater capacity, or insufficient pressurizer spray/increase heater capacity. In the former, the decrease in RCS pressure results in a decrease in DNBR margin, however the CPC System generates a low DNBR reactor trip to protect the fuel before the SAFDL is reached. The design basis for the CPC system includes consideration of inadvertent RCS depressurization due to actuation of full spray without heater actuation (Reference 1).In the latter case, the resulting increase in reactor system pressure leads to a reactor trip on high pressurizer pressure. This event is bounded by the DCD Tier 2 Section 15.2.3, "Loss of Condenser Vacuum," event, which is characterized by a faster pressure transient.

Pressurizer Level Control System Control Group (as addressed in Section 5.2.4.6 of the CSCCF TeR): This postulated control group failure can result in either an increase or decrease in RCS inventory. The increase in RCS inventory is already considered in the DCD Tier 2 Section 15.5.2, "CVCS Malfunction," analysis. The applicant reports that the decrease in reactor coolant inventory scenario is bounded by the DCD Tier 2 Section 15.6.2, "Failure of Letdown Line Outside of Containment," which has a larger coolant flow discharge rate than the postulated control group failure event. However, Table 5.2-7 of the CSCCF TeR cites the DCD Tier 2 Section 15.6.2, "Letdown Line Break," flow as 28 pounds per second (lb/sec) versus 25 lb/sec as stated in DCD Tier 2 Section 15.6.2. In addition, Section 5.2.4.6 of the CSCCF TeR indicates that the charging valves (CV212 valves) are closed, whereas the DCD Tier 2 Section 15.6.2, Letdown Line Break analysis assumes the minimum charging flow of 70.4 gpm during the transient.

In the March 28, 2016, response to RAI 371-8456, Question 07.07-9 (ML16088A379), the applicant states that the letdown break flow rate described in Table 5.2-7 of the CSCCF TeR, will be revised to 25 lb/sec. The applicant further clarifies that the charging flow assumed in Section 5.2.4.6 of the CSCCF TeR is the same as that assumed in the DCD Tier 2 Section 15.6.2 analysis, i.e., that the control valve is throttled back, not closed. The applicant's response also includes explicit analysis results comparing the DNBR-related parameters for the Pressurizer Level Control System Control Group Failure against the Letdown Line Break and SGTR events which show that the DNBR SAFDL is not violated for the Pressurizer Level Control System Control Group Failure. The applicant's response is acceptable as it demonstrates the minimum DNBR limit is not violated for failures associated with the Pressurizer Level Control System Control Group. The applicant has provided revised pages

(pages 51 and 90) for incorporation in the next revision of the CSCCF TeR. The incorporation of these proposed markups into the next revision of the CSCCF TeR is confirmatory item. The staff verified that the proposed markups have been incorporated into Revision 1 of the Control System CCF Analysis TeR. As such, this confirmatory item has been satisfied.

CVCS Control Group (as addressed in Section 5.2.4.7 of the CSCCF TeR): Multiple failures of the CVCS control group can decrease reactor coolant boron concentration, or increase or decrease coolant inventory. The decrease in reactor coolant boron concentration adds reactivity to the core and can challenge the shutdown margin needed achieve and maintain the reactor in a subcritical state. This postulated event, however, is bounded by the DCD Tier 2 Section 15.4.6, "Inadvertent Decrease in Boron Concentration in the Reactor Coolant System," analysis, which assumes the maximum possible value for the dilution charging flow. The fuel is protected by the CPC system which is designed to take into account an uncontrolled boron dilution event (Reference 1). The increase and decrease in reactor coolant inventory events are covered by the Pressurizer Level Control System Control Group failures above.

Control Rod Control – RRS/RPCS Control Group (the CSCCF TeR, Section 5.2.4.8): The RRS/RPCS controls the reactor in response to turbine load, and sends multiple signals including reactor power to the steam bypass control system and the FWCS; reactor coolant average temperature to the steam bypass control system, the FWCS, and the pressurizer level control system; and turbine load index to the steam bypass control system and the FWCS. Failures in the RRS/RPCS control group, therefore, can produce numerous spurious output signals involving the aforementioned control systems.

Worst case scenarios for challenges to both fuel cladding integrity and RCS integrity are presented. At low power conditions, the worst case initiating event relative to fuel cladding integrity (DNBR) is a CEA withdrawal demand and decrease in feedwater flow caused by a RRS/RPCS failure. A decrease in feedwater flow is caused by TLI fail low signal.. The CSCCF TeR, Section 5.2.4.8, however, also refers to the turbine power (TLI) fail high as causing the excessive feedwater due to valve transfer from DV to EV, which is inconsistent with the previous description and inconsistent with the information provided in Table 5.1-1 of the CSCCF TeR.

In March 4, 2016, response to RAI 371-8456, Question 07.07-10 (ML16064A398), the applicant revised the event description to state that the excessive feedwater could result from a reactor power fail high signal. The applicant's response is acceptable as it corrects Section 5.2.4.8 to include that a reactor power fail high signal also causes an increase in feedwater flow. The staff reviewed Revision 2 of APR1400-Z-J-NR-14012 and confirmed that a reactor power fail high signal was added closing the confirmatory item associated with RAI 371-8456, Question 07.07-10.

The postulated CEA withdrawal at low power in combination with excessive feedwater caused by either a reactor power or TLI fail high signal is bounded by the DCD Tier 2 Section 15.4.1, "Uncontrolled CEA Withdrawal," event at low power as the excessive feedwater adds negative reactivity due to the positive MTC at low powers the TLI fail low signal, which decreases feedwater flow, is bounded by the DCD Tier 2 Section 15.4.1, "Uncontrolled CEA Withdrawal," as the Section 15.4.1 analysis assumes a LOOP at time zero and a corresponding decrease in feedwater flow due to the reactor coolant pump coastdown. The staff agrees the DCD Tier 2 Section 15.4.1, "Uncontrolled CEA Withdrawal," analysis bounds the RRS/RPCS failures and hence the DNBR SAFDL will not be violated during low power operation. Section

At full power conditions, a CEA withdrawal demand and RCS temperature fail low causes a reactivity insertion transient in combination with a drop in pressurizer water level (due to the pressurizer level control program response to low T_{avg}). The programmed drop in pressurizer level is reported to be to 30 percent (as measured between the lower and upper instrumentation taps). Because the DCD Tier 2 Section 15.4.1, "Uncontrolled CEA Withdrawal," events are evaluated for a range of initial pressurizer levels down to 21 percent (per DCD Tier 2 Section 15.0.0.2.2 and Table 15.0-3), the postulated event is bounded by the DCD Tier 2 Section 15.4 safety analysis and the DNBR SAFDL is not violated.

The RCS integrity is evaluated for both low power and high power modes of operation. At low power, the worst case set of failures is identified to be an erroneous CEA withdrawal demand combined with TLI fail low, reactor coolant temperature fail high, and inadvertent turbine runback, resulting in withdrawal of CEAs, a decrease in feedwater flow, and an increase in reactor coolant inventory, all of which contribute to the primary system pressure increase. The transient event is promptly terminated by a reactor trip on high pressurizer pressure with the peak RCS pressure reasonably expected to remain below the acceptance criterion of 110 percent design. At power conditions, the CEA withdrawal accompanied by a turbine runback and setback demand causes a rapid increase in pressure resulting in a prompt reactor trip on high pressurizer pressure. Section 5.2.4.8 of the CSCCF TeR states that the primary system pressure remains within the acceptance criteria (110 percent of design 2500 psia). However, considering the DCD Tier 2 Section 15.4.2, "CEA Withdrawal at Power," event results in a peak RCS pressure of approximately 106 percent of design, it is unclear whether the postulated CEA withdrawal accompanied by a turbine runback will result in a peak RCS pressure within 110 percent design pressure. Therefore, the staff asked the applicant in RAI 371-8456, Question 07.07-12, to provide additional justification that the CEA withdrawal accompanied by a turbine runback and setback remains below the 110 percent of design pressure acceptance criteria. The issue identified in RAI 371-8456, Question 07.07-12, was tracked as an open item. In the May 27, 2016, response to RAI 371-8456, Question 07.07-12 (ML16148B201), the applicant provided analysis results which demonstrated that both peak RCS and steam generator pressures remain below 110 percent of the nominal design pressure. The staff's review of the methodology, assumptions, and initial conditions determined that conservative predictions of peak RCS and steam generator pressure were calculated. As peak RCS and steam generator pressures remained below the 110 percent acceptance criteria, the staff finds the applicant's response acceptable and the open item associated with RAI 371-8456, Question 07.07-12, is closed and resolved.

Control Rod Control – DRCS Control Group (the CSCCF TeR, Section 5.2.4.9): The multiple failures associated with this control group are the same as the RRS/RPCS control group reviewed and evaluated above.

RCP Control System Control Group (the CSCCF TeR, Section 5.2.4.10): Multiple failures of the RCP control group result in a complete loss of forced coolant flow and the applicant concludes that such postulated failures are covered by the DCD Tier 2 Section 15.3.1, "Loss of Forced Reactor Coolant Flow," analysis. The staff issued RAI 371-8456, Question 07.07-13, to request the applicant to specify whether a more severe loss of flow event could occur as a result of multiple failures of the RCP Control System Control Group, specifically a forced reactor pump speed reduction due to a bus electrical under-frequency event instead of the pump coastdown assumed in DCD Tier 2 Section 15.3.1, "Loss of Forced Reactor Coolant Flow."

In the April 8, 2016, response to RAI 371-8456, Question 07.07-13 (ML16099A001), the applicant provided a description of the connection of the RCPs to their respective electrical

supply buses and states that the APR1400 design does not subject the RCPs to a sustained frequency decay of greater than 3 hertz per second (Hz/sec). The 3 Hz/sec under-frequency transient is shown in Figure 1 of the RAI response to be less severe than a 4-pump coastdown. The response is acceptable as the applicant has demonstrated failures within the RCP Control System Group are bounded by the Chapter 15.3.1, "Loss of Forced Reactor Coolant Flow," analysis.

Feedwater Heater Train A / B Control Group (as addressed in Sections 5.2.4.11 and 5.2.4.12 of the CSCCF TeR): Multiple failures of the Feedwater Heater Train control groups will result in either an increase in heat removal by the secondary system due to loss of steam to feedwater heaters, or a decrease in heat removal from the secondary system resulting from inadvertent closure of a feedwater train valve. The fuel is protected by the CPC system which is designed to take into account either an increase or a decrease in heat removal by the secondary system.

The increase in heat removal by the secondary system is already addressed as a DBE in DCD Tier 2 Section 15.1.1, which assumes a maximum 100ºF decrease in feedwater temperature. The decrease in heat removal by the secondary system is addressed in the DCD Tier 2 Section 15.2.7 analysis of the Loss of Normal Feedwater event which assumes a more bounding total loss of feedwater flow as compared to the postulated loss of one train.

Feedwater High Pressure Heater Bypass Line Control Group (as addressed in Section 5.2.4.13 of the CSCCF TeR): Multiple failures with this control group could cause inadvertent opening of the feedwater heater bypass line, resulting in an increase in feedwater flow of less than 25 percent which the applicant reports to be less than that analyzed in the DCD Tier 2 Section 15.1.2 Increase in Feedwater Flow DBE. However, the limiting event that appears to be analyzed in DCD Tier 2 Section 15.1.2 is the inadvertent actuation of auxiliary feedwater, adding 10 percent of the rated main feedwater flow.

Therefore, the staff asked the applicant in RAI 371-8456, Question 07.07-14 how the 10 percent increase assumed in DCD Tier 2 Section 15.1.2 bounds the 25 percent increase assumed in the inadvertent opening of the feedwater heater bypass line case. In the March 4, 2016, response to RAI 371-8456, Question 07.07-14 (ML16064A398), the applicant provides clarification that the Increase in Feedwater Flow event analyzed in DCD Tier 2 Section 15.1.2.1 assumes an increase in feedwater flow of 70 percent above the nominal flow (for a total flow rate of 170 percent), which bounds the Feedwater High Pressure Heater Bypass Line Control Group failure event evaluated in Section 5.2.4.13 of the CSCCF TeR and therefore, the applicant's response is acceptable.

Feedwater Pumps On/Off Control Group (as addressed in Section 5.2.4.14 of the CSCCF TeR): Multiple failures of the Feedwater Pumps On/Off control group can cause inadvertent start or stop of a feedwater pump. The increase or decrease in feedwater flow resulting from such inadvertent actuations are covered by the DBEs analyzed in DCD Tier 2, Sections 15.1.2 and 15.2.7. The fuel is protected by the CPC system which includes both excessive feedwater flow and a loss of feedwater flow in its design basis.

Non-Class 1E 13.8 kV Power to Station Auxiliaries Control Group (as addressed in Section 15.2.4.15 of the CSCCF TeR): Multiple failures within this control group cause loss of power to the RCPs and main feedwater booster pumps. This event is covered by the DCD Tier 2 Section 15.3.1 Loss of Forced Reactor Coolant Flow DBE which is typically a limiting DNBR event. The fuel is protected by the CPC system which is designed to take into account a loss of electrical power to all RCPs.

Condenser Vacuum Control System Control Group (as addressed in Section 5.2.4.16 of the CSCCF TeR,): Failure of this control group can cause either an increase in condenser vacuum (due to actuation of a standby vacuum pump) or a decrease in condenser vacuum. The former case does not affect plant operation, and the latter case is covered by the DCD Tier 2 Section 15.2.3 Loss of Condenser Vacuum event.

Turbine Control System Control Group (as addressed in Section 5.2.4.17 of the CSCCF TeR): Multiple failures of this control group could result in either a turbine trip or an increase in turbine control valve admission area. The turbine trip is already analyzed as a DBE in DCD Tier 2 Section 15.2.2, and the postulated full open turbine control valve event is bounded by the more limiting DCD Tier 2 Section 15.1.4, "Inadvertent Opening of a Steam Generator Relief or Safety Valve," event. The fuel is protected by the CPC system which is designed to take into account the inadvertent opening of the turbine control valves (Reference 1). Miscellaneous BOP Control Group (Section 5.2.4.18 of the CSCCF TeR): Multiple failures of this BOP control group can cause loss of the circulating water pumps or the condensate pumps, resulting in loss of condenser vacuum, which is already a DBE analyzed in DCD Tier 2 Section 15.2.3, "Loss of Condenser Vacuum."

Based on the above evaluation, the staff finds that multiple failures within a single control group will not result in consequences more severe than those presented in Chapter 15 of the DCD Tier 2.

<u>Failure Type 3: Multiple Failures of More than One Control Group</u>

This evaluation addresses multiple spurious outputs resulting from failures of multiple control groups as an initiating event. Section 5.3.2 of the CSCCF TeR states that best estimate analysis methods are used to perform the analyses, including the use of nominal initial conditions as listed in Table 5.3-3.

In accordance with the guidelines provided in SRP BTP 7-19, CCFs are considered beyond design basis and may be evaluated using best-estimate methods. SRP BTP 7-19 further defines best-estimate to be "realistic assumptions," including normal plant conditions. Therefore, the staff finds the use of the nominal values listed in Table 5.3-3 acceptable as it conforms to the use of realistic assumptions per SRP BTP 7-19.

Section 5.3.3 of the CSCCF TeR describes the plant initial conditions assumed in the best-estimate calculations, but does not address the core lifetime-related parameters such as moderator temperature coefficient of reactivity, axial power shape, and scram reactivity characteristics. Therefore, in RAI 371-8456, Question 07.07-15, the staff asked what time in life core related parameters were used to evaluate the acceptability of multiple control group failures. In the March 4, 2016, response to RAI 371-8456, Question 07.07-15 (ML16064A398), the applicant stated that the parameters that most significantly affect the DNBR transient are the moderator temperature coefficient (MTC) and fuel temperature coefficient (FTC) of reactivity, which are most limiting at end-of-cycle core conditions, and the core radial peaking factor, which is most limiting at beginning-of-cycle core conditions. The response included tables for comparison of the core-related parameters assumed in the analysis of Multiple Failures of More than One Control Group as described in Section 5.3.3 of the CSCCF TeR versus the limiting DNBR and over-pressurization events presented in DCD Tier 2 Chapter 15. The parameters used in the DCD Tier 2 Chapter 15, analyses are selected based on sensitivity studies to be most limiting for either minimizing DNBR or maximizing reactor system pressure. The parameters assumed in the analysis in Section 5.3.3 of the CSCCF TeR are based on realistic

assumptions for worst-time-in-core-life for each particular parameter therefore the applicant's response is acceptable. The applicant has provided revised pages 59 and 60 for the CSCCF TeR. The incorporation of these proposed markups into the next revision of the CSCCF TeR was confirmatory item. The staff verified that the proposed markups have been incorporated into the Revision 1 of the CSCCF TeR. As such, this confirmatory item has been satisfied.

The multiple control group failures are assumed to occur simultaneously. The worst combinations of control group failures relative to fuel cladding integrity and RCS integrity are identified and selected for analysis in Section 5.3.2 of the CSCCF TeR.

Section 5.3.2 of the CSCCF TeR identifies the worst case set of initiating events relative to fuel cladding integrity to be multiple failures of the steam bypass control system (opening of all turbine bypass valves), the feedwater high pressure heater control system (decrease in feedwater heating), and FWCS (increase in feedwater flow). These failures cause cooldown of the RCS and resultant reactivity addition due to moderator temperature coefficient feedback, and a challenge to the DNBR SAFDL. The results of the analysis of this set of initiating events, as described in Section 5.3.5.1 of the CSCCF TeR, attribute the rise in reactor power to the primary system cooldown. Table 5.3-1 of the CSCCF TeR, however, also identifies failure of the control rod control groups (RRS/RPCS and DRCS) to be a contributor to the initiating event. Therefore, the staff asked in RAI 371-8456, Question 07.07-16 if the applicant analysis also included a concurrent CEA withdrawal. In the March 4, 2016, response to RAI 371-8456, Question 07.07-16 (ML16064A398), the applicant states that the DNBR event described in Section 5.3.5.1 of the CSCCF TeR includes a concurrent CEA withdrawal as identified Table 5.3-1 of the CSCCF TeR. The applicant's response is acceptable as it clarifies that failure in the RRS/RPCS which causes a CEA withdrawal is included in the fuel cladding integrity analysis. The applicant has provided a revised page 60 of the CSCCF TeR. The incorporation of the proposed markups into the CSCCF TeR is already addressed as part of the confirmatory item to RAI 371-8456, Question 07.07-15. In addition, staff has also verified that the RAI 371-8456, Question 07.07-16, proposed markups have been incorporated into the Revision 1 of the CSCCF TeR. As such, this confirmatory item has been satisfied.

The worst case initiating event in terms of RCS integrity involves multiple failures of the FWCS (termination of feedwater), inadvertent withdrawal of CEAs, and condenser vacuum pump trip (resultant turbine trip). These failures cause an increase in RCS pressure, and the analysis shows that a reactor trip on high pressurizer pressure occurs at 5 seconds to terminate the transient with primary system pressure reaching a peak pressure of 2611 psia at 7.7 seconds, which is well below the 2750 psia acceptance criterion (110 percent design).

The staff reviewed the analysis assumptions, method and results for multiple control group failures due to a software design defect or a CSCCF (i.e., Type 3 failures). The staff reviewed the assumptions as given in Section 5.3., "Assumptions Used in the Evaluation," of the CSCCF TeR, which are assumed for both the fuel rod integrity and RCS pressure evaluations and found them to be acceptable. The staff also agrees that the use of best estimate initial conditions and analysis values (e.g., rod worths, reactivity feedbacks, etc.) is consistent with SRP BTP 7-19 and therefore acceptable. Likewise, the staff agrees that the use of RELAP5/Mod3.3 code is acceptable for an evaluation of this type.

The staff reviewed the combination of control group failures given in Table 5.3-1 of the CSCCF TeR for the fuel cladding integrity analysis and found them to be acceptable. The staff also reviewed the sequence of events presented in Table 5.3-4 of the CSCCF TeR and the RCS parameters of interest as shown in Figures 5.3-1 to 5.3-5 of the CSCCF TeR. The staff finds

the sequence of events and the corresponding system performance consistent with the failures assumed and therefore acceptable. The staff agrees the minimum DNBR limit is not violated and that fuel integrity is maintained.

The staff reviewed the combination of control group failures given in Table 5.3-2 of the CSCCF TeR for the primary system pressure analysis and found them to be acceptable. The staff also reviewed the sequence of events presented in Table 5.3-5 of the CSCCF TeR and the RCS parameters of interest as shown in Figures 5.3-6 to 5.3.10 of the CSCCF TeR. The staff finds the sequence of events and the corresponding system performance consistent with the failures assumed and therefore acceptable. The staff agrees the RCS pressure boundary integrity is maintained as peak pressure does not exceed 110 percent of the design pressure.

Failure Type 4: Multiple Failures of IFPD Control Commands

Multiple failures of IFPD commands due to a software defect are assumed as initiating events that could challenge fuel cladding integrity and RCS integrity. However, because IFPD commands pass through the DCS controllers, the worst case of failure combinations in terms of fuel cladding integrity and RCS integrity are already evaluated as Failure Type 3 initiating events.

7.7.5 Combined License Information Items

No applicable items were identified in the FSAR for the non-safety I&C systems. No additional COL information items need to be included in DCD Tier 2 Tier 2 Table 1.8-2.

7.7.6 Findings and Conclusions

The staff concludes that the design of the control systems not required for safety is acceptable and meets the relevant requirements of GDC 1, 10, 13, 15, 19, 24, 28, 29, and 44, and of 10 CFR 50.34(f), and 10 CFR 50.55a(h)(3).

The staff conducted a review of these systems for conformance to RGs, industry codes and standards applicable to these systems.

The staff conducted a review of the plant transient response to normal load changes and AOOs such as reactor trip, turbine trip, upsets in the feedwater, and steam bypass systems. With regard to control systems not required for safety, the staff review confirmed the non-safety control systems design meets the requirements of GDC 13.

The staff's review of the control systems considered the features of these systems for both manual and automatic control of the process systems. With regard to control systems not required for safety, the staff review confirmed the non-safety control systems design meets the requirements of GDC 19 with regard to normal plant operations.

The staff's review determined that multiple failures within a single control group resulting from a shared signal or a control system CCF will not result in plant conditions that exceed the acceptance criteria applicable to the DCD Tier 2 Chapter 15 plant safety analysis.

The staff reviewed the CSCCF TeR to ensure that failures of the non-safety control systems do not affect plant safety, and the non-safety control system design demonstrates satisfactory compliance to10 CFR 50.55a(h)(3) and the requirements of GDC 24.

The staff's review determined the applicant's design for the non-safety control system design meets the guidance of the standard review plant that stipulates that the consequential effects of AOOs and accidents do not result in control system failures that would cause plant conditions more severe than those bounded by the analysis of the events. This review is based upon the requirements of GDC 24 as well as IEEE Std 603-1991, Clause 4.8.

The conclusions of the analysis of AOOs and accidents, as presented in Chapter 15 of the FSAR have been used to confirm that plant safety is not dependent upon the response of the control systems. The staff determined that the non-safety control system design confirm that failures of the control systems themselves or as a consequence of supporting system failures, such as loss of power sources, do not result in plant conditions more severe than those described in the analysis of design basis accidents and AOOs.

7.8 Diverse I&C Systems

7.8.1 Introduction

Diversity of the I&C systems is described in DCD Tier 2 Section 7.8; the D3 TeR; and the CCF Coping Analysis TeR. The design information in these documents consists of:

- The D3 design for the I&C systems.
- The design features that prevent and mitigate a software CCF of the safety-related I&C systems.
- The design features to address an ATWS.
- A methodology to evaluate the D3 aspects of the I&C architecture to determine if the I&C system will adequately protect the health and safety of the public in the unlikely event of a software CCF.

7.8.2 Summary of Application

DCD Tier 1: The Tier 1 information associated with this section is found in DCD Tier 1 Section 2.5.1, "Reactor Trip System and Engineered Safety Features Initiation," Section 2.5.2, "Diverse Actuation System," Section 2.5.3, "Qualified Indication and Alarm System," and Section 2.5.5, "Control System Not Required for Safety."

DCD Tier 2: The applicant provided a system description of the defense-in-depth and diversity analysis DCD Tier 2 Section 7.8, which is summarized in the following discussion.

The DAS executes the automatic reactor trip, ESF actuation, and alarm and display functions to address the potential for a software CCF and an ATWS. The DAS is a diverse I&C system from the safety-related I&C systems (PPS and ESF-CCS).

In the event of a software CCF, manual and automatic commands are initiated from the DAS and transmitted to the CIM) for signal prioritization and actuation of plant components. This path allows the actuation and control of safety-related systems by the operator in the event of a CCF of the safety-related I&C systems. CIM is credited as being diverse in operation from the Common Q Safety PLC platform used in the PPS and ESF-CCS. In addition, the CIM priority logic is developed using discrete logic gates. The CIM implements state-based priority in that for normal or accident condition except CCF, each command is generated by a logical OR of the

demand from the ESF-CCS with the demand from the DPS. When the resulting signals conflict (e.g., open vs close), the outputs are driven to the safe state which is selectable on a component basis. The manual diverse actuation signal blocks the command from ESF-CCS and DPS.

ITAAC: The ITAAC associated with DCD Tier 2 Section 7.8 are given in DCD Tier 1 Table 2.5.2-5, "Diverse Actuation System ITAAC."

Technical Specifications: There are no Technical Specifications associated with DCD Tier 2 Section 7.8.

7.8.3 Regulatory Basis

The design of diverse I&C systems shall meet the relevant requirements of the following Commission regulations:

1. GDC 1, 13, 19, 22, and 24

2. 10 CFR 50.55a(h)(3), "Safety Systems," requires compliance with IEEE Std 603-1991. For DAS isolated from safety-related systems, the applicable requirements of 10 CFR 50.55a(h)(3) are IEEE Std 603-1991, Clause 6.3, "Interaction Between the Sense and Command Features and Other Systems."

3. 10 CFR 50.62, "Requirements for reduction of risk from ATWS events for light-water-cooled nuclear power plants."

4. 10 CFR 52.47(b)(1), "Contents of applications; technical information," requires that a design certification contain the ITAAC that are necessary and sufficient to provide reasonable assurance that, if the inspections, tests, and analyses are performed and the acceptance criteria met, a plant that incorporates the design certification is built and will operate in accordance with the design certification, the provisions of the Atomic Energy Act of 1954, and NRC regulations.

The staff used the guidance listed below to assess the adequacy of the I&C D3 analysis to evaluate conformance to the applicable regulatory criteria:

1. SRP Section 7.8.

2. SRP BTP 7-19.

3. SRM to SECY-93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor Designs," Item 18, II.Q.

4. NUREG/CR-6303.

5. DI&C-ISG-04, Revision 1.

6. SRP Appendix 18-A, "Crediting Manual Operator Actions in D3 Analyses," Revision 0, November 2009.

7. NUREG-0711, "Human Factors Engineering Program Review Model," Revision 3, January 2012.

8. Generic Letter 85-06, “Quality Assurance Guidance for ATWS Equipment That Is Not Safety-Related,” and its enclosure, April 1985.

7.8.4 Technical Evaluation

The objectives of this review are to verify that the ATWS mitigation systems and equipment are designed and installed in accordance with the requirements of 10 CFR 50.62, and that other diverse I&C systems within the scope of this section comply with the Staff position on D3 for digital I&C systems. The staff verified the following:

- Adequate D3 has been provided within the design to meet NRC requirements.
- The displays and manual controls for critical safety functions initiated by operator action are diverse from those available on the computer systems used in the automatic portion of the protection systems.

7.8.4.1 Diverse System Description

The 10 CFR 50.62 requires, in part, that each pressurized water reactor must have equipment from sensor output to final actuation device that is diverse from the RTS to automatically initiate the auxiliary (or emergency) feedwater system and to initiate a turbine trip under conditions indicative of an ATWS, and for certain cases, requires a diverse scram system from the sensor output to interruption of power to the control rods.

The DCD Tier 2 Section 7.8, “Diverse Instrumentation and Control Systems,” states in part that the DAS consists of the diverse I&C systems that are provided to protect against potential software CCF of digital safety-related I&C systems including the PPS and ESF-CCS. It also states that the design has sufficient D3 to tolerate ATWS events or an AOO or a PA in concurrence with a software CCF that inhibits the digital safety-related I&C systems from performing their safety functions.

The staff found that there were several instances where the DCD Tier 1 design descriptions were inconsistent with DCD Tier 2 and other referenced technical reports with respect to how software CCF was addressed. Therefore, in RAI 33-7880, Question 07.08-2, the staff requested the applicant to revise Tier 1 information such that Tier 1 design is consistent with Tier 2 information. In the July 16, 2015, response to RAI 33-7880, Question 07.08-2 (ML15197A288), the applicant committed to revise Section 2.5.2.1 of DCD Tier 1 to state the following: “The DAS also mitigates the effects of a postulated [software CCF] within digital safety-related I&C systems.” The applicant also committed to revise Section 3.3.1 of the D3 TeR to state the following: “The DAS is designed to comply with the requirements of defense against a postulated CCF within digital safety-related I&C systems.” Based on the proposed changes to DCD Tier 1 and the D3 TeR, the staff finds that the applicant’s response to RAI 33-7880, Question 07.08-2, is satisfactory. The incorporation of the proposed markups into the next revision of the FSAR and the D3 TeR was a confirmatory item. The staff verified that the proposed markups have been incorporated into Revision 1 of DCD Tier 2 Section 7.8 and Revision 1 of the D3 TeR. As such, this confirmatory item has been satisfied.

The DAS consists of the DPS, the DMA switches, and the DIS. The DPS is provided to meet the requirements of 10 CFR 50.62 and hence helps ATWS mitigation. The DPS design includes the following functions: reactor trip, turbine trip, auxiliary feedwater actuation, and safety injection actuation. The DPS, DIS, and DMA switches help comply with the acceptance criteria in SRM to SECY-93-087 and SRP BTP 7-19. The DMA switches permit the operator to actuate

ESF systems in a timely manner from the MCR after a postulated CCF of the PPS and ESF-CCS. The DMA switches are located in the MCR for manual ESF actuation of critical safety functions. The DPS and DMA switches are independent and diverse from the PPS and ESF-CCS. The DPS and DMA switches are connected to the CIM to cope with a software CCF of the PPS and ESF-CCS. The DIS provides diverse indications to monitor critical variables. It also controls the heater power for proper heated junction thermocouple (HJTC) output signal level, when the software CCF of digital safety-related I&C systems occurs.

7.8.4.1.1 Diverse Protection System

The DPS is provided to reduce the risk from an ATWS event. The DPS design includes the following functions: reactor trip, turbine trip, auxiliary feedwater actuation, and safety injection actuation. These functions are provided to help the mitigation of an ATWS event and to mitigate the effects of a postulated CCF within the PPS and ESF-CCS.

The reactor trip function provides a diverse mechanism to decrease the risk from the ATWS events and mitigates the effects of a postulated software CCF of the digital computer logic within the PPS and ESF-CCS, concurrent with a steam line break inside containment. The DPS initiates an automatic reactor trip when either pressurizer pressure or containment pressure exceeds a predetermined value. These values can be found in Table 7.8-1 of DCD Tier 2 Section 7.8. The DPS also initiates a reactor trip on turbine trip (RTOTT) if the RPCS is out of service. The DPS RTOTT can be manually enabled from the DPS operator module (DPS-operator module) in the MCR. A 2oo4 logic design is used by the DPS to open the TCBs of the RTSS. This removes motive power to the CEDMs, as shown in Figures 7.8-1 and 7.8-2 of DCD Tier 2 Section 7.8. For reactor trip, the DPS energizes the shunt trip coil of the RTSS TCBs while the PPS de-energizes the undervoltage trip coil to cause the RTSS TCBs to open. The DPS manual reactor trip is provided to permit the operator to trip the reactor from the DPS-operator module in the MCR.

The turbine trip function is automatically initiated whenever the DPS reactor trip conditions are met. The DPS turbine trip signal is automatically generated with a 3-second time delay after initiation of the DPS reactor trip signal. DCD Tier 2 Section 7.8, Figure 7.8-2 shows a block diagram of the reactor trip and turbine trip circuitry; Figure 7.8-3 shows the DPS turbine trip signal.

The AFAS is initiated when the level in either of the two SGs decreases below a predetermined value. DCD Tier 2 Section 7.8, Table 7.8-1, gives this value. Each AFAS generated independently by the DPS and ESF-CCS gets prioritized in the CIM using state-based priority logic. Hence, either system can actuate the auxiliary feedwater. Electrical isolation is maintained between the DPS and CIM by providing isolation at the ESF-CCS loop controller cabinet. DCD Tier 2 Section 7.8, Figure 7.8-4, shows the DPS-AFAS.

The SIAS is initiated when the pressurizer pressure decreases below a predetermined value. DCD Tier 2 Section 7.8, Table 7.8-1 gives this value. Each SIAS generated independently by the DPS and ESF-CCS gets prioritized in the CIM using state-based priority logic. Hence, either system can actuate the SIS. Electrical isolation is maintained between the DPS and CIM by providing isolation at the ESF-CCS loop controller cabinet. DCD Tier 2, Section 7.8, Figure 7.8-5, shows the DPS-SIAS.

7.8.4.1.2 Diverse Manual ESF Actuation Switches

The DMA switches allow the operator to actuate ESF systems manually from the MCR. Hence, after a postulated CCF of the PPS and ESF-CCS, the ESF systems can be manually actuated in a timely manner. The DMA switches provide the following signals: the SIAS, MSIS, CIAS, CSAS, AFAS-1, AFAS-2, and signal for auxiliary feedwater flow/ SG level control. AFAS-1 is used for SG1 while AFAS-2 is used for SG2. DCD Tier 2, Section 7.8, Table 7.8-3, shows all the DMA signals. The DMA switches are hardwired to the CIM through the isolation devices and are independent and diverse from the safety-related system. The auxiliary feedwater flow/SG1 level and auxiliary feedwater flow/SG2 level are manual stations required to control auxiliary feedwater flow/SG level after the activation of diverse AFAS-1 and AFAS-2. The functions of the DMA switches are enabled by the DMA enable switch on the MCR safety console. DCD Tier 2 Section 7.8, Figure 7.8-6, shows the DMA switches block diagram.

7.8.4.1.3 Diverse Indication System

The DIS provides indications to monitor critical variables following a postulated software CCF of safety-related I&C systems. The DIS is independent from the APC-S and QIAS-P because the DIS receives its hardwired signal inputs through isolation devices in the APC-S and QIAS-P. The DIS is also diverse from the QIAS-P. Additionally, the DIS provides control functions of heater power for the proper HJTC output signal level. This helps the mitigation of the effects of a postulated software CCF of the QIAS-P. The DIS manual transfer switch is used to manually transfer the control function from the QIAS-P to the DIS. The DIS display and the DIS manual transfer switch are located on the MCR safety console. The DIS cabinet is classified as non-seismic equipment. However, the DIS HSI equipment on the MCR safety console is qualified as seismic Category II and powered by non-class 1E vital bus.

7.8.4.2 D3 Analysis for APR1400 I&C Systems

7.8.4.2.1 ATWS Diversity Evaluation

10 CFR 50.62 requires, in part, that each pressurized water reactor must have equipment from sensor output to final actuation device that is diverse from the RTS to automatically initiate the auxiliary (or emergency) feedwater system and to initiate a turbine trip under conditions indicative of an ATWS, and for certain cases, requires a diverse scram system from the sensor output to interruption of power to the control rods.

The DCD Tier 2 Section 7.8, “Diverse Instrumentation and Control Systems,” states that DAS design has sufficient D3 to tolerate the following beyond DBEs:

a. ATWS.

b. An AOO or a PA concurrent with a software CCF that prevents the safety-related I&C system from performing their required functions.

The DAS is comprised of the DPS, DMA, and DIS. DCD Tier 2 Section 7.8.1.1, “Diverse Protection System,” states that the DPS augments the PPS to meet the requirements of 10 CFR 50.62 for the reduction of risk from ATWS events. In addition, the DPS assists the mitigation of the effects of a postulated software CCF of the digital computer logic within the PPS and ESF-CCS. The D3 TeR, Section 5.1, “Diverse Protection System,” states, “The DPS is designed to mitigate the effects of an ATWS event characterized by an AOO concurrent with a failure of the protection system.”

The DPS initiates an automatic reactor trip when either pressurizer pressure exceeds 2400 pounds per square inch absolute (psia) or containment pressure exceeds 3 pounds per square inch gauge pressure (psig). The DPS automatically initiates a turbine trip whenever the DPS reactor trip conditions have been met. The DPS actuates the AFWS on low steam generator level (22.4 percent of wide range) in any of the steam generators. Hence, the DAS provides a diverse method to trip the reactor, trip the turbine, and initiate the AFWS on conditions indicative of an ATWS.

Therefore, staff finds DAS is the credited I&C system that provides the ATWS mitigation function required by 10 CFR 50.62. The staff used the diversity analysis guidance in NUREG/CR-6303 to evaluate the diversity of the DAS as compared to the PPS.

The diversity categories in NUREG/CR-6303 are:

- Design diversity,
- Equipment diversity,
- Functional diversity,
- Human diversity,
- Signal diversity, and
- Software diversity.

Design diversity is the use of different approaches, including software and hardware, to solve the same, or a similar, problem. The focus for this diversity category is on technology, approach, and architectural differences. Essentially, the design diversity attribute relates to technology choice and usage. This diversity category has three diversity attributes (listed in order of effectiveness) that contribute to diversity between two designs that meet the same or similar requirements:

- different technologies (e.g., analog versus digital),
- different approaches within the same technology (e.g., transformer-coupled alternating current instrumentation versus direct current-coupled instrumentation), and
- different architecture (i.e., arrangement and connection of components).

Equipment diversity is the use of different equipment to perform similar safety functions. The term “different" means sufficiently unlike, as to significantly decrease vulnerability to common failure. The diversity attributes for this diversity type, in order of effectiveness, are:

- different manufacturers of fundamentally different designs,
- same manufacturer of fundamentally different designs,
- different manufacturers making the same design, and
- different versions of the same design.

Equipment diversity acknowledges the features that contribute to diversity in the equipment essential to providing logic processing of functions. The focus for these criteria under the general "equipment" diversity attribute is on the type of logic processing equipment employed. These diversity attributes for this diversity type, in order of effectiveness, are:

- different logic processing equipment architecture,
- different logic processing version in the same architecture,
- different component integration architecture, and
- different data-flow architecture.

Functional diversity exists if two systems perform different physical functions though the physical functions may have overlapping safety effects. For example, cooling systems normally intended to function when containment is isolated are functionally different from other liquid control systems intended to inject coolant or borated water for other reasons. Three diversity attribute criteria (listed in decreasing order of effectiveness) that contribute to the diversity of functions between two independent systems, are:

- different underlying mechanisms,
- different purpose, function, control logic, or actuation means, and
- different response time scale.

Human diversity focuses on the life-cycle resources that constitute potential sources of systematic faults. The diversity attributes for this diversity category are:

- different design organizations/companies,
- different engineering management teams within the same company,
- different design and development teams, and
- different implementation and testing teams.

Signal diversity defines the use of different sensed parameters to initiate protective action, in which any of the parameters may independently indicate an abnormal condition, even if the other parameters fail to be sensed correctly. The diversity attributes for this diversity category are:

- different reactor or process parameters sensed by different physical effects,
- different reactor or process parameters sensed by the same physical effect, and
- the same reactor or process parameter sensed by a different redundant set of similar sensors.

Software diversity is defined as the use of different programs designed and implemented by different development groups with different key personnel to accomplish the same safety goals.

For example, use of two separately designed programs to compute when a reactor should be tripped. The diversity attributes for this diversity category are:

- different algorithms, logic, and program architecture,
- different timing and/or order of execution,
- different operating system, and
- different computer language.

Table 7.8-1: Diverse Platforms of I&C Systems

Platform	Subsystems	Comments
Common Safety PLC	PPS Bistable Processor PPS LCL Processor CPCS Processor RT Selective 2-out-of-4 Logic ESF-CCS GC and LC EDG Sequencer (Shed and Load) QIAS-P Controller QIAS-N Controller Operator Module (OM) Control Panel Multiplexers (CPM) ESF-CCS Soft Control Module (ESCM) Maintenance and Test Panel (MTP) Interface and Test Processor (ITP)	Digital system with operating system software and application software developed or commercially dedicated according to IEEE Std 7-4.3.2
Non-Safety DCS	Power Control System NSSS Process Control System BOP Process Control Process - Component Control System (P-CCS) Process Soft Control Workstation Information Processing System (IPS)	Digital system with operating system software and application software that is totally diverse from the common safety PLC
FLC	Diverse Protection System (DPS) Diverse Indication System (DIS)	FPGA-based digital systems without CPU and operating system software
Hardware Based Modules	APC-S Diverse manual ESF actuation (DMA) switches Component Interface Module (CIM) EDG Starting Circuit Ex-core Neutron Flux Monitoring System (ENFMS)	The platform is not a PLC based or implemented on an FPGA, but may not be analog circuitry (e.g., discrete integ-rated logic circuitry).
Analog Based Modules	Sensors ESF Component Actuated Devices Reactor Trip Switchgear Emergency Diesel Generator (EDG) EDG Output Breakers Offsite AC Power Crosstie Breakers Safety Channel Batteries Safety Channel Inverters	No software involved

Table 7.8-1 above, gives the various diverse platforms which are used in the plant I&C systems and the DAS. The D3 TeR, Section 6.2.1, “Diversity Evaluation between the DPS and the PS,” gives the detailed analysis results of diversity attributes between the DPS and the PPS.

The DPS is implemented on FLC. The PPS, on the other hand, is implemented on the common safety PLC platform which is dedicated for nuclear applications. The two platforms use different technology in order to provide design diversity. In the January 29, 2018 supplemental response provided by the applicant to RAI 33-7880, Question 07.08-1 (ML18029A859), the applicant provided further clarification in support of their claim that the PPS and DPS are diverse. The applicant stated that the FLC for the DAS uses hardware in the FPGA that is diverse from the hardware in the EEPROM-based programmable logic device (EPLDs) used in the common safety PLC platform. In addition to this, the FPGA for the DAS is programmed by a diverse programming tool as compared to the tool used to program the EPLD for the common safety PLC platform. The applicant committed to revise DCD Tier 1 Table 2.5.2-5 and Section 6.2.1 of the D3 TeR to incorporate the information provided in their supplemental response. Since the DPS and PPS are implemented using two diverse technologies the staff finds there is adequate design diversity between the DPS and PPS. The incorporation of the proposed markups into the next revision of the FSAR and the D3 TeR was a confirmatory item. The staff verified that the proposed markups have been incorporated into DCD Tier 1 Table 2.5.2-5 and Section 6.2.1 of the D3 TeR. As such, this confirmatory item has been resolved. The reactor trip mechanism of the DPS is also diverse from that of the PPS. For reactor trip, the DPS energizes the shunt trip coil of the RTSS TCBs and this breaks power to the CEDMs. The PPS de-energizes the undervoltage trip coil to cause the RTSS TCBs to open and break power to the CEDMs. Hence, there is functional diversity. DCD Tier 2 Section 7.2.1.9, “Diversity and Defense-in-Depth,” states in part that each RTSS circuit breaker has diverse methods of being automatically opened via the shunt trip and undervoltage trip devices. For additional diversity, the RTSS consists of one set of four RTSGs (RTSS 1) and another set of four RTSGs (RTSS 2) with diverse design features. The DPS manual reactor trip is provided to permit the operator to trip the reactor from the DPS-operator module in the MCR.

The D3 TeR, Section 5.1, “Diverse Protection System,” states:

> The DPS is designed to transmit reactor trip signals to a total of eight shunt trip devices of the RTSS 1 and RTSS 2 reactor trip breakers. The PPS transmits reactor trip signals to a total of eight undervoltage trip devices of the RTSS 1 and RTSS 2 reactor trip circuit breakers. Four trip circuit breakers of RTSS 1 are diverse from four trip circuit breakers of RTSS 2. This arrangement ensures the capability of [DPS] to interrupt power to the [CEDMs] regardless of the PPS failure to trip the reactor.

In RAI 342-8291, Question 07.08-8, the staff requested the applicant to describe the level and types of diversity between the RTSG and the RTCB. In the March 9, 2016, response to RAI 342-8291, Question 07.08-8 (ML16069A3830), the applicant stated that each RTSG contains a RTCB as part of the RTSG element. Diverse design mechanism between RTSGs in RTSS 1 and RTSGs in RTSS 2 will be established at the component procurement stage. For the further clarification, the applicant committed to revising Section 7.2.1.3 of DCD Tier 2 to state the following:

> The RTSGs in RTSS 1 are supplied from a different manufacturer than the RTSGs in RTSS 2, thereby providing reasonable assurance that a different actuation mechanism is used in the RTCBs in the two different sets of RTSGs.

Based on the clarification on how diversity will be achieved between the RTSGs in RTSS 1 and RTSGs in RTSS2 and proposed revisions to DCD Tier 2 Section 7.2.1.3, to include this clarification, the staff finds that the applicant's response to RAI 8291, Question 07.08-8, is satisfactory. The incorporation of the proposed markups into the next revision of the FSAR was a confirmatory item. The staff verified that the proposed markups have been incorporated into Revision 1 of DCD Tier 2 Section 7.2. As such, this confirmatory item has been satisfied.

Hardware description language (HDL) is used to program the DPS FLC whereas the PPS software is based on an application software run on top of an operating system. The staff finds using different programming languages for the DPS FLC and the PPS provides software diversity. The D3 TeR, Section 6.2.1, "Diversity Evaluation between the DPS and the PPS," also states that, "The DPS is designed and tested by different engineers of different design and test team from the PPS design and test team." Hence, human diversity is provided between the PPS and the DPS.

The acceptance criteria for the DPS ITAAC Item 2 on Table 2.5.2-5 (2 of 3) of DCD Tier 1, states, "The as-built DPS is developed by diverse design group from the design group(s) which developed the PPS and ESF-CCS software." The applicant did not describe what constitutes a diverse design group. Therefore, in RAI 33-7880, Question 07.08-1, the staff requested that the applicant provide definition(s) for diverse design group and define criteria the groups would need to meet in order to be considered diverse from one another. In the July 16, 2015, response to RAI 33-7880, Question 07.08-1 (ML15197A288), the applicant provided the following definition of "different design team":

- The DPS and PPS/ESF-CCS engineers belong to different engineering teams within the same I&C engineering department.
- Communications between the DPS and PPS/ESF-CCS design teams are controlled by the project office.
- Different system testers are assigned to test the DPS and PPS/ESF-CCS during development.

The applicant committed to revise Item 2 on Table 2.5.2-5 (2 of 3) of DCD Tier 1 to state the following: "The as-built DPS is developed by a different design team than the design teams which developed the PPS and ESF-CCS." Based on the proposed revisions to the DCD Tier 1 Table 2.5.2-5 to clarify what diverse design group means, the staff finds that the applicant's response to RAI 33-7880, Question 07.08-1, is satisfactory and human diversity is provided between the PPS and the DPS. The incorporation of the proposed markups into the next revision of the FSAR was a confirmatory item. The staff verified that the proposed markups have been incorporated into Revision 1 of DCD Tier 1 Table 2.5.2-5. As such, this confirmatory item has been satisfied.

Based on the credited diversity attributes and the diverse reactor scram actuation of DAS, the staff finds that the DAS design meets the diversity requirements of 10 CFR 50.62 to provide automatic auxiliary feedwater and turbine trip initiation and to interrupt power to the control rods using diverse equipment.

7.8.4.2.2 Evaluation of I&C System D3 Design

GDC 22 requires, in part, 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.

Item 18, II.Q of the SRM to SECY-93-087, Positions 1, 2, and 3, state that an applicant shall analyze each postulated common-[cause] failure for each event that is evaluated in the accident analysis section of the safety analysis report (SAR) using best-estimate methods and demonstrate that there is adequate diversity within the design for each of these events. If a postulated common-[cause] failure could disable a safety function, then a diverse means, with a documented basis that the diverse means is unlikely to be subject to the same common-[cause] failure, is required to perform either the same function or a different function. If applicable, the applicant should demonstrate that vulnerabilities to common-[cause] failures have been adequately addressed. NUREG/CR-6303 provides guidance for simplifying the I&C system for software CCF analysis and configuring appropriate I&C systems into blocks and selecting the appropriate I&C block(s) to postulate software CCF s concurrent with AOOs and postulated accidents. Concurrent failure of each set of identical blocks in all divisions should be postulated in turn, and the result of the failure should be documented as a finding of the analysis.

Table 7.8-2 Diversity Attributes between I&C System Platforms

Diverse I&C Platforms (Refer to Table A-1.)		Diversity Attributes against Common Safety PLC Platform					
		Design	Equipment	Functional	Human	Signal	S/W
Non-Safety DCS		O	O	O	O	O	O
FPGA	DPS	O	O	O	O		O
	DIS	O	O		O		O
Hardware Based Device (CIM)		O	O		O		N/A
Analog (Actuator)		O	O		O		N/A
Analog (Sensor)		O	O		O		N/A

O: Diverse, N/A: Not Applicable

Table 7.8-2 above provides a summary of the various diversity attributes which are shared in the design of the five different platforms used by the plant I&C systems.

The CCF Coping Analysis TeR, Section 4.2.2, “Available I&C Functions,” gives the following diverse plant functions and systems that remain available after a CCF in the safety-related I&C systems:

- DPS,
- Diverse Indication System,

- Diverse Manual ESF Actuation Switches,
- APC-S (both safety-related and non-safety),
- P-CCS (both automatic and manual functions),
- Manual Reactor Trip (in the MCR/ RSR),
- Local Manual Actions (at local equipment), and
- Indications, displays, and alarms provided in the IPS.

The staff used the diversity guidance of NUREG/CR-6303 to evaluate the adequacy of diversity within the I&C design. The diversity evaluation between the DPS and the safety related system has already been described in Section 7.8.4.2.1. The diversity evaluation between the DIS and the safety related system and the DMA switches and the safety-related system is given below.

7.8.4.2.3 Diverse Displays and Manual Controls

Item 18, II.Q, Point 4, of SRM to SECY-93-087 states that a set of displays and controls located in the MCR shall be provided for manual, system-level actuation of critical safety functions and monitoring of parameters that support the safety functions. These credited displays and controls shall be independent and diverse from the safety-related computer system. The guidance of SRP BTP 7-19 states that displays and manual controls provided for D3 conformance with Item 18, II.Q, Point 4 of SRM to SECY 93-087 should be sufficient both for monitoring the plant state and to enable control room operators to actuate the systems that will place the plant in a hot shutdown condition. In addition, the displays and controls should be sufficient for the operator to monitor and control the following critical safety functions:

- Reactivity control / level,
- Core heat removal,
- Reactor coolant inventory,
- Containment isolation, and
- Containment integrity.

The DCD Tier 2 Section 7.8, “Diverse Instrumentation and Control System,” states that, “The DMA switches are provided to permit the operator to actuate ESF systems in a timely manner from the MCR after a postulated CCF of the PPS and ESF-CCS.” The CCF Coping Analysis TeR, Section 4.2.2, “Available I&C Functions,” states, “The DMA switches provide protection against CCF of PPS and ESF-CCS implemented in accordance with [SRP] BTP 7-19 requirement of SRP. These DMA switches are implemented by manual, system level hardwired switches to manage the following critical safety functions: reactivity control, core heat removal, reactor coolant inventory, containment isolation, and containment integrity, addressed in SRP BTP 7-19.” The DMA switches are hardwired to the lowest level in order to achieve system-level actuation at the lowest level in ESF-CCS architecture.

- The DMA switches consist of following switches for system level actuation:

- Safety injection (2 trains)
- Containment spray
- Auxiliary feedwater (each SG)
- Main steam isolation (each SG)
- Containment isolation
- Letdown isolation

The DCD Tier 2 Section 7.8.1.3, "Diverse Indication System," states that, "The DIS provides functions to monitor critical variables following a postulated software CCF of safety-related I&C systems." It also states, "The DIS provides control functions of HJTC output signal level to assist the mitigation of the effects of a postulated software CCF of the QIAS-P. The control function is manually transferred from the QIAS-P to the DIS by the DIS manual transfer switch." Based on the information provided, the staff could not determine whether a software CCF of the QIAS-P could affect the transfer of HJTC control to the DIS. Therefore, in RAI 342-8291, Question 07.08-12, the staff requested that the applicant clarify whether the DIS manual transfer switch for HJTC control is safety or non-safety and address the potential for a software CCF of the QIAS-P to affect the transfer of HJTC control to the DIS. In the March 9, 2016, response to RAI 342-8291, Question 07.08-12 (ML16069A3830), the applicant stated following:

1. The DIS manual transfer switch for the HJTC heater power control is classified as non-safety equipment since the DIS is designed to be a non-safety system.

2. The QIAS-P is composed of a software-driven part and an analog part. The analog part includes the signal processing and conditioning circuits for both input signals from field sensors and transmitters and output signals for the HJTCs. The analog part of the QIAS-P also includes signal splitting and isolation devices both for forwarding core exit thermocouples (CETs)/HJTC signals to the DIS and for exchanging signals associated with the HJTC heater power control during a postulated software CCF of the software-driven part of the QIAS-P. The analog part includes no software-driven functions, and so is not susceptible to a postulated software CCF. A postulated software CCF of the software-driven part of the QIAS-P does not affect the function of the signal splitting and isolation devices for forwarding CET/HJTC signals to the DIS and for exchanging signals associated with the HJTC heater power control in the analog part of the QIAS-P (i.e., the HJTC heater power control transfer device and the HJTC heater power supply module shown in Figure 5-4). The software-driven part of the QIAS-P has neither an electrical link nor a signal interface with the DIS, and all the signal interfaces between the QIAS-P and DIS satisfy the physical separation and electrical isolation requirements of IEEE Std 384-1992, as endorsed by RG 1.75, Revision 3. Consequently, a postulated software CCF of the software-driven part of the QIAS-P does not adversely affect the DIS's ability to perform its diverse function of the HJTC heater power control, or operation of the manual transfer switch to switch the HJTC heater power control from the QIAS-P to the DIS.

The applicant committed to revising the "List of Figures" of the D3 TeR to add Figure 5-4, "DIS Signal Block Diagram." The applicant will also revise Section 5.2 of the D3 TeR to include the justification of why a software CCF would not affect the DIS's ability to perform its diverse

function of the HJTC heater power control or the transfer of HJTC heater power control function from the QIAS-P to the DIS. Therefore, since (a) a postulated software CCF of the software-driven portion of the QIAS-P does not affect the function of the signal splitting and isolation devices, (b) the software-driven part of the QIAS-P has neither an electrical link nor a signal interface with the DIS, and (c) all the signal interfaces between the QIAS-P and DIS satisfy the physical separation and electrical isolation requirements of IEEE Std 384-1992, as endorsed by RG 1.75, Revision 3, the staff finds that the applicant's response to RAI 342-8291, Question 07.08-12, is satisfactory. The incorporation of the proposed markups into the next revision of the D3 TeR was a confirmatory item. The staff verified that the proposed markups have been incorporated into Revision 1 of the D3 TeR. As such, this confirmatory item has been satisfied.

Diversity between DIS and safety-related computer system

The portion of the safety-related system that needs to be diverse from the DIS is the QIAS-P. The QIAS-P is part of the AMI which is provided to allow the operator to assess the state of the plant following DBEs by monitoring instruments, equipment, or systems that provide automatic action. The D3 TeR, Section 6.2.2, "Diversity Evaluation between the DIS and the QIAS-P," gives the detailed analysis results of diversity attributes between the DIS and the QIAS-P.

The DIS is implemented on FLC. Whereas, the QIAS-P is implemented on a PLC platform which is dedicated for nuclear applications. The use of two diverse platforms provides design diversity. HDL is used to program the DIS FLC whereas the PPS is based on an application software run on top of an operating system. The use of different programming languages provides software diversity. The D3 TeR, Section 6.2.2, "Diversity Evaluation between the DIS and the QIAS-P," also states that DIS is designed and tested by different engineers of different design and test team from the QIAS-P. Hence, human diversity is provided for the development of the PPS and DPS.

However, the CETs/HJTCs signals are routed through QIAS-P before it is received at the DIS. These signal inputs are used to measure the temperature of the RCS and the coolant level of the Reactor Vessel. The staff needed to verify that a software CCF of the QIAS-P wouldn't prevent the DIS from performing its intended safety function and that the DIS would still receive the CETs/HJTCs hardwired signals in case of a postulated software CCF of the QIAS-P. In RAI 33-7880, Question 07.08-3, the staff requested that the applicant demonstrate that by routing the CETs/HJTCs signals through the QIAS-P, the DIS would still be able to meet Item 18, II.Q, Point 4 of the SRM on SECY 93-087 in case of a potential software CCF of the QIAS-P and DIS. The applicant also had to demonstrate that the DIS would still receive the CETs/HJTCs hardwired signals in case of a postulated software CCF of the QIAS-P. In the July 16, 2015, response to RAI 33-7880, Question 07.08-3 (ML15197A290), the applicant stated that the DIS is independent from the safety-related computer system including the QIAS-P, because the entire signal path from field sensors to input modules of the DIS uses hardwires and analog components without the involvement of the computer part of the QIAS-P. All the CET and HJTC signals come from field sensors to the QIAS-P via hardwires. The signals to be delivered to the DIS are routed through pairs of signal splitters and isolators which are software CCF-free analog components, and then routed to the output terminals in the QIAS-P cabinet.

Since the entire signal path from field sensors to input modules of the DIS uses hard wires and analog components without the involvement of the computer part of the QIAS-P, even in case of a postulated software CCF of the QIAS-P, the signal path will not be affected and the DIS will still receive the CET and HJTC signals. The CET and HJTC signals come from sensors in the

reactor vessel and go directly to the QIAS-P. This information is further explained in the applicant's response to RAI 33-7880, Question 07.08-4; and RAI 342-8291, Question 07.08-12. The applicant has committed to including this information in the next revision of the FSAR. Therefore, since (a) a postulated software CCF of the software-driven portion of the QIAS-P does not affect the function of the signal splitting and isolation devices, (b) the software-driven part of the QIAS-P has neither an electrical link nor a signal interface with the DIS, (c) all the signal interfaces between the QIAS-P and DIS satisfy the physical separation and electrical isolation requirements of IEEE Std 384-1992, as endorsed by RG 1.75, Revision 3, and (d) the applicant provided design commitments in the response to RAI 33-7880, Question 07.08-4, the staff finds that the applicant's response to RAI 33-7880, Question 07.08-3, is satisfactory. RAI 33-7880, Question 07.08-3, is closed and resolved.

The DIS also receives variables from the APC-S. The APC-S also sends signals from the safety sensors to safety-related systems such as the PPS, ESF-CCS Loop Controller, and QIAS-P. The D3 TeR, Section 5.1, states, "The safety class sensors and APC-S are analog equipment." The staff found that the applicant did not provide sufficient information to demonstrate that the APC-S is analog equipment and that it cannot be affected by a software CCF of the safety-related system. The applicant also did not provide sufficient information to demonstrate that the DIS is capable of receiving necessary variables if the APC-S is affected by a software CCF. Therefore, in RAI 33-7880, Question 07.08-4, the staff requested that the applicant demonstrate the communication and functional independence between the DIS and the APC-S and QIAS-P. In the July 16, 2015, response to RAI 33-7880, Question 07.08-4 (ML15197A290), the applicant stated that the APC-S is a safety-related software CCF-free analog system that provides signal conditioning/splitting for the field sensor signals. The APC-S also provides isolation functions when signals are split to non-safety systems such as the DIS, using the analog components. The QIAS-P is divided into computer and analog parts. The computer part provides safety-related displays in accordance with its own design requirements. The analog part is software CCF-free and provides signal conditioning/splitting for the CETs/HJTCs, and isolation functions for split signals sent to the DIS. The analog part also exchanges signals associated with the manual switchover of the HJTC heater power control with the DIS during software CCF of the computer part of the QIAS-P. The input signals of the DIS flows through the APC-S and the analog part of the QIAS-P. During software CCF conditions, the DIS can perform its required functions since the APC-S and the analog part of the QIAS-P are able to provide the hard-wired input signals to the DIS without being affected by the software CCF. Therefore, since the APC-S is an analog equipment and thus not susceptible to software CCF, the staff concludes that there is functional independence between the systems.

Item 18, II.Q, Point 4 of the SRM to SECY-093-87 states that the displays and controls shall be independent and diverse from the safety computer system. The safety computer system in the APR1400 I&C design including the PPS, CPCS, ESF-CCS, and the digital part of the QIAS-P can be affected by a software CCF. This safety computer system has neither a communication link nor an interface with the DIS. The safety computer system is designed to use a safety common platform based on PLC while the DIS utilizes a FLC-based platform. Hence, the DIS is independent and diverse from the safety computer system. In addition, the DIS receives only the hardwired analog signal inputs (no digital signal) from the APC-S and the analog part of the QIAS-P. Random failures of the APC-S and the analog part of the QIAS-P are not assumed to occur at the same time as a software CCF of the safety computer systems. The APC-S and the analog part of the QIAS-P can provide the input signals to the DIS even if there is a software CCF. This allows the DIS to perform its required functions. Therefore, since the functionality of the DIS is not affected by a software CCF of the software-driven portion of the QIAS-P (staff

evaluated the applicant's response to RAI 342-8291, Question 07.08-12), the staff concludes that the DIS is functionally independent from the computer based portion of the QIAS-P. The applicant proposed to modify Tier 2 Section 7.8.1.3 of the FSAR to include the basis presented in the response to RAI 33-7880, Question 07.08-4. The incorporation of the proposed markup into the next revision of FSAR was a confirmatory item. The staff verified that the proposed markups have been incorporated into Revision 1 of DCD Tier 2 Section 7.8. As such, this confirmatory item has been satisfied.

In the July 16, 2015, response to RAI 33-7880 Question 07.08-5 (ML15197A290), the term "functional programmable unit" was introduced, including a definition for it. The term was defined as a computer that consists of one or more associated processing units and a peripheral equipment, as defined in Section 3.1.8 of IEEE Std 7-4.3.2-2003. The response explains that if the equipment doesn't have any functional programmable units, it is not susceptible to a software CCF. The applicant stated that since the APC-S didn't have any functional programmable unit it is not susceptible to a software CCF. The staff found that the definition of functional programmable unit provided in this response does not provide sufficient clarity to demonstrate that the APC-S and other similar systems are not susceptible to a software CCF. Specifically, it was not clear whether the term "functional programmable unit" is equivalent to the staff's definition of common software as defined in SRP BTP 7-19. SRP BTP 7-19 states, "In this guidance, common software includes software, firmware, and logic developed from software-based development systems." In RAI 342-8291, Question 07.08-11, the staff requested clarification as to why any system in the APR1400 design that doesn't have a "functional programmable unit," is not susceptible to a software CCF. The staff also requested further clarification with regards to the APC-S and its non-susceptibility to software CCF in comparison to what the staff considers as software as defined in SRP BTP 7-19.

In the March 9, 2016, response to RAI 342-8291, Question 07.08-11 (ML16069A3830), the applicant stated that the APC-S is conventional analog equipment which does not include any 'functional programmable unit' as Section 3.1.8 of IEEE Std 7-4.3.2-2003. In addition, the APC-S does not use any "common software," such as software, firmware, and logic developed from software-based development systems. The signal conditioning/ splitting and isolating devices of the APC-S are conventional analog circuits which do not include any firmware or logic developed from software-based development systems. Therefore, the APC-S is not susceptible to a postulated software CCF. The applicant committed to revise Section 4.1.1.5 of the Safety I&C System TeR to state the following:

> The signal conditioning/splitting and isolating devices of the APC-S are conventional analog circuits which are not developed from software-based development systems. Therefore, the APC-S is not susceptible to a postulated [software CCF].

The applicant committed to revise Sections 5.1, 8, and 9 of the D3 TeR to state the following:

> The safety class sensors and the APC-S are conventional analog equipment which do not include any functional programmable unit, as defined in IEEE Std [7-4.3.2-2003]. In addition, the APC-S does not use any common software. The signal conditioning/splitting and isolating devices of the APC-S are conventional analog circuits which do not include any firmware or logic developed from software-based development systems. Therefore, the safety class sensors and APC-S are not susceptible to a postulated software CCF.

The applicant also committed to revise Section 8 of D3 TeR to include references to IEEE Std 7-4.3.2-2003 and IEEE 100 (Seventh Edition), "The Authoritative Dictionary of IEEE Standards Terms." The applicant committed to revise Section 9 of the D3 TeR to include definitions for functional programmable unit, common software, and firmware.

Based on the clarification of the technology used for the APC-S and the added definitions of functional programmable unit, common software, and firmware to the D3 TeR, the staff finds that the applicant's response to RAI 342-8291, Question 07.08-11, is satisfactory. The incorporation of the proposed markup into the next revision of the D3 TeR and the Safety I&C System TeR was a confirmatory item. The staff verified that the proposed markups have been incorporated into Revision 1 of DCD Tier 2 Section 7.8, Revision 1 of the Safety I&C System TeR, and Revision 1 of the D3 TeR. As such, this confirmatory item has been satisfied.

Based on the information provided regarding the DIS and its independence and diversity from safety-related I&C systems susceptible to software CCF, the staff finds the DIS is sufficiently diverse from the safety-related system to meet the requirements of Item 18, II.Q, Point 4 to the SRM on SECY-093-87.

<u>Diversity between DMA and safety-related computer system</u>

Per Item 18, II.Q, Point 4 to the SRM on SECY-093-87, the DMA switches need to be diverse from the ESFAS functions of the PPS and ESF-CCS. The DMA switches are implemented by using conventional switches which are hardwired directly to the CIM through isolators. Whereas, PPS and ESF-CCS are implemented on the common PLC platform which is dedicated for nuclear applications. The CCF Coping Analysis TeR, Section 4.2.2, "Available I&C Functions," states:

> To achieve system-level actuation independently and diversely from the ESF-CCS, the DMA switches are connected to the lowest level in the ESF-CCS architecture.

The two platforms are diverse and hence there is design diversity.

There is no software associated with the DMA switches, while the PPS/ESF-CCS is implemented using a software based platform. Hence, there is software diversity between the DMA switches and the PPS/ESF-CCS. Also, the ESF signals from the DMA switches are directly connected to the CIM using hardwired cables while the ESF signals from the PPS/ESF-CCS are generated using the common safety PLC platform. The signals from the DMA switches and the PPS/ESF-CCS are combined in the CIM. The ESF signals from the DMA switches are based on manual operator action while the ESF signals from the PPS/ESF-CCS is based on input from sensors. Hence, there is signal diversity. The DMA switches are designed and tested by different design and test team from the PPS/ESF-CCS design and test team. Hence, there is also human diversity. Based on the credited diversity attributes the staff finds that the DIS and DMA design meets the diversity provisions of the SRM to SECY-93-087, Item 18, II.Q, Point 4 and SRP BTP 7-19, Point 4.

The CIM receives its component control signals from the DPS, DMA switches, and ESF-CCS. CCF Coping Analysis TeR, Section 4.2.2, states, "The CIM is a non-software-based qualified nuclear safety grade module. Therefore the CIM is not subjected to the same CCF with ESF-CCS which is implemented by qualified PLC platform. The CIM provides the priority logic function between ESF-CCS actuation signals and DMA switch signals and also provides the interface function from the ESF-CCS to the plant component."

The staff found that the applicant did not provide sufficient information to demonstrate and verify that the CIM is not subject to the same CCF as the PPS and ESF-CCS. Therefore, in RAI 342-8291, Question 07.08-6, the staff requested that the applicant verify whether the statement made in the D3 TeR, regarding the CIM being fully tested meets the 100 percent combinatorial testing criteria for software-based systems, as specified in SRP BTP 7-19, or demonstrate that the CIM does not need to conform to this guidance. In the April 18, 2016, response to RAI 342-8291, Question 07.08-6 (ML16109A371), the applicant referenced the CIM TeR, Section 2, third paragraph which states in part:

> The CIM consists of three sections: priority logic section, base section, and diagnosis section. The priority logic section and base section are implemented by hardware device and the design is fully tested. In addition, the diagnosis section does not provide any inputs to the priority or base sections. Therefore, there is no potential for a hardware or software design defect in these sections.

The applicant proposed to add a new section (Section 5.4, "Priority Logic Development Testing") to the CIM TeR. This section will explain that the CIM priority logic section is fully tested to ensure there are no design defects in the priority logic configuration. The test cases will confirm that the logic generates the correct Energize/De-energize output states by encompassing all input signal state combinations, together with (1) all Input Select Switch and Mode Select Switch combinations, and (2) the logic states of any internal latches and time delays. To facilitate this testing, all input and switch states will be manually or automatically stimulated. The Energize/De-energize output states of the priority logic will be manually or automatically compared to manually generated acceptance states. If an automated comparison method will be employed, the automated test results will be manually verified by sampling the test cases.

In the November 18, 2016, supplemental response to RAI 342-8291, Question 07.08-6 (ML16323A505), the applicant revised Section 2 of the CIM TeR. The statement regarding fully testing the CIM was removed and further explanation about the functions of each section of the CIM was provided. This further clarified that the priority section of the CIM does not contain any software and that it is not susceptible to the same CCF as the PPS and ESF-CCS. Also, since the applicant claimed that the CIM does not contain any software, there is no need to perform 100 percent combinatorial testing. Based on the clarification from the response that the CIM does not contain any software and that that it is not susceptible to the same CCF as the PPS and ESF-CCS, the staff finds that the applicant's response to RAI 342-8291, Question 07.08-6, is satisfactory. The incorporation of the proposed markup into the next revision of D3 TeR and CIM TeR was a confirmatory item. The staff verified that the proposed markups have been incorporated into Revision 1 of the D3 TeR and Revision 1 of the CIM TeR. As such, this confirmatory item has been satisfied.

7.8.4.3 D3 Best-Estimate Analysis

The 10 CFR 50.62 requires, in part, diverse equipment to automatically respond to ATWS events. GDC 22 requires in part that the effects of postulated accident conditions on redundant channels do not result in loss of the protection function and 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.

Item 18, II.Q, Point 2 of the SRM to SECY-93-087 states:

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

The staff evaluated the ability of the applicant's credited I&C D3 mitigation systems to mitigate AOOs and PAs, concurrent with a CCF of the PPS/ESF-CCS. To address the D3 mitigation plant response to a CCF of the PPS, staff used the guidance found in SRP BTP 7-19, Section B.3, Items 1 and 2. The staff also used the guidance in NUREG/CR-6303 to evaluate the adequacy and sufficiency of credited I&C system diversity to address the acceptance criteria of SRP BTP 7-19. NUREG/CR-6303, Guidelines 5 and 6 describe the method for postulating CCF of the I&C system using the block diagram of the protective system.

The CCF Coping Analysis TeR, Section 5, "CCF Coping Analysis," states in part that the acceptance criteria required by SRP BTP 7-19 are met for all AOOs and PAs with a CCF in the safety-related I&C systems. The CCF is conservatively postulated to exist before the events occur and to prevent the safety-related I&C systems from providing any mitigating actuation and control of their associated safety equipment. The D3 TeR, Section 7.1, "Event Evaluation Methods," states:

> The evaluation consists of two phases. The first phase consists of a qualitative evaluation to identify the events that require more detailed analysis using computer program. The second phase consists of a quantitative analysis for those events that are determined to require further analysis by the qualitative evaluation phase.

The section also further gives the major characteristics of the realistic evaluation methodology different from DCD Tier 2, Chapters 6 and 15 safety analysis. They are summarized below:

a. A CCF of the digital safety-related I&C systems is postulated, such that reactor trip functions implemented in the RPS and the ESF functions implemented in the ESF-CCS do not actuate. The failure includes both automatic and manual actuation (except for the hardwired diverse manual ESF actuation and the hardwired manual reactor trip).

b. Additional independent single failure is not assumed in the evaluation. According to SRP BTP 7-19, all safety-related and non-safety systems or components independent from the CCF are assumed to function correctly.

c. The initiating event is the malfunction of the control system or a controlled component within the plant system.

d. Initial conditions for an event are at their nominal values. The nominal or average capacities are assumed when some systems or components are actuated during the event.

e. The postulated CCF in the digital PPS/ESF-CCS does not prevent the reactor trip on high pressurizer pressure or high containment pressure and the diverse turbine trip which are actuated by the DPS. The DPS uses digital equipment and software that are diverse from the PPS and ESF-CCS.

f. The postulated CCF in the digital PPS/ESF-CCS does not prevent the auxiliary feedwater and SIS actuation functions which are actuated by the DPS.

g. Hardwired diverse ESF manual actuations at the system level are provided for:

- Safety Injection,
- Containment Spray,
- Auxiliary Feedwater Actuation,
- Main Steam Isolation,
- Containment Isolation, with Letdown Isolation, and
- RCPs are assumed to be normally operating if offsite power is available.

h. Offsite power is assumed to be available during the event if LOOP is not the initiating event.

i. It is assumed that no operator action is taken during 30 minutes after an event initiation. At 30 minutes after the event, the operators begin administrative control of the plant under the appropriate recovery procedures to achieve a hot shutdown condition. Alarms and indications are provided via equipment not affected by the postulated CCF in the digital safety-related I&C systems to support operators to perform a controlled cooldown of the plant.

j. A postulated CCF in similar software modules results in similar blocks failing in the same manner, i.e., similar software blocks do not fail in a random manner.

In Section 5.1 of the CCF Coping Analysis Technical Report, the applicant identifies a two-step methodology for the D3 analysis: The first step is to do a qualitative evaluation for all the Chapter 15 DBEs. If this step reasonably demonstrates that the applicable acceptance criteria are met then no further analysis is done. If, however, the first step indicates that the course of the event, assuming a CCF in the RPS, may be different from the corresponding Chapter 15 analysis, then a detailed analysis using computer programs is conducted. The detailed analysis is performed with best-estimate assumptions utilizing NRC-approved codes, i.e., the same codes that are used in the FSAR Chapter 15 analyses.

Section 5.3 of the CCF Coping Analysis TeR provides the D3 qualitative evaluation results and Section 5.4 of the CCF Coping Analysis TeR provides the quantitative analysis for those events found to require further analysis in Section 5.3 of the CCF Coping Analysis TeR. The applicant considered each of the following categories of events in the two-step methodology:

- Increase in Heat Removal by Secondary System,
- Decrease in Heat Removal by Secondary System,
- Decrease in Reactor Coolant Flow Rate,
- Decrease in RCS Flow Rate,

- Reactivity and Power Distribution Anomalies,
- Increase in RCS Inventory,
- Decrease in RCS Inventory, and
- Radioactive Material Release from a Subsystem or Component.

The staff reviewed the applicant's D3 evaluation in accordance with SRP BTP 7-19. This was done to confirm that each event analysis was done appropriately and that the applicant's D3 evaluation demonstrates adequate diversity.

7.8.4.3.1 Increase in Heat Removal by Secondary System

The DBEs evaluated in this category of events are:

- Decrease in Feedwater Temperature,
- Increase in Feedwater Flow,
- Increase in Steam Flow,
- Inadvertent SG safety relief valve (SRV) Opening, and
- Steam System Piping Failure.

All these events are classified as AOOs with the exception of the steam system piping failure, which is a PA.

In Section 5.3.1.1 of the CCF Coping Analysis TeR, the applicant provided an engineering calculation demonstrating that the decrease in feedwater temperature (due to the loss of a feedwater heater train) results in a rise in reactor power to a level that is below the preset required overpower margin (ROPM). The ROPM is the power level which can be accommodated without fuel failure. Also, since the RCS temperature becomes lower during the event, the RCS pressure will also be lower; hence, the RCS pressure boundary is maintained. Based upon the staff's review of the applicant's D3 evaluation, the staff determined that a decrease in feedwater temperature event concurrent with a CCF does not challenge the D3 of the digital safety-related I&C systems; therefore, no further analysis of this event is required by the applicant.

For the increase in feedwater flow event (Section 5.3.1.2 of the CCF Coping Analysis TeR), the staff reviewed the applicant's analysis which showed that the ROPM is not clearly sufficient to cover the estimated power increase due to the increased feedwater flow. As a result, the applicant determined that a detailed quantitative analysis is warranted. The applicant provided the detailed quantitative analysis in Section 5.4.2.1 of the CCF Coping Analysis TeR. The staff reviewed the detailed analysis and determined that the core power increased to a new steady-state value just below the ROPM and that the RCS pressure initially decreased but subsequently increased to near the initial pressure. The minimum departure from nucleate boiling (MDNBR) remained well above the SAFDL and the RCS pressure limit was not challenged. Based on the staff's review of the applicant's detailed quantitative analysis, the staff concluded that an increase in feedwater flow event concurrent with a CCF does not challenge the D3 of the digital safety-related I&C systems.

The staff reviewed the applicant's analysis for the increase in main steam flow event (Section 5.3.1.3 of the CCF Coping Analysis TeR) and the inadvertent opening of a steam generator relief or safety valve event (Section 5.3.1.4 of the CCF Coping Analysis TeR). Since the reactor power increase for both events is the same, i.e., no more than 11 percent per FSAR Section 15.1.3.3.3, and is well below the ROPM, the staff determined that the DNBR SAFDL is not challenged. Since the RCS temperature initially decreases during these events, but will be restored to the nominal value by the pressurizer pressure control system, the staff also determined that the RCS overpressure limit is not challenged. Based on the staff's review of the applicant's qualitative analysis, the staff concluded that neither the increase in main steam flow event concurrent with a CCF, nor the inadvertent opening of a steam generator relief or safety valve event concurrent with a CCF, challenges the D3 of the digital safety-related I&C systems; therefore, no further analysis of these events is required by the applicant.

The staff reviewed the qualitative analysis provided by the applicant for a steam system piping failure inside and outside containment event (Section 5.3.1.5 of the CCF Coping Analysis TeR). The applicant determined that a detailed quantitative analysis is necessary to address the steam line break (SLB) event outside containment (Section 5.4.2.2 of the CCF Coping Analysis TeR) and inside containment (Section 5.4.2.8 of the CCF Coping Analysis TeR) because it expects that the consequences for the SLB with a CCF can be worse than that for the case presented in DCD Tier 2, Sections 6.2, and 15.1.5. The staff reviewed the applicant's SLB outside containment, which assumed full power reactor operation with D3 best-estimate conditions. The analysis showed that the reactor power undergoes a large power increase for about 13 minutes before a reactor trip by the DAS's high pressurizer pressure trip logic. The applicant concluded that a small amount of fuel experiences departure from nucleate boiling (DNB) and is therefore considered to fail. The applicant calculated the radiological consequences based upon the assumed fuel failures. During the staff's review of the applicant's calculation, the staff noted that the applicant did not provide enough information regarding the calculation of the amount of fuel which underwent DNB, i.e., the staff could not confirm that the applicant's source term for the radiological analysis was adequate. Therefore, on January 28, 2016, the staff issued RAI 379-8476, Question 07-1, to address this issue (ML16028A041). In the March 3, 2016, response to this RAI (ML16063A210), the applicant stated that a statistical convolution method was used to determine the amount of failed fuel rods. The staff noted that the resulting two-hour exclusion area boundary and eight-hour low population doses were given and were well below the 10 CFR 50.34 guidelines. The response provides the information sought and is therefore acceptable. RAI 379-8476, Question 07-1, is closed and resolved.

The staff also reviewed the SLB analysis for a break inside containment (Section 5.4.2.8 of the CCF Coping Analysis TeR). The staff's review regarding the acceptability of the mass and energy release code for containment response is documented in Section 6.2.1.4 of this SER. The staff noted that for this beyond DBE, the peak containment pressure is less than the American Society of Mechanical Engineers (ASME) factored load category limit. The applicant's analysis of the SLB inside containment shows that the DPS high containment pressure trip setpoint is reached within four seconds after accident initiation, resulting in reactor trip. The response of the RCS and the core were not presented as part of the applicant's SLB inside containment analysis. The staff finds this acceptable because the RCS and core response for the SLB inside containment is bounded by the SLB outside containment. Based on the staff's review of the applicant's detailed quantitative analyses, the staff concludes that a steam system piping failure inside and outside of containment concurrent with a CCF does not challenge the D3 of the digital safety-related I&C systems.

Based upon the staff's review of the increase in RCS heat removal events, the staff finds:

- the applicant's D3 analyses demonstrate adequate diversity, and
- there are no credited operator actions either cited or determined by this evaluation to be required as a diverse means of protective action.

7.8.4.3.2 Decrease in Heat Removal by Secondary System

The DBEs evaluated in this category of events are:

- Loss of External Load/Turbine Trip,
- Loss of Condenser Vacuum,
- Closure of Main Steam Isolation Valve,
- Loss of Non-Emergency Alternating Current Power,
- Loss of Normal Feedwater Flow, and
- Feedwater System Pipe Break.

All these events are classified as AOOs, with the exception of the Feedwater system pipe break, which is a PA.

In Section 5.3.2.1 of the CCF Coping Analysis TeR, the applicant provided a qualitative analysis to address the loss of external load. The staff reviewed this qualitative analysis to determine if a detailed quantitative analysis was necessary. In FSAR Chapter 15, the analysis of this event conservatively assumed that the NSSS control systems were in manual mode when the event occurred. When the NSSS control systems are not in manual mode (i.e., available), the event will be accommodated without a reactor trip. Furthermore, if the NSSS control systems were assumed to be in manual mode, the event would be terminated by the DAS high pressurizer pressure trip. Based on the staff's review of the applicant's qualitative analysis, the staff determined that the loss of external load event concurrent with a CCF does not challenge the D3 of the digital safety-related I&C systems; therefore, no further analysis of this event is required by the applicant.

The staff reviewed the applicant's qualitative analysis of the turbine trip event (Section 5.3.2.2 of the CCF Coping Analysis TeR) concurrent with a CCF. The staff determined that the turbine trip event has the same effect as the loss of load event; thus, a turbine trip does not challenge the D3 of the digital safety-related I&C systems and no further analysis is required by the applicant.

The staff reviewed the applicant's qualitative analysis of the loss of condenser vacuum event concurrent with a CCF. Based on the staff's review, the staff determined that the event concurrent with a CCF would be less limiting than the same event analyzed in DCD Tier 2 Section 15.2 because the NSSS control systems would be available to retard the RCS pressure increase. If the RCS pressure increased to the pressure trip setpoint despite normal control measures, the reactor would be tripped by the DAS high pressurizer pressure trip. The DAS low steam generator level trip is also available to mitigate this event. Furthermore, the staff determined that this event does not challenge the D3 of the digital safety-related I&C systems and that no further analysis of this event is required by the applicant.

The staff reviewed the applicant's qualitative analysis on the inadvertent closure of the MSIVs event and determined that the event is similar to the Loss of Condenser Vacuum event except that the steam flow is terminated more slowly. Since the DAS high pressurizer pressure trip provides protection from RCS overpressure, the staff was able to determine that this event does not challenge the D3 of the digital safety-related I&C systems; therefore, no further analysis of this event is required by the applicant.

The staff reviewed the applicant's qualitative analysis on the loss of non-emergency ac power to station auxiliaries' event addressed in Section 5.3.2.6 of the CCF Coping Analysis TeR. The staff noted that the DAS provides a high pressurizer pressure trip, which, in conjunction with the pressurizer safety valves, provides protection against over pressurization of the RCS. Furthermore, the loss of non-emergency ac power to the motor-generator sets results in the drop of the control rods by gravity into the core. Based on the staff's review, the staff determined that this event does not challenge the D3 of the digital safety-related I&C systems; therefore, no further analysis of this event is required by the applicant. The staff reviewed the applicant's qualitative evaluation for the loss of normal feedwater flow event (Section 5.3.2.7 of the CCF Coping Analysis TeR). The staff noted that although the CCF disables the RPS trips on high pressurizer pressure and low SG level, the event is mitigated by the corresponding trip in the DAS. The NSSS control systems will also act during this event to mitigate the transient. Based on the staff's review, the staff determined that this event does not challenge the D3 of the digital safety-related I&C systems; therefore, no further analysis of this event is required by the applicant.

The staff reviewed the applicant's qualitative analysis for the postulated accident of a feedwater system piping failure. The staff noted that the containment pressure for this event is bounded by the SLB event which discharges higher energy flow to the containment than a feedwater line break. The staff also noted that RCS overpressure protection is provided by the DAS pressurizer high pressure trip and the pressurizer safety valves. Based on the staff's review, the staff determined that this event does not challenge the D3 of the digital safety-related I&C systems; therefore, no further analysis of this event is required by the applicant.

Based on the staff's review of the DBEs evaluated under the decrease in heat removal by secondary system category, it can be seen that these events are either bounded by FSAR Chapter 15 analysis or various protective functions of the DAS. Hence, the staff finds:

- the applicant's D3 analyses demonstrate adequate diversity; and,
- there are no credited operator actions either cited or determined by this evaluation to be required as a diverse means of protective action.

7.8.4.3.3 Decrease in Reactor Coolant Flow Rate

The DBEs evaluated in this category of events are as follows.

- Partial Loss of Forced RCS Coolant Flow,
- Complete Loss of Forced RCS Coolant Flow, and
- RCP Rotor Seizure or RCP Shaft Break.

The loss of forced RCS flow events are classified as AOOs and the pump seizure or shaft break event is classified as a PA. In all three events, the sudden drop in reactor core flow results in a challenge to the DNBR SAFDL.

The staff reviewed the applicant's qualitative analysis regarding the loss of forced reactor coolant flow in Section 5.3.3.1 of the CCF Coping Analysis TeR. The staff noted that in FSAR Section 15.3.1, the corresponding DBE analysis, the loss of power to all of the RCPs is more severe than the loss of power to a single RCP. The Chapter 15 analysis of the event shows that a RPS reactor trip actuation occurs on low RCP shaft speed. However, this RPS trip is not available due to the assumed CCF. The staff also noted that since the event can only be initiated by a complete LOOP, power to the CEDM would be lost and the CEAs would fall into the core by gravity after coil decay in the CEDM. Because of the time delays associated with this process, the applicant concluded that the Chapter 15 event analysis may not be limiting. Therefore, the applicant conducted a detailed quantitative analysis using CESEC-III and CETOP, which are computer codes reviewed as part of Chapter 15 of this SER. The staff reviewed the applicant's detailed analysis, presented in Section 5.4.2.3 of the CCF Coping Analysis TeR. The detailed analysis showed that, while the decline in DNBR was greater than that shown in FSAR Chapter 15, the MDNBR was higher because the initial DNBR value was higher. The staff noted that the higher initial DNBR was a result of using best estimate assumptions. The staff subsequently noted that the MDNBR remained above the SAFDL during the transient. Based on the staff's review of the applicant's detailed quantitative analysis, the staff concluded that this event concurrent with a CCF does not challenge the D3 of the digital safety-related I&C systems.

The staff reviewed the applicant's qualitative analysis of an RCP rotor seizure presented in Section 5.3.3.3 of the CCF Coping Analysis TeR. The applicant describes a plausible course of events following RCP rotor seizure. In the Chapter 15 analysis of the event, a reactor trip on low RCS flow is triggered by the RPS within 2 seconds. Since the low RCS flow trip is not available in the DAS, the RCS flow would be maintained at about 75 percent; therefore, the applicant determined that a detailed quantitative analysis is warranted. The applicant provided the detailed analysis of the RCP rotor seizure in Section 5.4.2.4 of the CCF Coping Analysis TeR. The staff noted that in the FSAR Chapter 15 analysis, the MDNBR occurred within 3.5 seconds of the start of the event, whereas in Section 5.4.2.4 of the CCF Coping Analysis TeR the applicant states that the MDNBR did not occur until 178.6 seconds after event initiation, just before a new quasi-steady power level is reached. The staff also noted that in Figure 5-25 of the CCF Coping Analysis TeR, the MDNBR occurs right after the event initiation (<5 seconds), not at 178.6 seconds. Therefore, on January 28, 2016, the staff issued RAI 379-8476, Question 07-2, to address this inconsistency (ML16028A041). In the March 3, 2016, response to this RAI (ML16063A210), the applicant stated that the staff's observation was correct and committed to revising section 5.4.2.4.2.c of the CCF Coping Analysis TeR. The proposed revision was presented as part of the RAI response. The staff determined that the revision is acceptable and tracked RAI 379-8476, Question 07-2, as a confirmatory item. The staff verified that the proposed markups have been incorporated into Revision 1 of the CCF Coping Analysis TeR. As such, this confirmatory item has been satisfied.

The staff noted that the steady-state power level is nearly the same as the initial power level during the RCP rotor seizure event concurrent with a CCF, but the flow is approximately 25 percent lower. Due to the best-estimate assumption of nominal power peaking factors, the initial DNBR is 1.7 times higher than that assumed in the FSAR Chapter 15 analysis. Furthermore, the staff noted that the MDNBR does not challenge the DNBR SAFDL. Since the reactor does not trip but remains stable for 30 minutes, the operators have sufficient time to take

manual control of the plant and execute a controlled cooldown. Based on the staff's review of the applicant's detailed quantitative analysis, the staff concluded that this event concurrent with a CCF does not challenge the D3 of the digital safety-related I&C systems.

The staff reviewed the applicant's qualitative analysis of an RCP shaft break event presented in Section 5.3.3.4 of the CCF Coping Analysis TeR. The staff noted that an RCP shaft break event is very similar to an RCP rotor seizure event, in that the RCS flow rate decreases from its nominal steady state value due to failure of an RCP. Despite the different failure modes of a rotor seizure event and shaft break event, in an RCP shaft break event, the RCP rotor is still capable of rotating freely, thereby offering less resistance to flow during the rapid RCS flow decrease. Thus, the results of a shaft break event are conservatively less severe than for a rotor seizure event. Based on the staff's review, the staff determined that this event does not require further analysis by the applicant because the detailed quantitative analysis for the RCP rotor seizure event bounds the RCP shaft break event; furthermore, the staff concluded that the quantitative analysis for the RCP rotor seizure event concurrent with a CCF demonstrates adequate D3 of the digital safety-related I&C systems.

Based on the staff's review of the decrease in RCS flow rate events, the staff finds:

- the applicant's D3 analyses demonstrate adequate diversity; and,
- there are no credited operator actions either cited or determined by this evaluation to be required as a diverse means of protective action.

7.8.4.3.4 Reactivity and Power Distribution Anomalies

The DBEs evaluated in this category of events are:

- Uncontrolled CEA Withdrawal from Subcritical or Low-Power Startup Condition.
- Uncontrolled CEA Withdrawal at Power.
- CEA Mis-operation.
- Startup of an Inactive RCP at an Incorrect Temperature.
- CVCS Malfunction Resulting in Decreased RCS Boron Concentration.
- CEA Ejection.

All these events are classified as AOOs with the exception of the CEA Ejection, which is categorized as a PA.

The staff reviewed the applicant's evaluation of the uncontrolled CEA withdrawal from subcritical or low-power startup condition event, which is provided in Section 5.3.4.1 of the CCF Coping Analysis TeR. The applicant states that the evolution of the event would be similar to that presented in Section 15.4.1 of the FSAR, but because nominal conditions are assumed for the CCF event, the pressurizer pressure would initially be 75 psi higher in the CCF event. The applicant concludes that the D3 high pressurizer pressure trip would terminate the event prior to the DNBR SAFDL being reached and that no detailed computer analysis is needed. However, the staff noted that in Figure 15.4.1-3 of the FSAR the RCS pressure response shows a peak pressure of approximately 2250 psia at approximately 33 seconds (where the high pressurizer

pressure trip setpoint is 2377 psia). Furthermore, the staff noted that in Figure 15.4.1-4 of the FSAR, the MDNBR occurred at approximately 30 seconds following a variable overpower trip. Because the MDNBR occurs approximately 3 seconds before peak pressure is obtained in the Chapter 15 analysis of the event, and because the DNBR decreases at a rapid rate prior to the trip, the staff was unable to conclude that the CCF event transient could be arrested via the DPS high pressurizer pressure trip before a DNBR SAFDL would be violated.

Therefore, on January 28, 2016, the staff issued RAI 379-8476, Question 07-3, to address this issue (ML16028A041). In the May 31, 2016, response to this RAI (ML16152B040), the applicant provided a detailed computer analysis of the uncontrolled CEA withdrawal from subcritical or low-power startup condition event using realistic assumptions and methods, as allowed by SRP BTP 7-19 Point 2. The analysis showed that the peak pressure was well below the acceptance criterion of 193.34 kg/cm^2 (2750 psia) and the MDNBR remained above the MDNBR limit of 1.29 and slightly above the value determined in the FSAR analysis of the event. Relative to the FSAR analysis, reactor trip was later in the coping analysis and peak reactor power was higher. However, the use of a realistic power peaking factor and moderator temperature coefficient, along with assuming no LOOP kept the MDNBR higher than the FSAR value. Therefore, (a) since the MDNBR was greater than the DNBR SAFDL value of 1.29 (therefore, no violation of the SAFDL value) and (b) since RCS pressure remains within 110 percent of the system design pressure of 2750 psia (therefore, the integrity of the reactor coolant pressure boundary is maintained), the staff finds the applicant's response acceptable. RAI 379-8476, Question 07-3, is closed and resolved.

The staff reviewed the applicant's evaluation of the uncontrolled CEA withdrawal at power event, which is provided in Section 5.3.4.2 of the CCF Coping Analysis TeR. The applicant concluded that this event need not be analyzed because its evaluation is essentially similar to the evaluation of the event at subcritical or low power conditions. Pending the resolution of RAI 379-8476, Question 07-3, the staff was unable to conclude that an uncontrolled CEA withdrawal at power (with software CCF) was less limiting than the event at low power or startup conditions (with software CCF). Therefore, on January 28, 2016, the staff issued RAI 379-8476, Question 07-4, to address this issue (ML16028A041). In the May 31, 2016, response to this RAI (ML16152B040), the applicant provided a qualitative analysis, discussing how the FSAR analysis of the event would change if only a DPS high pressurizer pressure trip were available to terminate the event, and realistic initial conditions and equipment availability assumptions were used. In addition, the applicant provided a detailed quantitative analysis of the event which showed large margins to the acceptance criteria (RCS pressure and MDNBR limits). The staff finds the applicant's response acceptable. RAI 379-8476, Question 07-4, is closed and resolved.

The staff reviewed the applicant's qualitative evaluation of a single dropped CEA, which is presented in Section 5.3.4.3 of the CCF Coping Analysis TeR. The staff noted that in the FSAR analysis, no reactor trip occurs and the DNB SAFDL is not violated. Since the RPS is not active in this event, a CCF in that system would not affect the course of the event. The staff was able to determine that this event does not challenge the D3 of the digital safety-related I&C systems; therefore, no further analysis of this event is required by the applicant. The staff reviewed the applicant's qualitative evaluation of a single withdrawn CEA, which is presented in Section 5.3.4.4 of the CCF Coping Analysis TeR. The staff noted that no reactor trip functions or ESF actuation functions are required for mitigation of this event; thus, the Chapter 15 analysis bounds the CCF event. The staff was able to determine that this event does not challenge the D3 of the digital safety-related I&C systems; therefore, no further analysis of this event is required by the applicant.

The staff reviewed the applicant's qualitative evaluation of the startup of an inactive RCP event, which is presented in Section 5.3.4.5 of the CCF Coping Analysis TeR. The staff noted that the RPS is not needed to mitigate the event; therefore, a CCF in the RPS has no effect and the CCF event is bounded by the Chapter 15 analysis. The staff was able to determine that this event does not challenge the D3 of the digital safety-related I&C systems; therefore, no further analysis of this event is required by the applicant.

The staff reviewed the applicant's qualitative evaluation of an inadvertent deboration event, which is presented in Section 5.3.4.7 of the CCF Coping Analysis TeR. The staff noted that the Chapter 15 analysis of this event concludes that the RPS high pressurizer pressure trip will provide event termination via a reactor trip in modes 1 and 2. Furthermore, in the event of a CCF in the RPS, the DPS high pressurizer pressure trip will terminate the transient. The staff also noted that for modes 3 through 6, the Chapter 15 analysis shows that mode 4 results in the shortest time for detection and termination of the event, i.e., 72.8 minutes. The staff concluded that since the operator has sufficient time beyond the 30 minutes assumed for earliest operator action to recognize and terminate the boron dilution, then the inadvertent deboration event concurrent with a CCF for modes 3 through 6 does not pose a threat to reactor safety. The staff was able to determine that this event does not challenge the D3 of the digital I safety-related I&C systems; therefore, no further analysis of this event is required by the applicant.

The staff reviewed the applicant's qualitative evaluation of an inadvertent loading of a fuel assembly into the improper position event, which is presented in Section 5.3.4.8 of the CCF Coping Analysis TeR. The staff noted that the RPS is not needed to mitigate the event; thus, a CCF in the RPS has no effect on the outcome of this transient. The staff was able to determine that this event does not challenge the D3 of the digital safety-related I&C systems; therefore, no further analysis of this event is required by the applicant.

The staff reviewed the applicant's qualitative evaluation of a CEA ejection accident, which is presented in Section 5.3.4.9 of the CCF Coping Analysis TeR. The staff noted that the applicant also conducted a detailed quantitative analysis in Section 5.4.2.5 of the CCF Coping Analysis TeR as a result of the qualitative evaluation being inconclusive regarding safety performance in the course of a CEA ejection event concurrent with CCF. The staff reviewed the quantitative analysis and determined that the applicant's use of best-estimate assumptions (e.g., nominal power peaking factors) makes the course of the event such that reactor trip does not occur. Furthermore, the fuel SAFDLs are never challenged. The staff was able to determine that this event does not challenge the D3 of the digital safety-related I&C systems.

Based on the staff's review of the reactivity and power distribution anomalies events, the staff finds the following.

- the applicant's D3 analyses demonstrate adequate diversity and,
- there are no credited operator actions either cited or determined by this evaluation to be required as a diverse means of protective action, although operator actions are required to bring the plant to a safe shutdown condition.

7.8.4.3.5 Increase in RCS Inventory

The DBEs evaluated in this category of events are:

- Inadvertent Operation of the SIS.
- CVCS Malfunction that Increases RCS Inventory.

These two events are categorized as AOOs.

The staff reviewed the applicant's qualitative evaluation of the inadvertent operation of the ECCS event concurrent with a CCF, which is presented in Section 5.3.5.1 of the CCF Coping Analysis TeR. The staff noted that since best estimate conditions (e.g., nominal full power) are assumed, the SIS injection pumps do not have sufficient head to deliver flow into the RCS. Furthermore, if the transient took place with the RCS pressure below the SI pump shutoff head, the SIS would increase RCS inventory and pressure until the RCS pressure became greater than the SI pump shutoff head (with the SDC system isolated). If the transient occurred with the shutdown cooling system in operation, the shutdown cooling relief valves would mitigate the pressure transient. Additionally, the staff noted from the Chapter 15 analysis of this transient that if this event occurred at low RCS temperatures, brittle facture limits would not be violated. Lastly, the staff noted that there are no reactor trip functions or ESF actuation functions required to mitigate this event. The staff was able to determine that this event does not challenge the D3 of the digital safety-related I&C systems; therefore, no further analysis of this event is required by the applicant.

The staff reviewed the applicant's qualitative evaluation of the CVCS malfunction that increases RCS inventory event, which is presented in Section 5.3.5.2 of the CCF Coping Analysis TeR. The applicant utilizes the results of the FSAR Section 15.5.2, "non-LOOP CVCS Malfunction that Increases RCS Inventory," analysis to evaluate the pressurizer level response assuming a CCF in the digital I&C systems. The staff noted that the pressurizer is calculated to take more than 30 minutes to fill, i.e., there is sufficient time for the operator to take action to isolate the CVCS. Assuming CVCS is not isolated, the DAS high pressurizer pressure trip will provide protection for the primary system integrity by tripping the reactor. The pressurizer SRVs (PSRVs) also provide overpressure protection for water solid conditions with RCS letdown isolated. The staff was able to determine that this event does not challenge the D3 of the digital safety-related I&C systems; therefore, no further analysis of this event is required by the applicant.

Based on the staff's review for the increase in RCS inventory category of events, the staff finds:

- the applicant's D3 analyses demonstrate adequate diversity; and
- there are no credited operator actions either cited or determined by this evaluation to be required as a diverse means of protective action.

7.8.4.3.6 Decrease in RCS Inventory

The DBEs evaluated in this category of events are as follows.

- Inadvertent Opening of a PSRV.
- Failure of Small Lines Carrying Primary Coolant Outside the Containment.
- SGTR.
- LOCAs.

The inadvertent opening of a PSRV event is classified as an AOO and the SGTR and LOCA events are classified as PAs.

The staff reviewed the applicant's qualitative evaluation of an inadvertent opening of a PSRV event, which is presented in Section 5.3.6.1 of the CCF Coping Analysis TeR. The staff noted that this event is covered by a LOCA (Section 5.3.6.5 of the CCF Coping Analysis TeR). The staff reviewed the D3 LOCA analysis concurrent with a CCF below. The staff reviewed the applicant's evaluation of the break of a letdown line outside containment event, which is presented in Section 5.3.6.2 of the CCF Coping Analysis TeR. The staff noted that there are multiple alarms to alert the operator that the line has broken. These alarms are not affected by a CCF in the RPS. In the Chapter 15 analysis, the applicant conservatively assumed that operator action, closing the letdown line isolation valves, does not occur until thirty minutes after event initiation. Furthermore, the staff noted that there are no RPS trips or ESFAS trips required for mitigation of the event. The staff was able to determine that this event does not challenge the D3 of the digital safety-related I&C systems; therefore, no further analysis of this event is required by the applicant.

The staff reviewed the applicant's qualitative evaluation of the SGTR event, which is presented in Section 5.3.6.3 of the CCF Coping Analysis TeR. The staff noted that this event challenges the radiological release limits and poses the potential for SG overfill with water entering the main steam lines. The applicant's qualitative evaluation concludes that a detailed quantitative analysis is required. The staff reviewed the applicant's quantitative analysis of a SGTR concurrent with a CCF in Section 5.4.2.6 of the CCF Coping Analysis TeR. The staff noted that the same manual actions credited in the FSAR Section 15.6.3 analysis are available in the D3 analysis with a CCF in the RPS. The operator is assumed to manually trip the reactor at 30 minutes. The SGTR analysis focuses on calculation of DNBR since the radiological consequences for the DBA are bounded by the FSAR Section 15.6.3 if no fuel failure occurs. The staff noted that the radiological results of the D3 SGTR analysis are bounded by the Chapter 15 analysis due to the D3 analysis assumption that the turbine bypass system is available for cooldown (i.e., turbine bypass discharges to the main condenser as opposed to the MSSV discharging directly to atmosphere as assumed in the Chapter 15 analysis). The D3 analysis shows that the minimum DNBR is well above the fuel SAFDL; therefore no fuel fails and the Chapter 15 analysis bounds the D3 analysis. Furthermore, the staff noted that during this event with a CCF, steam generator overfill is prevented by normal operation of the FWCS prior to operator intervention. The staff was able to determine that this event does not challenge the D3 of the digital safety-related I&C systems.

The staff reviewed the applicant's qualitative evaluation of a LOCA concurrent with a CCF, which is presented in Section 5.3.6.5 of the CCF Coping Analysis TeR. The staff noted that the applicant concluded that a detailed quantitative analysis is warranted. The staff reviewed the results of the detailed quantitative analysis of the large break LOCA, presented in Section 5.4.2.7 of the CCF Coping Analysis TeR. The analysis shows that the DPS SIS actuation (low pressurizer pressure) results in four safety injection pumps injecting flow in addition to the flow from the SIT.

The staff noted that because best-estimate core conditions and availability of all four trains of SI are assumed in the D3 analysis, the Chapter 15 analysis of large break LOCA event remains bounding.

The staff noted that the applicant did not present a detailed qualitative nor quantitative evaluation for a small break LOCA concurrent with a CCF. In addition, for the D3 analysis of small break LOCA, an RCP trip will not occur due to the assumed CCF in the RPS. The lack of automatic RCP trip for small break LOCA is not in conformance with TMI Action Plan Item II.K.3.5 (NUREG-0737). However, the staff has accepted manual RCP trip for small break

LOCA based, for example, on zero degrees hot leg subcooling indication (Generic Letter 85-12). Therefore, on January 28, 2016, the staff issued RAI 379-8476, Question 07-5, to address this issue (ML16028A041). In the March 17, 2016, response to this RAI (ML16077A309), the applicant described the operator actions that will be taken as part of the EOP. Specifically, the RCPs remain in operation until they are manually tripped by the operator when RCS subcooling is less than the minimum setpoint. The staff noted that this EOP is in accordance with staff guidance; therefore, the staff determined that the applicant's response is acceptable. RAI 379-8476, Question 07-5, is closed and resolved.

Based on the staff's review of the decrease in RCS inventory events, the staff finds the following.

- the applicant's D3 analyses demonstrate adequate diversity, and
- there are no credited operator actions either cited or determined by this evaluation to be required as a diverse means of protective action.

7.8.4.3.7 Radioactive Material Release from a Subsystem or Component

In regard to radiological consequences of design basis accidents, the staff reviewed the two transients for which the applicant calculated fuel failure, that is, the SGTR and the SLB outside containment events, which are presented in Section 5.4.2.6 and 5.4.2.8 of the CCF Coping Analysis TeR, respectively. The staff noted that the calculated exclusion area boundary and low population zone doses are less than those reported in FSAR Chapter 15, and are below the criteria specified in 10 CFR 52.47 (a)(2)(iv).

The staff evaluated the inside containment release events (LOCA, SLB, CEA ejection), and noted that the DAS provides the manual containment isolation function credited in the FSAR analysis to limit offsite dose consequences. Considering the use of best-estimate assumptions for the D3 analyses versus the conservative FSAR assumptions (e.g., coincident LOOP, reactor coolant iodine and noble gas activity levels at plant Technical Specification limits, conservative iodine spiking factor, bounding failed fuel fractions assumed in the FSAR) the staff determined that the radiological consequences of inside containment release events meet the D3 acceptance criteria.

The staff evaluated the events that result in radiological release outside of containment, i.e., the small line break, the SGTR, the main steam line break, and the fuel handling accident. The staff noted that the small line break does not cause fuel failure, and since the FSAR Section 15.6.2.5 analysis of the small line break conservatively assumes iodine and noble gas activity levels at plant Technical Specification limits, the applicant's D3 analysis is bounded by the Chapter 15 analysis. Similarly for a SGTR event, the staff determined that the corresponding Chapter 15 analysis is bounding.

The staff noted the fuel handling accident (categorized as a PA) does not involve a reactor trip and considering the conservative assumptions used in the Chapter 15 analysis, the staff determined that the Chapter 15 analysis remains bounding.

For these reasons, the staff finds that the applicant's D3 analysis criteria on radiological consequences are met.

The staff has reviewed the D3 analyses of DBEs as submitted by the applicant in the CCF Coping Analysis TeR. The staff's review has addressed the effects of software CCF in the

safety-related I&C system on the results and consequences of the FSAR Chapter 15 safety analysis.

The staff concludes that the APR1400 protection system is designed with adequate diversity such that the occurrence of a DBE concurrent with a software CCF in the safety-related I&C system will not result in consequences exceeding the acceptance criteria Points 1 and 2 as specified in SRP BTP 7-19. This conclusion supports the staff's overall review of FSAR Section 7.8, "Diverse I&C Systems," based on compliance with portions of 10 CFR 50.55a(h)(3) and GDC 21, 22, 24, and 29, applicable to this safety evaluation.

7.8.4.4 Manual Actions for D3

GDC 19, "Control Room," states that a control room shall be provided from which actions can be taken to operate the nuclear power unit safely under normal conditions and to maintain it in a safe condition under accident conditions, including LOCAs.

To address Point 3 of the NRC four-point D3 policy stated in the SRM to SECY-93-087, Item 18, II.Q, for disabled safety functions due to a CCF of the protection system, the D3 design should provide a "diverse means" to perform either the same function or a different function. The staff's position, as stated in SRP BTP 7-19, Section 3.5, states:

> If manual operator actions are used as the diverse means or as part of the diverse means to accomplish a safety function, a suitable HFE analysis should be performed by the applicant to demonstrate that plant conditions can be maintained within recommended acceptance criteria for the particular AOO or postulated accident. The acceptability of such actions is to be reviewed by the NRC staff in accordance with Appendix 18-A of SRP Chapter 18, "Crediting Manual Operator Actions in D3 Analyses"…For complex situations and for actions with limited margin, such as less than 30 minutes between time available and time required, a more focused staff review will be performed.

Therefore, the applicant can credit manual operator actions, performed from the MCR, as a diverse means to perform the safety function that would have been performed by the failed protection system. Upon the staff's review of the applicant's D3 plant response provided in the D3 TeR and design information provided in DCD Tier 2 Section 7.8, the staff could not identify any manual operator actions that were credited within 30 minutes of an event initiation as a diverse means to perform the disabled safety functions as required by Point 3 of the NRC's D3 policy.

7.8.4.5 Independence from protection systems

The guidance of SRP Section 7.8 states that diverse actuation systems functions should be independent and diverse from the RTS and ESFAS. ATWS mitigation systems should be diverse from the RTS. For ATWS mitigation systems, 10 CFR 50.62 requires diversity from the sensor output to the final actuation device.

For diverse actuation systems isolated from safety-related systems, the applicable requirements of 10 CFR 50.55a(h)(3) are IEEE Std 603-1991, Clause 6.3, "Interaction Between the Sense and Command Features and Other Systems." 10 CFR Part 50, Appendix A, GDC 24, "Separation of Protection and Control Systems," as it relates to assuring the protection system is 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 of the protection system as well as assuring that interconnection of the protection and control systems is limited to assure that safety is not significantly impaired.

Diversity between the DPS and the PPS is discussed in Section 7.8.4.2.1 of this SER. Diversity between the DMA switches and the ESFAS is discussed in Section 7.8.4.2.3 of this SER. Electrical, physical and communications isolations are maintained between the safety-related system and the DAS as evaluated in Section 7.1.4.10 of this SER. In the locations where sensors are shared between the safety-related I&C system and the DAS, the qualified isolators in the APC-S prevent a DAS failure from affecting the safety-related system.

The DPS is electrically isolated and physically separated from the protection system. The DPS uses signals from safety class sensors. These signals pass through isolators located at the APC-S and from there go onto the DPS signal processing modules. The APC-S also sends signals from the sensors to safety-related systems such as the PPS, ESF-CCS loop controller and QIAS-P. However, independence is maintained between the DPS and the safety equipment by the isolators in the APC-S.

Similarly, the DIS receives its analog inputs from signal splitters/isolators in the APC-S as well QIAS-P channel A. This is via a hardwired connection. The isolators ensure that a non-safety signal from the DIS doesn't have detrimental effect on a safety signal or safety-related system. The staff needed to understand how the DIS is independent from the APC-S and QIAS-P when it receives signals from those systems. Therefore, in RAI 33-7880, Question 07.08-4, the staff requested that the applicant demonstrate the communication and functional independence between the DIS and the APC-S and QIAS-P. The evaluation of the applicant's response to this RAI is documented in Section 7.8.4.2.3 of this SER.

The DMA signals are hardwired directly to the CIM module via isolators. The CIM also receives component control signals from the ESF-CCS and DPS. The CCF Coping Analysis TeR, Section 4.2.2, states, the ESF-CCS commands to Port X in the CIM are terminated and diverse actuation commands from the DPS to Port Y in the CIM are terminated. The D3 TeR, Section 5.1, states that isolation is provided at the ESF-CCS loop controller cabinet to maintain electrical isolation between the DPS and the CIM. Based on the above information, the staff finds that the DAS is independent from the RTS and ESFAS. The DAS meets the applicable requirements of 10 CFR 50.55a(h)(3) and 10 CFR Part 50, Appendix A, GDC 24.

7.8.4.5.1 Diverse Power Supplies

10 CFR 50.62 requires that ATWS equipment be independent from the existing RTS. The guidance of SRP Section 7.8 states that logic and actuation device power for the ATWS mitigation system should be from an instrument power supply independent from the power supplies for the existing RTS. Each DPS cabinet is located in a separate room. Each DPS channel is powered from two redundant non-Class 1E vital buses that are independent from Class 1E vital buses.

The staff found that it is unclear whether the power supplies for the DAS are diverse and independent from the power supplies for the RTS and whether a software CCF of the safety-related system could the DAS power source. Therefore, in RAI 342-8291, Question 07.08-13, the staff requested that the applicant clarify whether a software CCF of a safety-related I&C system could result in a loss of power to the DAS and consequently prevent

the DAS from performing its diverse functions. In the March 9, 2016, response to RAI 342-8291, Question 07.08-13 (ML16069A383), the applicant stated that the power source for the DPS and the DIS is the non-Class 1E 120 volts alternating current (Vac) I&C power system which supplies continuous, reliable, and regulated alternating current power to the plant non-safety I&C equipment while the power source for the DMA switches is the Class 1E 120 Vac I&C power system which supplies continuous, reliable, and regulated alternating current power to the plant safety-related I&C equipment (including the PPS and ESF-CCS). Both Class 1E and non-Class 1E 120 Vac I&C power systems consist of inverters, regulating transformers, manual/automatic transfer switches, and distribution panels, as shown in DCD Tier 2, Figures 8.3.2-3 and 8.3.2-4, respectively. The non-Class 1E 120 Vac I&C power system has backup battery power and continuously provides 120 Vac power to the DPS and the DIS during a LOOP event. The battery capacities related with the Class 1E and non-Class 1E 120 Vac I&C power systems are described in DCD Tier 2 Table 8.3.2-4. The non-Class 1E 120 Vac I&C power system, which provides its output power to the DPS and the DIS, is independent from the Class 1E 120 Vac I&C power system. In addition, the non-Class 1E 120 Vac I&C power system does not use any software or firmware used in the Class 1E I&C systems. Therefore, the non-Class 1E 120 Vac I&C power system is not susceptible to a postulated software CCF caused by any of the safety-related I&C systems.

The Class 1E 120 Vac I&C power system continuously provides 120 Vac power to the interposing relays of the CIM that interfaces with the DMA switches. The Class 1E 120 Vac I&C power system is provided power from the direct current control center of the Class 1E 125 ventilation duct chase (Vdc) power system. Following a LOOP event, the EDG provides power to the direct current control center. If there is a station blackout due to EDG failure concurrent with a LOOP event, the alternate alternating current gas turbine generator provides power to the direct current control center for either the A or the B safety train. Additionally, the Class 1E 125 Vdc power system has battery backup power. The design information regarding the Class 1E 125 Vdc power system and the Class 1E 120 Vac I&C power system is described in DCD Tier 2 Section 8.3.2.1.2. The Class 1E 120 Vac I&C power system provides its output power to Class 1E I&C systems, including the APC-S, PPS, CIM, and ESF-CCS. The Class 1E 120 Vac I&C power system does not use any firmware or software within the system. Moreover, the equipment platform for the Class 1E 120 Vac I&C power system is diverse from the equipment for the safety-related I&C systems. Therefore, a software CCF which occurs within the safety-related I&C systems does not cause a failure of the Class 1E 120 Vac I&C power system.

Hence the characteristics of the DAS power supply systems are summarized as follows.

- Backup/alternate power sources are available during LOOP event (i.e., battery backup for the DPS and DIS; battery and EDG backups for the DMA switches).

- No software CCF is possible; the power supply systems do not use common software or firmware used in the safety related I&C systems.

The applicant will revise Sections 5.1, 5.2 and 5.3 of the D3 TeR in order to provide all the information contained in their response to RAI 342-8291, Question 07.08-13. Based on the information provided in the applicant's response, the staff concludes that power to the DAS can be continuously supplied regardless of a postulated software CCF or LOOP event. As such, the staff finds that the applicant's response to RAI 342-8291, Question 07.08-13, is satisfactory. The incorporation of the proposed markup into the next revision of the D3 TeR was a confirmatory item. The staff verified that the proposed markups have been incorporated into

Revision 1 of the D3 TeR. As such, this confirmatory item has been satisfied. The staff finds that the logic and actuation device power for the ATWS mitigation system is from an instrument power supply independent from the power supplies for the existing RTS and thus meets the requirements of 10 CFR 50.62.

7.8.4.6 Diverse I&C System Quality Assurance

10 CFR 50.62 states, in part, that diverse ATWS equipment must be designed to perform its function in a reliable manner. Generic Letter 85-06, "Quality Assurance Guidance for ATWS Equipment That Is Not Safety-Related," April 1985, provides acceptable guidance for the quality assurance of diverse I&C systems and components. The SRM to SECY-93-087, Item 18, II.Q, Point 3, states that automated backup system credited to mitigate CCFs may be performed by a non-safety system if the system is of sufficient quality to perform the necessary function(s) under the associated event conditions.

10 CFR Part 50, Appendix A, GDC 1, "Quality Standards and Records," states:

> Structures, systems, and components important to safety shall be designed, fabricated, erected, and tested to quality standards commensurate with the importance of the safety functions to be performed. Where generally recognized codes and standards are used, they shall be identified and evaluated to determine their applicability, adequacy, and sufficiency and shall be supplemented or modified as necessary to assure a quality product in keeping with the required safety function. A quality assurance program shall be established and implemented in order to provide adequate assurance that these structures, systems, and components will satisfactorily perform their safety functions. Appropriate records of the design, fabrication, erection, and testing of structures, systems, and components important to safety shall be maintained by or under the control of the nuclear power unit licensee throughout the life of the unit.

The DCD Tier 2 Section 7.8.2.1, "Diverse Protection System," states that, "The DPS is the non-safety system designed with augmented quality, as defined by Generic Letter 85-06. The software associated with the DPS is identified as ITS, as described in the Software Program Manual Technical Report." The definition for ITS can also be seen in the QAM and Quality Assurance Program Description. The DPS is composed of four channels (one cabinet for each channel). Each DPS cabinet is located in a separate room. Each DPS channel is powered from two redundant non-Class 1E vital buses that are independent from Class 1E vital buses. Each DPS channel can also be tested manually without causing component actuation during plant operations.

DCD Tier 2 Section 7.8.2.2, "Diverse Manual Engineered Safety Features Actuation Switches," states that, "The DMA switches provide the non-safety functions, but they are designed with augmented quality, as defined by Generic Letter 85-06." The DMA switches are: (1) designed with Class 1E qualified hardware with augmented quality, (2) seismically qualified, and (3) energized using Class 1E power.

The DCD Tier 2 Section 7.8.2.3, "Diverse Indication System," states that the DIS is a non-safety system designed with augmented quality, as defined by Generic Letter 85-06. The software associated with the DIS is identified as ITS as described in the Software Program Manual Technical Report. The DIS HSI equipment on the MCR safety console is qualified as seismic

Category II and powered by non-class 1E vital bus. The testing requirements of Generic Letter 85-06 and the conformance of the DAS to those requirements are described below in Section 7.8.4.7 of this SER.

Based on this information, the staff finds that the DAS meets the quality requirements of Generic Letter 85-06 and GDC 1. The diverse ATWS equipment is designed to perform its function in a reliable manner.

7.8.4.7 DAS Testing and Surveillance

The guidance of SRP Section 7.8 states that the applicant/licensee should identify the test, maintenance, surveillance, and calibration procedures. These provisions should be consistent with the guidance of Generic Letter 85-06 and its enclosure. The ATWS mitigation system should be testable at power (up to, but not necessarily including, the final actuation device).

Generic Letter 85-06 states in part that measures are to be established to test, as appropriate, non-safety ATWS equipment prior to installation and operation and periodically. Results of the test should be evaluated to ensure that the test requirements have been satisfied.

<u>DPS System Testing</u>

The DPS testing covers the trip path from sensor input to the RTSS. The system test doesn't affect the functions of the DPS. The DPS has manual and manually initiated automatic test functions. These are done through the DPS MTP. The manually initiated automatic test is performed periodically during power operation. During this test, the DPS trip outputs are automatically bypassed and the fixed test signals are inserted to cause a channel trip for each process parameter in the DPS. The manual test is performed during shutdown. During this test, the DPS trip outputs are not automatically bypassed. The fixed test signals, which are inserted through manual test selection, cause a channel trip for each process parameter. The channel trip signals generated by the manual test initiate the final actuation devices. During the refueling period, response time verification tests are performed for the DPS. This confirms whether the DPS response times are maintained within the acceptable range.

The DCD Tier 2 Section 7.8.2.1, "Trip Bypass", states:

> A trip channel bypass of the DPS is provided in each channel through the DPS-operator module and MTP to allow for the maintenance, repair, test, and calibration during operation to avoid inadvertent actuation of the protective action. When a trip channel is bypassed for test or maintenance, the bypass status is indicated in the MCR. The logic converts to 2oo3 while a channel is bypassed.

The DCD Tier 2 Section 7.8.2.3, "Operating Bypass", states:

> The DPS provides the operating bypasses for the SIAS. The DPS-SIAS operating bypass can be manually enabled during the RCS heatup and cooldown. The DPS-SIAS operating bypass is provided in each channel by using the DPS-operator module in the MCR. The DPS-SIAS is also automatically defeated by the actuation of MCR to RSR control transfer, which enables the plant operation in the RSR. When the DPS-SIAS operating bypass is enabled, the bypass status is indicated in the MCR.

DMA System Testing

A channel functional test is performed for the DMA switches. This is done through manual actuation of each function. The testing is performed during plant outages to confirm that the actuation switch can actuate the components.

DIS System Testing

A functional test is performed for the DIS during plant outages to verify the DIS functionality.

Based on the above information, the staff finds that the applicant has identified the test, maintenance, surveillance, and calibration procedures for the DAS and they are consistent with the guidance of Generic Letter 85-06 and its enclosure. The ATWS mitigation system is testable at power.

7.8.4.8 Power supply availability

The guidance of SRP Section 7.8 states that the reviewer should confirm with the organization responsible for the review of power systems that power sources will be available during and following a LOOP.

The DPS consists of four channels; one cabinet per channel. Each DPS cabinet is located in a separate room. Each DPS channel is powered from two redundant non-Class 1E vital buses that are independent from Class 1E vital buses. The DMA switches are designed with Class 1E qualified hardware with augmented quality and energized using Class 1E power. The DIS HSI equipment on the MCR safety console is powered by non-class 1E vital bus. An explanation of the power sources available during normal operation and during and following a LOOP event is described in Section 7.8.4.5.1, “Diverse Power Supplies,” of this SER.

7.8.4.9 Environmental qualification

The guidance of SRP Section 7.8 states that the diverse I&C system equipment as installed should be qualified for the environment that could exist during the events for which the equipment is assumed to respond.

The DCD Tier 2 Section 7.8.2.1, “Environmental Qualification,” states, “The DPS equipment is qualified to perform its intended protective function to the required environments of DBEs (including the main steam line break and LOCA).” Similarly the section also states that during DBEs, the DMA switches and the DIS are qualified to execute their intended protective functions. The DAS is not required to operate during a safe shutdown earthquake. Nevertheless, the DMA switches are designed with Class 1E hardware and seismically qualified. The DPS is designed and qualified to withstand its physical integrity during five 1/2 safe shutdown earthquakes followed by one safe shutdown earthquake. The DIS is classified as non-seismic equipment except the DIS equipment mounted on the safety console, which is qualified to withstand its physical integrity during five ½ safe shutdown earthquakes followed by one safe shutdown earthquake.

The DAS is also qualified for EMC and this is necessary to perform its intended functions. The DAS is not susceptible to EMI/RFI / surge generated externally during normal operation. Also, it does not generate EMI/RFI/surge to the level that may affect the normal operation of other systems. Hence, the staff finds that the DAS is qualified for the environment that could exist during the events for which the DAS is assumed to respond.

7.8.4.10 System status

The guidance of SRP Section 7.8 states that information should be available in the control room to indicate the operation of the diverse I&C systems. This aspect of the review may involve considerations included in emergency operating procedures.

Point 4 of the SRM to SECY-93-087 states that a set of displays and controls located in the MCR shall be provided for manual, system-level actuation of critical safety functions and monitoring of parameters that support the safety functions. These credited displays and controls shall be independent and diverse from the safety-related computer system. The guidance of SRP BTP-7-19 states that displays and manual controls provided for D3 conformance with Item 18, II.Q, Point 4 of the SRM on SECY 93-087 should be sufficient both for monitoring the plant state and to enable control room operators to actuate the systems that will place the plant in a hot shutdown condition. DCD Tier 2 Section 7.8.1.3, "Diverse Indication System," states that, "The DIS provides functions to monitor critical variables following a postulated software CCF of safety-related I&C systems."

GDC 13, "Instrumentation and Control," as it relates to assuring Instrumentation is provided to monitor variables and systems over their anticipated ranges for normal operation, for AOOs, and for accident conditions as appropriate to assure adequate safety, including those variables and systems that can affect the fission process, the integrity of the reactor core, the reactor coolant pressure boundary, and the containment and its associated systems. The hardwired signals provided by the DIS FPD would not be affected by safety-related system CCFs.

However, the staff needed the applicant to clarify whether any indications are provided to know when there is a software CCF of the safety-related system. The applicant also needed to explain what information is available in the control room to indicate the operation of the DPS and DMA switches. Therefore, in RAI 342-8291, Question 07.08-7, the staff requested that the applicant clarify how they know when a software CCF has occurred within the safety-related system, including the PPS and ESF-CCS. In the March 10, 2016, response to RAI 342-8291, Question 07.08-7 (ML16070A141), the applicant stated that there are no software CCF-specific alarms or indications. If a postulated software CCF occurs concurrently with a DBE, the DPS is automatically actuated and the trip alarms and indications are displayed on the DPS operator module (DPS-operator module) mounted on the MCR safety console, enabling the operator to be aware of the safety-related system CCF. Operators in the MCR can acknowledge the occurrence of a postulated software CCF based on the occurrence of any combination of the following DPS reactor trip, AFAS, and SIAS trip alarm(s):

- DPS Pressurizer High Pressure Reactor Trip.
- DPS Containment High Pressure Reactor Trip.
- DPS Steam Generator No. 1 Low Level AFAS Trip.
- DPS Steam Generator No. 2 Low Level AFAS Trip.
- DPS Pressurizer Low Pressure SIAS Trip.

One of the DPS design purposes is to mitigate the consequences of a DBE concurrent with a postulated software CCF of the safety-related I&C systems. During a postulated software CCF event, the PPS does not provide any expected protective actuations (i.e., a trip initiation of RPS or ESFAS function). In this case, the DPS provides the protective actuation (i.e., diverse reactor

trip, AFAS or SIAS initiation) when required, because the DPS has system diversity compared with the safety-related I&C systems. The applicant also stated that Section 4.2.3 of the D3 TeR will be revised to include the following:

> *If a postulated software CCF occurs concurrently with a DBE, the DPS is automatically actuated and the trip alarms and indications are displayed on the DPS operator module (DPS operator module) mounted on the MCR safety console, enabling the operator to be aware of the safety-related system CCF.*

Therefore, since a postulated software CCF of the safety-related system activates trip alarms and indications displayed on the DPS-operator module and in turn enables the operator to be aware of the safety-related system CCF, the staff finds that the applicant's response to RAI 342-8291, Question 07.08-7, is satisfactory. The incorporation of the proposed markup into the next revision of D3 TeR was a confirmatory item. The staff verified that the proposed markups have been incorporated into Revision 1 of D3 TeR. Hence, the staff finds that sufficient information is available in the control room to indicate the operation of the diverse I&C systems and that Item 18, II.Q, Point 4 of the SRM on SECY-93-087 is also met.

7.8.4.11 Potential for inadvertent actuation

The guidance of SRP Section 7.8 states that the diverse I&C systems design should limit the potential for inadvertent actuation and challenges to safety-related systems.

The DPS consists of four channels with 2oo4 coincidence logic. In addition, the energized-to-actuation design feature is used for the DPS trip actuation logic. Therefore, the DPS has a fault-tolerant capability. This ensures that the spurious DPS trip actuation can be minimized. A spurious actuation of DPS reactor trip results in the rods being released to drop into the core. Plant post reactor trip procedures are then followed to achieve a plant safe shutdown condition. A spurious DPS turbine trip is bounded by the loss of load event which is analyzed in Chapter 15 of the FSAR. In case of a spurious DPS auxiliary feedwater system actuation, the main FWCS reduces the main feedwater flow into the steam generators. This compensates for the auxiliary feedwater flow. A spurious DPS safety injection actuation during the RCS normal operating condition cannot result in actual safety injection to the RCS. This is because the safety injection function uses a relatively low system pressure as compared to the normal RCS pressure. However, the spurious DPS safety injection actuation during RCS heatup and cooldown conditions can result in a safety injection to the RCS. The applicant states that such an injection does not cause any significant risks to plant safety.

The staff found that there was insufficient information in the application to demonstrate that safety injections in the heatup and cooldown conditions cannot cause any significant risks to plant safety. Therefore, in RAI 342-8291, Question 07.08-15, the staff requested that the applicant describe why a safety injection into the RCS due to a spurious DPS safety injection actuation during RCS heatup and cooldown conditions, does not cause any significant risk to plant safety. In the March 9, 2016, response to RAI 342-8291, Question 07.08-15 (ML16069A383), the applicant referenced Sections 15.5.1.2 and 15.5.1.3.3 of DCD Tier 2, which explains the operation of the SIS as follows:

> Inadvertent operation of the SIS is only of consequence when it occurs below the SI pump shutoff head pressure. Above that pressure, there will be no injection of fluid into the system. Below the SI pump shutoff head pressure when the shutdown cooling system is isolated, the SI flow will increase RCS inventory and

> pressure until the pressure reaches the pump shutoff head pressure. During shutdown cooling system operation, the increase in RCS inventory and pressure will be mitigated by the shutdown cooling system relief valves…Plant operation above the SI pump shutoff head pressure will not be impacted by the inadvertent operation of the SIS. Below the SI pump shutoff head pressure when the shutdown cooling system is isolated, there will be an RCS inventory and pressure increase. This increase will be terminated when the pressure rises above the shutoff head pressure. Due to the pressure increase caused by this transient at low RCS temperatures, there is an approach to the brittle fracture limits of the RCS. If the SIS inadvertently actuates during shutdown cooling operation, the shutdown cooling relief valves mitigate the pressure transient.

In order to clarify this in the application, the applicant will be revising Appendix A, Section 1.8 of the D3 TeR as follows:

> The spurious DPS safety injection actuation during the RCS heatup and cooldown conditions can result in actual safety injection to the RCS. The spurious initiation of the [SIAS] from the DPS can cause the operation of the [SIS]. Inadvertent operation of the SIS is only of consequence when it occurs below the SI pump shutoff head pressure. Above that pressure, there will be no injection of fluid into the system. Below the SI pump shutoff head pressure when the shutdown cooling system is isolated, the SI flow will increase RCS inventory and pressure until the pressure reaches the pump shutoff head pressure. During shutdown cooling system operation, the increase in RCS inventory and pressure will be mitigated by the shutdown cooling system relief valves. Therefore, the safety injections in this RCS heatup or cooldown conditions do not cause any significant risks to the plant safety.

Based on the above information, the staff finds that the applicant's response to RAI 342-8291, Question 07.08-15, is satisfactory because the diverse I&C systems design limits the potential for inadvertent actuation and challenges to safety-related systems and conforms to the guidance in SRP Section 7.8. The incorporation of the proposed markups into the next revision of the D3 TeR was a confirmatory item. The staff verified that the proposed markups have been incorporated into Revision 1 of the D3 TeR. As such, this confirmatory item has been satisfied.

7.8.4.12 Manual initiation capability

The guidance of SRP Section 7.8 states that the ATWS mitigation systems and DAS should include the capability for initiation from the control room.

The ATWS mitigation system for the APR1400 design is the DPS. The DPS-operator module in the MCR has a DPS manual reactor trip. This permits the operator to trip the reactor in case the automatic PPS reactor trip, manual PPS reactor trip or the automatic DPS reactor trip don't perform their intended functions. Similarly, there are DMA switches on the MCR safety console. This allows for manual actuation of the ESF components even if the ESF-CCS succumbs to a CCF. A DMA actuation enable switch is needed for the use of the diverse switches and this enable switch is under operator administrative control. It is only enabled once the operators conclude that the safety-related I&C systems have a CCF. The hardwired conventional switches are not affected by CCF.

The staff needed to understand whether the DMA actuation enable switch is credited to mitigate a DBE concurrent with a software CCF of the safety-related system. Therefore, in RAI 342-8291, Question 07.08-14, the staff requested that the applicant clarify whether the DMA enable switch is susceptible to a software CCF of the safety-related system (including the PPS and ESF-CCS) and consequently prevent the DMA switches from performing their diverse functions. In the March 9, 2016, response to RAI 342-8291, Question 07.08-14 (ML16069A383), the applicant stated that the DMA enable switches are essential pieces of equipment which are used to enable the function of the DMA switches for the mitigation of a design bases event which occurs concurrent with a software CCF of the common safety-related I&C platform. The DMA enable switch can block the hardwired signal from the DMA switch to the CIM by using an AND gate function, as shown in the D3 TeR, Figure 5-3.

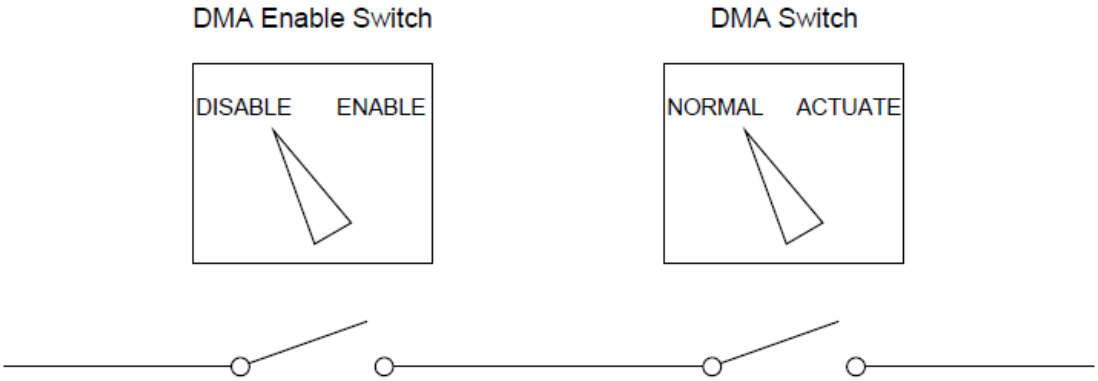

Figure 7.8-1 Configuration of DMA Switch and DMA Enable Switch

The AND gate function is implemented by a simple configuration using conventional hardwired switches, as shown in Figure 7.8-1 above. A DMA enable switch has contacts that are connected to each contact of the DMA switches in series, as shown in Figure 7.8-1. The DMA enable switch can switch these contacts at the same time to enable the function of DMA switches. The operator needs to turn the DMA enable switch to “Enable” and then turn the DMA switch to “Actuate” to send an actuation signal. These actuation signals of the DMA switches are input to the CIM in the ESF-CCS loop controller cabinets through an interposing relay for isolation. Therefore, the signals from the DMA enable switch and the DMA switch are isolated from the safety-related I&C systems. The DMA switches are normally disabled. The functions of the DMA switches can be enabled when the DMA enable switch is switched to enable mode by administratively controlled operator action. The function of the DMA switches is blocked unless operators conclude that safety-related I&C systems have a CCF. However, this block function is implemented by a simple configuration and the DMA enable switches and DMA switches do not use a software device in order to not be susceptible to a software CCF.

The applicant will also be revising the D3 TeR, Revision 0, Section 5.3, to clarify the information presented in their response. Based on the above information, the staff finds that the applicant’s response to RAI 342-8291, Question 07.08-14, is satisfactory because the staff finds that the ATWS mitigation systems and DAS include the capability for initiation from the control room. The incorporation of the proposed markups into the next revision of the D3 TeR was a confirmatory item. The staff verified that the proposed markups have been incorporated into Revision 1 of the D3 TeR. As such, this confirmatory item has been satisfied.

7.8.4.13 Completion of protective action

The guidance of SRP Section 7.8 states that the ATWS mitigation logic and DAS should be designed such that, once initiated, the mitigation function will go to completion.

The staff couldn't find any information pertaining to the completion of protective action in the FSAR. Therefore, in RAI 342-8291, Question 07.08-10, the staff requested that the applicant clarify that the ATWS mitigation logic and DAS is designed such that, once initiated, the mitigation function will go to completion. In the July March 9, 2016 response to RAI 342-8291, Question 07.08-10 (ML16069A380), the applicant stated that the DAS consists of the DPS, the DIS, and the DMA switches. The DPS provides the ATWS mitigation functions required by 10 CFR Part 50.62 for the reduction of risk from ATWS events. In addition, the DPS is designed to meet the requirements of Item 18, II.Q of the SRM on SECY-93-087 to assist in mitigation of the effects of a postulated software CCF of the digital computer logic within the PPS and ESF-CCS.

The applicant committed to revising Section 5.1 of the D3 TeR to include the following explanations:

> Once the diverse reactor trip signals are initiated automatically from the DPS cabinet, the diverse reactor trip function is completed by the actuation of shunt trip devices of reactor trip circuit breakers. The diverse reactor trip is completed when the reactor trip circuit breakers open. Deliberate operator action (i.e., reset of reactor trip circuit breakers) is required to clear the diverse reactor trip and close the reactor trip circuit breakers.

The applicant also clarified that the cycling AFAS refers to the repeated open/close actuations of the AFWS valves initiated by the DPS-AFAS. The setting and resetting of the DPS-AFAS repeats according to the changes of SG water level during plant transients. To clarify this term in Section 5.1 of the D3 TeR, the applicant proposes to include the following description:

> A DPS-AFAS occurs when the water level in a SG drops below the DPS-AFAS setpoint, and is reset when the SG water level is recovered to the reset setpoint. The setting and resetting of the DPS-AFAS repeats according to the changes of SG water level during plant transients. Once the DPS-SIAS is automatically initiated from the DPS, it is maintained until operator resets it. The DPS-SIAS can be reset when the pressurizer pressure is increased above its setpoint.

Further, the applicant clarified that the DMA switches are designed to permit the operator to actuate ESF systems in a timely manner from the MCR after a postulated CCF of the PPS and ESF-CCS. The DMA switches are normally disabled. The functions of the DMA switches could become enabled only by the actuation of the DMA enable switch. The DMA switches provide ESF actuation as required by Item 18, II.Q of the SRM on SECY-93-087, Point 4, and are listed in Appendix C of the D3 TeR.

The applicant also committed to revising Section 5.3 of the D3 TeR to include the following explanations:

> The DMA switches send latch signals to the CIM. Therefore, the ESF actuation initiated by the DMA switch continues until completion once initiated. These latch signals will be reset manually when the mitigation function is completed. Based on above descriptions, the DAS including the DPS and DMA switches is

designed such that, once initiated, the mitigation function continues until completion.

Based on the above information, the staff finds that the applicant's response to RAI 342-8291, Question 07.08-10, is satisfactory because the ATWS mitigation logic and DAS is designed such that, once initiated, the mitigation function will go to completion. The incorporation of the proposed markups into the next revision of the D3 TeR was a confirmatory item. The applicant submitted a supplemental response (ML16190A076) that changed the clarification to the cycling of the AFWS valves. The staff found that this response was not acceptable because it did not clearly describe how the AFWS valves are cycled by the DPS-AFAS and requested that the applicant revert back to the explanation provided in the previous response. Subsequently, the applicant provided another supplemental response (ML18120A302) to revert back to the explanation provided in the first response. The staff finds this response acceptable given that it is consistent with the original response that the staff found acceptable. The incorporation of the proposed markups into the next revision of the D3 TeR was a confirmatory item. The staff verified the the proposed markups have been incorporated into Sections 5.1 and 5.3 of the D3 TeR, Revision 3. As such, this confirmatory item has been satisfied.

7.8.5 Combined License Information Items

No applicable items were identified in the FSAR. No additional COL information items need to be included in DCD Tier 2 Table 1.8 2, "APR1400 Combined License Information Items," for DI&C system consideration.

7.8.6 Findings and Conclusions

The staff conducted a review of the DAS for conformance to the guidelines in the RGs and industry codes and standards applicable to these systems. Based on the review of the system design for conformance to the guidelines, the staff finds there is reasonable assurance the systems fully conform to the guidelines applicable to these systems.

Based on the applicant's commitment to the quality assurance guidance of Generic Letter 85-06 and review of the design of the diverse I&C systems, the staff finds that the quality assurance requirements of GDC 1 have been met as explained in Section 7.8.4.6 of this SER.

The diverse I&C systems are appropriately isolated from safety-related systems. Based on review of the interfaces of the ATWS mitigation system and equipment with the RTS, the staff concludes that the separation and independence design features of the RTS are not compromised by the ATWS mitigation system design. Where isolation devices are provided in the RTS to support ATWS mitigation interfaces, the isolation devices are applied and qualified to the guidelines of SRP BTP 7-11. Therefore, the staff concludes that the independence of these systems from safety-related systems satisfies the requirements of 10 CFR 50.55a(h)(3) and GDC 24 as explained in Section 7.8.4.5 of this SER.

Based on the review of diverse I&C system status information, manual initiation capabilities, and provisions to support safe shutdown, the staff concludes that information is provided to monitor the system over the anticipated ranges for normal operation, for AOOs, and for accident conditions as appropriate to assure adequate safety. Appropriate controls are provided for manual initiation of diverse I&C functions. These manual controls are to be independent of the digital systems that provide automatic initiation of the same functions. The diverse I&C systems appropriately support actions to operate the nuclear power unit safely under normal conditions

and to maintain it in a safe condition under accident conditions. Therefore, the staff finds that the design of the diverse I&C systems satisfies the requirements of GDC 13 and 19 as explained in Sections 7.8.4.4 and 7.8.4.10 of this SER.

The ATWS mitigation system instrumentation includes the DPS. Based on the review of these functions and the design bases submitted by the applicant, the staff concludes that the ATWS mitigation design includes an appropriate set of functions. Based on the above items, the staff concludes that the design of the ATWS mitigation system is acceptable and satisfies the specific design requirements identified in 10 CFR 50.62 for pressurized water reactor as explained in Section 7.8.4.13 of this SER.

Based on a review of diverse manual displays and controls, the staff concludes that these controls and displays are independent and diverse from the safety computer system, and sufficient for manual, system-level actuation of critical safety functions and monitoring of parameters that support the safety functions. Therefore, the staff concludes that the manual controls and displays meet the requirements of the SRM to SECY-93-087, Item 18, II.Q.

Based on review of DAS functions and design, the staff concludes that the DAS is acceptable. The functional requirements, independence requirements, and diversity requirements for this system are consistent with the applicant's D3 analysis, and fulfill the applicable guidance of the SRM to SECY-93-087, Item 18, II.Q, as explained in Section 7.8.4.13 of this SER.

The staff determined that the implementation of the identified acceptance criteria and guidelines in Section 7.8 of this SER satisfies the above stated applicable requirements with respect to the design, fabrication, erection, and testing commensurate with the importance of the safety functions to be performed.

7.9 Data Communication Systems

7.9.1 Introduction

The ARP1400 digital I&C systems utilize data communication systems as an integral part of its architecture. Data communication systems are described in DCD Tier 2, Sections 7.1 and 7.9, and the Safety I&C System TeR. The staff's review of the data communication systems against regulation and guidance are documented here.

7.9.2 Summary of Application

DCD Tier 1: The Tier 1 information associated with this section is found in DCD Tier 1, Section 2.5, "Instrumentation and Control."

DCD Tier 2: The applicant has provided a system description in DCD Tier 2, Sections 7.1 and 7.9, and the Safety I&C System TeR which is summarized as follows.

DCD Tier 2 Section 7.1, describes APR1400 data communication systems as providing data transfer within a safety division, between safety divisions, and between safety-related and non-safety-related systems.

Section 8 of the Safety I&C System TeR states the safety-related I&C system is implemented on a common PLC platform using Common Q. The staff reviewed and approved the Common Q Platform Topical Report (ML13112A110).

The DCD Tier 2 Section 7.9, describes the APR1400 data communication systems, which consist of safety-related and non-safety data networks. The safety-related SDN and SDL are implemented using the qualified Common Q PLC platform. The non-safety DCN-I is implemented using a non-safety DCS data communication network that has operating experience in the nuclear industry. The safety related data communication networks are designed to be independent and diverse from the non-safety network.

The DCD Tier 2 Section 7.9.1.1, states "SDN is used for communication between [safety-related] systems within one division…intra-division communications are separated and isolated from other divisions…the SDN is a broadcasting network with deterministic characteristics," and lists the safety-related systems that uses SDN.

The DCD Tier 2 Section 7.9.1.2, states "SDL is used for predefined data transmissions between each processor within a division, and to send broadcast data to other safety divisions and non-[safety-related] systems…SDLs use fiber-optic modems and cables to provide electrical isolation," and lists systems that uses SDL.

The DCD Tier 2 Section 7.9.1.3, states "DCN-I network provides non-safety data communication network to integrate the data from [safety-related] and non-safety systems," and lists the non-safety systems that connects to the DCN-I network.

The DCD Tier 2 Section 7.9.1.4, discusses data communication from safety-related system to non-safety system, from non-safety system to safety-related system, and between QIAS-N and other systems, and communications between the IPS and QIAS-N.

The APR1400 data communication systems, their qualifications, software classification, and interfaces are evaluated in Section 7.9.4 of this SER.

ITAAC: The ITAAC associated with data communication systems are given in DCD Tier 1, Section 2.5

Technical Specifications: There are no Technical Specifications associated with data communications systems.

7.9.3 Regulatory Basis

The relevant requirements of the Commission regulations for this area of review, and the associated acceptance criteria, are given in Section 7.1, Section 7.9, and Appendix 7.1-A, of SRP and are summarized below. Review interfaces with other SRP sections also can be found in Section 7.1 of SRP.

Requirements applicable to data communication systems are as follows:

1. 10 CFR 50.55a(h)(3), "Safety Systems," requires compliance with IEEE Std 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," and the correction sheet dated January 30, 1995. The minimum requirements that are applicable to all data communication systems are IEEE Std 603-1991, Clause 5.6.3, "Independence between Safety Systems and Other Systems."

2. GDC 1, 13, 19, 21, 22, 23, and 24.

To meet the above requirements, the SRP acceptance criteria applicable to data communication systems important to safety are listed in SRP Table 7-1, Section 3 (SRMs), Section 4 (RGs), and Section 5 (BTPs).

7.9.4 Technical Evaluation

The objectives of the review are to confirm that data communication systems (1) conform to applicable acceptance criteria and guidelines, (2) will perform the safety functions assigned to them, (3) will meet the reliability and availability goals assumed for the system, and (4) will tolerate the effects of random transmission failures.

The staff reviewed DCD Tier 2, Sections 7.1 and 7.9, and the Safety I&C System TeR to confirm that the data communications systems design satisfies applicable NRC regulations through a set of acceptance criteria – and that it can perform its safety functions for all plant conditions. SRP Section 7.9, "Data Communications Systems," lists the following major design considerations that should be emphasized for the review of data communications systems:

- Quality of Components and Modules.
- Data Communications Systems Software Quality.
- Reliability, Time Coherency of Data, Protocols.
- Performance.
- Control of Access.
- Single-Failure Criterion.
- Independence.
- System Testing and Inoperable Surveillance.
- EMI/RFI Susceptibility.
- D3.
- Data Communications Systems Exposed to Seismic Hazard.

The staff also identified "Control System Data Communication Functions" as another area of review for data communications systems. Several of these design considerations are fully or partially addressed in other sections of this SER, as indicated in Table 7.9-1.

Table 7.9-1. Section 7.9 References to Other Report Sections.

Design Considerations	SER Section(s)
Quality of Components and Modules	7.1.4.7
Data Communications Systems Software Quality	7.1.4.7
Single Failure Criterion	7.1.4.5
System Testing and Inoperable Surveillance	7.1.4.11
EMI/RFI Susceptibility	7.1.4.8
D3	7.8
Data Communications Systems Exposed to Seismic Hazard	7.1.4.8
Physical Separation and Electrical Isolation	7.1.4.10

7.9.4.1 Quality of Components and Modules

The applicant should confirm that quality assurance provisions of Appendix B to 10 CFR Part 50 and GDC 1 are applicable to the safety-related system, which includes data communication systems important to safety.

DCD Tier 2 Section 7.9.2.1, "Quality of Components and Modules," lists safety related components and modules that perform the protection functions: PPS, CPCS, ESF-CCS, and QIAS-P; non-safety components and modules include P-CCS, PCS, IPS, and QIAS-N data communication systems. The staff's evaluation of quality assurance is discussed in Section 7.1.4.7 of this SER. The evaluation of the overall quality assurance program is addressed in Chapter 17 of this SER.

7.9.4.2 Data Communications Systems Software Quality

The applicant should address the software quality requirements described in SRP Appendix 7.1-D, Section 5.3, for digital computer-based systems, which includes data communication systems important to safety.

The DCD Tier 2 Section 7.9.2.2, "Data Communication Systems Software Quality," lists data communication systems, and their designated software categories as discussed in the SPM TeR: safety critical, ITS, and ITA. The following table, Table 7.9-1, lists the types of data communication network, and their qualification and software classification, which is based on the description in DCD Tier 2 Section 7.9.1.

Table 7.9-2. APR1400 Data Communication Network, Qualification, and Software Classification

Source: DCD Tier 2 Section 7.9.1					
Data Communication Network Type	**Qualification**		**Software Classification**		
	Seismic	**Environmental**	**Safety-critical**	**ITS**	**ITA**
SDL	Yes	Yes	Yes	Yes	No
SDN	Yes	Yes	No	Yes	No
DCN-I	No	No	No	No	Yes

The staff's evaluation of the software quality is discussed in Section 7.1.4.7 of this SER.

7.9.4.3 Reliability, Time Coherency of Data, Protocols, Effects of Data Storm, Performance, and Control of Access

7.9.4.3.1 Reliability

Clause 5.15 of IEEE Std 603-1991 requires appropriate analysis be performed on the system design for which either quantitative or qualitative reliability goals have been established to determine that such goals have been achieved. To meet the requirements of IEEE Std 603-1991, Clause 5.15, data communications systems in support of safety functions should demonstrate sufficient reliability in accordance with the acceptance criteria described in SRP Section 7.9. SRP Section 7.9 states that the data communications system design should identify and address potential hazards. The design should preclude the inadvertent activation of unneeded data communications functions that is included in the data communications system design. Error detection should be at least as good as a four-byte cyclic CRC. Corrupted messages (missing or corrupted packets), missing messages, and duplicate messages should be detected and repaired.

The Safety I&C System TeR, Section 4.6.1.4, states, "Error checking techniques for data integrity such as CRC are incorporated into the communication protocol to assure the integrity of the transmitted data…the system is designed such that communication failures shall not prevent [safety-related] systems from performing their intended safety functions as analyzed in Appendix C."

The Safety I&C System TeR, Appendix C, Section C.3.1, states, "the serial data link is a point-to-point serial RS-422 link…a 32 bit CRC assures the integrity of the received data…the processor module has independent transmit links and receive links…the communication data is optically isolated and transmitted to the other divisions."

The staff finds the use of the 32-bit CRC for error detection conforms to guidance, and hence demonstrates that the safety-related system data communications system adequately meets the reliability requirements of IEEE Std 603-1991, Clause 5.15.

The Safety I&C System TeR, Section 4.3.2.4, states:

> The SDL is deterministic. Communication between two processors is via SDL for the exchange of predefined data packets. Processors on each end of the SDL are configured to send/receive a predefined set of data. The send and receive ports of the SDL are independent. More detailed design information on the SDL communications is described in Reference 12… The data is received and transmitted in a deterministic manner. Each processor module has four SDL ports (two transmit and two receive). Each direction works independently. The transmission is purely unidirectional without acknowledgment from the other side.

Reference 12 is the Westinghouse Common Q Topical Report, which the staff has approved with limitation and conditions.

The DI&C-ISG-04, Section 1, "Interdivisional Communications," Staff Position 5 states, "The cycle time for the safety function processor should be determined in consideration of the longest possible completion time for each access to the shared memory… Failure of the system to meet the limiting cycle time should be detected and alarmed." To comply with DI&C-ISG-04, Section 1, Staff Position 5, the applicant states "The [processor module] transmits signals to SDL in a deterministic transmit cycle, and the controller receives only defined messages and stores in a predefined shared-memory…The [function processor] detects failure of the limiting cyclic time through self-diagnostic function, and generates alarm." The Safety I&C System TeR, Appendix C, Section C3.1, states "[t]he [function processor] operates asynchronously to the CP and the operation does not perform any communication handshaking or accept interrupts from the other divisions."

The Safety I&C System TeR, Section 4.6.2.6, "Communication of ESCM," states "Ethernet is used for communication from IFPD to ESCM to send identification data of a component." Ethernet is generally does not have deterministic behavior however since a failure of this connection does not prevent the ESCM from performing its intended safety function.

Based on the information provided, the staff finds that the safety-related I&C systems design is adequate to provide for data communications reliability to meet Clause 5.15 of IEEE Std 603-1991. Specifically, the staff finds the use of deterministic cyclic processing without the use of process driven interrupts for all safety applications enable deterministic data communications for APR1400 safety-related I&C systems. The staff's evaluation of the Safety I&C System TeR, Appendix C, "Conformance to DI&C-ISG-04," is detailed in Section 7.9.4.6 of this SER. The evaluation of the isolation is documented in Section 7.9.4.6 of this SER.

7.9.4.3.2 Time Coherency of Data

The SRP Section 7.9 states that methods should be employed to ensure the correct sequence of data packets at receiving data communications systems nodes. Similarly, DI&C-ISG-04, Section 1, Staff Position 12, states in part, "that communication faults should not adversely affect the performance of required safety functions in any way. Faults, including communication faults, originating in non-safety equipment, do not constitute "single failures" as described in the single failure criterion of 10 CFR Part 50, Appendix A." Credible communication faults include,

but not limited to, “Messages may be repeated at an incorrect point in time,” and “Messages may be sent in the incorrect sequence.”

In Section 4.1.3.4 of the safety evaluation for the Common Q Platform Topical Report, Revision 3, the staff found the applicant has satisfied DI&C-ISG-04, Section 1, Staff Position 12, due to a sequence counter value that is generated by the processor module’s processing section for each set of data that is transmitted. The receiving processor module’s communication section monitors this sequence counter to ensure that the next set of data is received at the correct point in time. For more details, see the staff’s evaluation of the Common Q Platform Topical Report. Based on the information presented in topical report, the staff finds the system adequately ensures that out of sequence messages are flagged during every processing cycle to meet the requirements of IEEE Std 603-1991, Clause 5.15.

7.9.4.3.3 Protocols

The SRP Section 7.9 states protocols proposed for use, whether standard or proprietary, should be analyzed for hazards and performance deficits posed by unneeded functionality and complication.

The safety critical and ITS software used for data communications systems in support of safety functions within the digital safety-related I&C system follows the software development process detailed in the SPM TeR. The review of unneeded data communications functions and its impact on the supported safety function, as well as the software hazards analysis on the data communications software, are completed as part of RG 1.152, Revision 3, SDOE review. The staff’s evaluation of this technical report is documented in Section 7.1.4.7 of this SER.

7.9.4.3.4 Effects of Data Storms

GDC 13 requires instrumentation to be provided to monitor variables and systems over their anticipated ranges for normal operation, for AOOs, and for accident conditions as appropriate to assure adequate safety, including those variables and systems that can affect the fission process, the integrity of the reactor core, the reactor coolant pressure boundary, and the containment and its associated systems. Appropriate controls shall be provided to maintain these variables and systems within prescribed operating ranges.

DI&C-ISG-04, Section 1, Staff Position 19, states, in part, that “If data rates exceed the capacity of a communications link or the ability of nodes to handle traffic, the system will suffer congestion. All links and nodes should have sufficient capacity to support all functions.” To conform with DI&C-ISG-04, Section 1, Staff Position 19, the applicant stated “…even if incorrect data are broadcasted or a broadcast data storm occurs on a network causing an excess of data traffic, this failure does not adversely affect the performance of the [function processor] because communication bandwidth is sufficient for the true data rate including overhead.” The staff requested the applicant to demonstrate how the effects of data storms are addressed for this connectivity in order to provide reliable data transmissions to support safety-related system functions as required by GDC 13, as summarized in RAI 348-8279, Question 07.09-12.

RAI 348-8279, Question 07.09-12, had two parts, one asking about handling of erroneous data per DI&C-ISG-04, Section 1, Staff Position 4, and one about effects of data storms per DI&C-ISG-04, Section 1, Staff Position 19. In the August 30, 2016, supplemental response to RAI 348-8279, Question 07.09-12, the applicant provided additional markups to address staff’s concerns and also committed to incorporating the response into the Safety I&C System TeR.

The supplemental response regarding DI&C-ISG-04, Section 1, Staff Position 4, is acceptable since the applicant has design measures to handle erroneous data such that communication errors and malfunctions will not interfere with the execution of the safety functions. The staff also finds the design features for ESCM such as deterministic cycles and separate communication and safety function processor help prevent data storms from affecting safety functions. Section 7.9.4.6.3 of this SER evaluated conformance to DI&C-ISG-04, Section 1, Staff Position 4.

The supplement response regarding DI&C-ISG-04, Section 1, Staff Position 19, is acceptable since the applicant has design measures to ensure proper performance of all safety function since the function processor is independent of the Ethernet processor, and due to the fact that there are other ESCM consoles available. Should an ESCM console become unusable due to a broadcast data storm, operators can use another ESCM console that is not affected by the failed Ethernet interface, or operators can always use the ESCM located at the safety console that have no Ethernet interface. The verification that the proposed markups are incorporated into the next revision of the FSAR was a confirmatory item. The staff verified that the proposed markups have been incorporated into the Safety I&C System TeR, Revision 1. As such, this confirmatory item has been satisfied.

Based on the commitment to include the design criteria in the FSAR and the Safety I&C System TeR, to withstand data traffic and the interfacing IFPD and ESCM systems will be designed with thresholds for network traffic that are consistent with maximum data rates of the network devices, the staff finds that the applicant has addressed the effects of data storms to demonstrate that the IFPD to ESCM connectivity will be sufficiently reliable to support the functions required by GDC 13.

7.9.4.3.5 Performance

Clause 5.5 of IEEE Std 603-1991 requires safety-related 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 603-1991 requires, as a part of the design basis, identification of the critical points in time or the plant conditions, after the onset of a DBE.

To meet IEEE Std 603-1991, Clauses 5.5 and 4.10, data communications systems in support of the protection system should demonstrate real-time performance in accordance with SRP BTP 7-21. SRP BTP 7-21 stipulates that:

1. The level of detail in the architectural description should be sufficient that the staff can determine the number of message delays and computational delays interposed between the sensor and the actuator,

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.

The DCD Tier 2 Section 7.1.2.74 states:

> Applicable I&C systems listed in Table 7.1-1 are designed in accordance with SRP BTP 7-21. Real-time performance is determined by performing response time analysis for all safety functions. An analysis for each function is performed to demonstrate that the actual system response time is less than the response time requirements.

The design features that provide for real-time, deterministic behavior of the SDL and SDN data communication networks are described in Section 4.6.1.3 of the Safety I&C System TeR and Section 5.3 of the Common Q Platform Topical Report, Revision 3. Section 4.6.1.3 states:

> data communication system is deterministic…SDL communication is dependent on the repeatable and predictable execution of an application…the execution of an application program is repeated at predetermined intervals…there is no difference in data transfer rate, data bandwidth, data accuracy, and error performance during normal and abnormal operations. The SDN has a deterministic network protocol that is used for non-nodes communication within a division.

The SDN have a deterministic Process data transfer mode (for communication between nodes within a division) and a non-deterministic Message data transfer mode (for on-demand data communication from FPDs). Section 4.6.1.3 of the Safety I&C System TeR states that message transfer is non-deterministic. Since message transfer is not performed cyclically, but only when one or more of the attached communication interfaces have data to send, the staff requested the applicant to discuss if there are operational limits for message transfer in RAI 348-8279, Question 07.09-17. In the March 4, 2016, response to RAI 348-8279, Question 07.09-17, the applicant provided additional markups to address staff's concerns and also committed to incorporating the response into the Safety I&C System TeR. The staff finds the response acceptable since the applicant stated that the message transfer mode of the SDN will not be used in the APR1400 safety-related systems. The verification that the proposed markups are incorporated into the next revision of the FSAR was a confirmatory item. The staff verified that the proposed markups have been incorporated into the Safety I&C System TeR, Revision 1. As such, this confirmatory item has been satisfied.

Section 5.3 of Common Q Platform Topical Report, Revision 3 describes the design requirements for deterministic system behavior with guaranteed maximum computing and reaction times and constant communication loads. This section states that the design requires each process unit to process its assigned function in a strictly cyclical manner with a predefined cycle time. During each operating cycle, the sequence of processing steps is always the same. The control flow is independent from the process data. The message sizes and communications rates are constant, resulting in constant communication loads under all circumstances. In addition, the communication protocols used in the system do not require acknowledgement of the transmitted message by the receiver. Thus, the processor receiving the message cannot influence the operation of the sending processor. As discussed in the safety evaluation for the Common Q Platform Topical Report, Revision 3, the staff found the deterministic behavior of the system, as described in Section 5.3 of the topical report, ensures adequate performance of the data communications system to accomplish its safety function to meet Clause 5.5 of IEEE Std 603-1991.

7.9.4.3.6 Control of Access

IEEE Std 603-1991, Clause 5.9, requires the safety-related system design to permit the administrative control of access to safety-related system equipment. To meet the requirements of IEEE Std 603-1991, Clause 5.9, data communications systems in support of safety functions should demonstrate that adequate access controls are incorporated into the design of the data communications system in accordance with the acceptance criteria described in SRP Section 7.9. SRP Section 7.9 states that data communications should not present an electronic path by which unauthorized personnel can change plant software or display erroneous plant status information to the operators. Remote access to safety-related systems should not be implemented. In addition, RG 1.152, Revision 3, Regulatory Positions C.2.1-2.5 provides additional criteria for access control.

The DCD Tier 2 Section 7.9.2.5 discusses how APR1400 safety-related systems meets requirements of Clause 5.9 of IEEE Std 603-1991. The applicant states:

> Equipment related to the data communication systems is administratively controlled by key-locked doors on equipment cabinets to protect against unauthorized access. The indication of access to the cabinets by door switches is provided in the MCR. Access to the cabinets is normally required only during system testing, calibration, and maintenance. In addition to the security provisions provided by the above, system software is protected against unauthorized alterations. The protection includes setpoints and software coding by an administrative control of access to software media by the plant owner. Access to the data communication systems is administratively or password controlled.

Appendix A.5.9 of [the Safety I&C System TeR] supplements the control of access security design features by stating “access to equipment rooms and cabinets are controlled by the utility to only personnel who are intended to have access.”

The Safety I&C System TeR provides additional information on the security controls during the development of the platform, as well as a description of the controls for the development environment of the APR1400 application software to prevent unauthorized modification to the platform and application. This technical report provides a description of the security features in the system that can be used to prevent unauthorized or inadvertent access to the system during operations to address the criteria of RG 1.152, Revision 3, Regulatory Positions C.2.1-C.2.5. RG 1.152, Regulatory Positions C.2.1-C.2.5, provide criteria for the protection of digital safety-related systems and establishment of an SDOE for those systems. The evaluation of the access controls provided for the SDOE of the system to address RG 1.152, Revision 3, Regulatory Positions C.2.1-C.2.5, are discussed in Section 7.1.4.7.1.11 of this SER.

7.9.4.4 Single Failure Criterion and Data Communications System Failure Modes

GDC 21 requires, in part, the protection system to be designed for high functional reliability and in-service testability commensurate with the safety functions to be performed. IEEE Std 603-1991, Clause 5.1 requires, in part, safety-related systems to perform all safety functions required for a DBE in the presence of any single detectable failure within the safety-related systems concurrent with all identifiable but non-detectable failures.

To meet the requirements of GDC 21, and IEEE Std 603-1991, Clause 5.1, data communications systems in support of safety functions should address the single failure criterion guidance described in SRP Section 7.9. SRP Section 7.9 states that data communications systems design should ensure that channel assignments to individual communication subsystems are appropriate to assure that both redundancy and diversity requirements within the supported systems are met. In addition, the redundant divisions that communicate with each other should be independent from one another such that a single failure will not propagate to other redundant divisions.

The DCD Tier 2 Section 7.9.2.6 states:

> the SDN and SDL in each division are physically separated and functionally isolated from other divisions…a single failure within the SDN and SDL does not affect a required safety function…the FMEA for the PPS and the ESF-CCS provides the failure effects and analysis for the failure of communication modules, as shown in [FSAR] Tables 7.2-7 and 7.3-8.

7.9.4.4.1 Evaluation of Data Communications Single Failure Protection

Based on the staff's evaluation of the information presented in DCD Tier 2 Chapter 7, as supplemented by the Safety I&C System TeR, the staff finds the applicant has adequately demonstrated that the data communications systems in support of safety-related I&C systems meet IEEE Std 603-1991, Clause 5.1, and GDC 21, by providing sufficient redundancy or alternative means to prevent loss of safety functions due to a single failure. The specific details of the staff's review regarding the safety-related I&C system data communications to meet the requirements of IEEE Std 603-1991, Clause 5.1 and GDC 21 is summarized below. Safety systems that do not use data communications between redundant safety divisions were not included in this evaluation.

<u>PPS the following.</u>

Section 4.1.1.1 of the Safety I&C System TeR states the following.

> PPS consists of four redundant divisions that perform the necessary bistable, coincidence, initiation logic, and maintenance and test function…the PPS provides the reactor trip signals to the RTSS using hardwired cables and ESFAS initiation signals to the ESF-CCS via fiber optic SDLs.

As discussed in the safety evaluation for Common Q Platform Topical Report, the staff noted that…

> …no single failure will defeat more than one of the four redundant PPS divisions. These redundant divisions are electrically isolated and physically separated. Qualified isolation devices have been tested to ensure functional operability when subject to physical damage, short circuits, open circuits, or the application of credible fault voltages on the device output terminals.

As such, the staff finds the data communications system that supports the PPS functions is adequate to satisfy the requirements of IEEE Std 603-1991, Clause 5.1 and GDC 21.

<u>ESF-CCS</u>

Section 4.1.1.2 of the Safety I&C System TeR states:

> the ESF-CCS consists of four independent divisions that perform additional [2oo4] voting logic, component control logic, and priority logic function. The [group controller] of each ESF-CCS division receives four division ESFAS initiation signals derived from the ESFAS portion of the PPS and performs additional selective [2oo4] coincidence logic to generate the ESF actuation signal. The [group controller] also receives two division ESFAS initiation signals derived from the [RMS] and performs [1oo2] logic to generate the ESF actuation signal. The ESF actuation signals are transmitted to the [loop controller] of the ESF-CCS. The [loop controller] executes the component control logic and outputs the component control signal to the CIM.

As discussed in Section 7.3.4.2 of this safety evaluation, the safety-related ESF I&C system consists of four channels of sensors, APC-S, and four divisions of the ESFAS portion of the PPS, the ESF-CCS, and CIM; the ESF-CCS design consists of processors arranged in primary and standby processor configurations within each ESF-CCS division; ESFAS functions are divided into the ESF-CCS distributed segments which receive the ESF initiation signals from the PPS through the fiber optic cable; separation is provided between protective ESFAS processing function and auxiliary functions of human-system interfaces, data communication and automatic testing; the SDL supports the transmission of protection data on a continuous cyclical basis independent of plant transients. The staff finds that the ESF-CCS data communications functions meet the requirements of IEEE Std 603-1991, Clause 5.1, and 10 CFR Part 50, Appendix A, GDC 21. Section 7.3.4.3.2 of this safety evaluation discussed the single failure criterion evaluation of the APR1400 ESFAS and ESF design.

<u>CPCS</u>

Section 4.1.1.3 of the Safety I&C System TeR states the following.

> …the CPCS has four redundant channels that compute the DNBR and LPD values using process values, [RCP] speed, CEA position and ex-core neutron flux. The CPCS compares the DNBR and LPD values against setpoints to determine if fuel design limits are exceeded. When these values exceed a safety limit, a trip signal is transmitted to the PPS using hardwired cables.

As discussed in the safety evaluation for Common Q Platform Topical Report, staff noted the following.

> …no single failure will defeat more than one of the four redundant CPCS divisions. Qualified isolation devices have been tested to ensure functional operability when subject to physical damage, short circuits, open circuits, or the application of credible fault voltages on the device output terminals.

Therefore, the staff finds that the CPCS data communications functions meet the requirements of IEEE Std 603-1991, Clause 5.1 and GDC 21.

QIAS-P

Section 4.1.1.4 of the Safety I&C System TeR states the following.

> …the QIAS-P, which has two independent divisions A and B, is implemented on the common PLC platform for the [safety-related] system. The QIAS-P processes the plant parameters that are input from the [safety-related] I&C system via SDN, APC-S via hardwired interface, and process instrumentation directly. The safety FPDs for the QIAS-P are installed on the MCR [safety console]. The QIAS-P transmits data to the QIAS-P safety FPD via the SDN for RG 1.97, [Revision] 4, Types B and C variables. The QIAS-P also transmits the sensor signals and their calculated variables to the IPS and QIAS-N through the MTP and ITP, respectively. In the case of the IPS, this data communication is a unidirectional protocol from the MTP. In the case of the ITP, the SDL data communication is used to transmit data to the QIAS-N.

Based on the provision of two independent divisions of QIAS-P, the staff finds the QIAS-P meets the single failure requirements of IEEE Std 603-1991, Clause 5.1 and GDC 21.

7.9.4.5 Data Communications System Failure Modes

10 CFR Part 50, Appendix A, GDC 23, requires the protection system to be designed to fail into a safe state or into a state demonstrated to be acceptable on some other defined basis if conditions such as disconnection of the system, loss of energy (e.g., electric power, instrument air), or postulated adverse environments (e.g., extreme heat or cold, fire, pressure, steam, water, and radiation) are experienced. NUREG/CR-6082, “Data Communications,” provides additional discussion of independence and failure modes.

The postulated communication failures are based on the failures described in DI&C-ISG-04, Section 1, Staff Position 12. DI&C-ISG-04 states that these credible communications may include, but are not limited to the following.

- Messages may be corrupted due to errors in communications processors, errors introduced in buffer interfaces, errors introduced in the transmission media, or from interference or electrical noise.
- Messages may be repeated at an incorrect point in time.
- Messages may be sent in the incorrect sequence.
- Messages may be lost, which includes both failures to receive an uncorrupted message or to acknowledge receipt of a message.
- Messages may be delayed beyond their permitted arrival time window for several reasons, including errors in the transmission medium, congested transmission lines, interference, or by delay in sending buffered messages.
- Messages may be inserted into the communication medium from unexpected or unknown sources.
- Messages may be sent to the wrong destination, which could treat the message as a valid message.

- Messages may be longer than the receiving buffer, resulting in buffer overflow and memory corruption.

- Messages may contain data that is outside the expected range.

As discussed in the safety evaluation for the Common Q Platform Topical Report, the staff noted the following.

> For interdivisional communications through the high speed data links, there are design features including the mirror RAM check (described in Section 4.1.1.5 of the [Common Q Platform Topical Report safety evaluation]) and the use of CRC's (described in Section 4.1.3.2 of the [Common Q Platform Topical Report safety evaluation]) that provide added assurance that data corruption during transmission from the data source (another safety division) and the receiving safety processor will be identified and handled by the safety processor and will not adversely affect the safety function. Westinghouse provided explanations for how the Common Q system would respond to each of the 12 faults listed in DI&C-ISG-04, Section 1, Staff Position 12, within the Common Q [Platform Topical Report], Section 5.6.12. For each of these cases, specific design features of the Common Q system that have been evaluated by the staff in the Common Q [Platform Topical Report safety evaluation] were credited for ensuring that the integrity of the safety functions would be maintained. The staff determined that communications faults, including the 12 examples contained in [DI&C-ISG-04, Section 1, Staff Position 12], will not adversely affect the performance of the required safety functions, and that the Common Q platform complies with [Staff Position 12].

Sections C.5.1.1, C.5.1.2, C.5.1.3, and C.5.1.4 of the Safety I&C System TeR stated "The compliance of the platform is provided in Reference 12 [Common Q Platform Topical Report]." for DI&C-ISG-04, Section 1, Staff Position 12. The staff issued RAI 348-8279, Question 07.09-16, to request the applicant to discuss if there are any data communication failures that are APR1400 I&C architecture specific. In the March 10, 2016, response to RAI 348-8279, Question 07.09-16 (ML16070A142), the applicant stated, in part, "In the design of the [SDL] between the bistable and the [LCL], the LCL and [group controller], the CPP and the CEAC/CPP, and the ITPs, as stated in Section C.5.1.1, C.5.1.2, C.5.1.3, and C.5.1.4 of the Safety I&C System TeR, there are no data communication failures, except those platform specific failures discussed in the Common Q Platform Topical Report, Revision 3. The staff requested the applicant to supplement this response with analysis regarding potential communication failures of the APR1400 design related to the changes to the approved Common Q, such as a different CPU version, the redundant CPU processor configuration, input/output extension, and increase of the maximum CPU load. The analysis in the Common Q platform topical report did not cover these differences or new features. As a result, additional analysis is needed. The applicant should provide communication failure analysis based on the differences between what was approved in the Common Q Platform Topical Report and the APR1400 design. In the August 18, 2016, supplemental response to RAI 348-8279, Question 07.09-16 (ML16231A496), the applicant stated the following, in part.

> …this supplemental response is to provide design information relating to the hot standby configuration of the ESF-CCS configuration; specifically, the design documents that describe how the hot-standby configuration will work and the

self-diagnostics design information to support the hot-standby configuration. In addition, this response also provides additional analysis for the PM646B.

However, the staff reviewed the revised response and determined that it did not provide analysis regarding potential communication failures of the APR1400 design related to the changes to the approved Common Q Platform Topical Report such as a different CPU version, the redundant CPU processor configuration, input/output extension, and increase of the maximum CPU load. As such, RAI 348-8279, Question 07.09-16, was tracked as an open item.

In the July 27, 2017, supplemental response to RAI 348-8279, Question 07.09-16 (ML17208B030), the applicant provided additional communication failure analysis specific to those failures for components that were not included in the Common Q Platform Topical Report, the CPU load limits for the Master/Slave configuration (for hot-standby configuration), and the switch over process between the Master and Slave within the ESF-CCS. The analysis demonstrated how the effects from communication failures were limited to within one safety division or that the failures are bounded by what is analyzed for components within the scope of the Common Q Platform Topical Report. The applicant also provided proposed markups for the Safety I&C System TeR that describe the hot-standby configuration used for BOP-ESFAS within the ESF-CCS and the communication failure analysis discussed in the response. Because the applicant provided an analysis of communication failures for components and configuration not addressed by the Common Q Platform Topical Report and demonstrated how these failures do not impact the safety function, the staff finds the response is acceptable. The verification that the proposed markups are incorporated into the next revision of the Safety I&C System TeR was a confirmatory item. The staff verified the proposed markups have been incorporated into Revision 2 of the Safety I&C System TeR. As such, this confirmatory item has been satisfied.

Based on the resolution of the open item associated with RAI 348-8279, Question 07.09-16, and the provision of information that demonstrate how communication failures are addressed by the design in accordance with DI&C-ISG-04, the staff determined that the data communications error handling methods employed ensure that the data communication systems meet the requirements of GDC 23.

7.9.4.6 Independence

7.9.4.6.1 Independence between Redundant Portions of the Safety System

The IEEE Std 603-1991, Clause 5.6.1, requires redundant portions of the safety-related system to be independent and physically separated from each other to the degree necessary to retain the capability to accomplish the safety function. SRP Appendix 7.1-C, provides acceptance criteria for the requirements of IEEE Std 603-1991. Section 5.6 of SRP Appendix 7.1-C states that three aspects of independence should be addressed, including physical independence, electrical independence, and communications independence. RG 1.75, Revision 3, describes a method acceptable to the staff for complying with the NRC's regulations with respect to the physical independence requirements of the circuits and electrical equipment that comprise or are associated with safety-related systems. RG 1.75, Revision 3, endorses IEEE Std 384-1992 as an acceptable method for satisfying the regulatory requirement concerning physical independence of circuits and electrical equipment that comprise safety-related systems. SRP BTP 7-11 provides guidance on application and qualification of isolation devices used to ensure electrical independence for safety-related systems. In addition, DI&C-ISG-04 provides acceptance criteria for communications and functional independence between redundant divisions of safety-related systems.

Physical Separation and Electrical Isolation

The evaluation of physical separation and electrical isolation requirements to meet the requirements of IEEE Std 603-1991, Clause 5.6.1 is provided in Section 7.1.4.10 of this SER.

Communications Independence

The DCD Tier 2 Section 7.2.2.3, "Independence," states:

> Independence between redundant portions of the safety system. The routing of Class 1E and associated cabling and sensing lines from sensors meets the guidance of [RG 1.75, Revision 3] and [RG 1.151, Revision 1]. The cablings for the four safety divisions are routed separately. The PPS divisions receive ac power from the vital bus power supply system. The PPS does not share the power between divisions.

This section of the FSAR does not discuss how data communication independence between redundant portions of the PPS is achieved to meet the requirements of IEEE Std 603-1991, Clause 5.6.1. The staff issued RAI 45-7883, Question 07.09-6 to request the applicant to provide either a summary of how communications independence requirements are met or reference the particular section of the Safety I&C System TeR where data communication independence between redundant portions of the safety system is being analyzed. In the November 3, 2015, response to RAI 45-7883, Question 07.09-6 (ML15307A679), the applicant referenced Section 4.6.2.1 of the Safety I&C System TeR, which describes the interdivisional serial data links used for data communication between safety portions of the PPS). The staff finds this response satisfactory because the applicant identified the specific location of the information for demonstrating communication independence in the licensing basis, but the staff would like the response to be part of the FSAR. The staff issued a supplemental question requesting the applicant to incorporate the response into DCD Tier 2 Section 7.2.2.3. In the June 16, 2016, supplemental response to RAI 45-7883, Question 07.09-6 (ML16168A473), the applicant committed to updating DCD Tier 2 Section 7.2.2.3, to discuss communication independence. The supplemental response is acceptable. The verification that the proposed markups are incorporated into the next revision of the FSAR was a confirmatory item. The staff verified that the proposed markups have been incorporated into the Revision 1 of DCD Tier 2 Section 7.2.2.3. As such, this confirmatory item has been satisfied.

The SDL is used to send data within a safety division, to send data to other safety divisions, and to send data to non-safety divisions. Table 7.9-3 lists the data communication of Serial Data Link.

Table 7.9-3: SDL for Safety Systems Data Communication

Source: DCD Tier 2 Section 7.9; the Safety I&C System TeR

Systems	From	To	Network Type	Purpose
PPS	Redundant bistable processor in one division	(1) Redundant LCL processors within the same division (2) Redundant LCL	(1) Non-fiber SDL (2) Fiber optic SDL	Transmit (TX): Bistable trip status for LCL voting logic

Systems	From	To	Network Type	Purpose
		processors in other divisions		Receive (RX): none
PPS	Redundant LCL processors in one division	(1) ESF-CCS group controller within the same division (2) ESF-CCF group controller in other divisions	SDL	TX: Initiation signals to the group controllers for selective 2oo4 voting logic RX: none
PPS	Bistable processors, Local Coincidence Logic processors	MTP, Operator Module, and ITP	Bidirectional SDN	TX: Send status data to receiving systems RX: Receives testing data
PPS	Safety Console: Operating bypass switch hardwired to CPM	PPS BS	SDL	TX: CPM sends signal to PPS bistable processor
PPS	Safety Console: Setpoint reset switch hardwired to CPM	PPS bistable processor	SDL	TX: CPM sends signal to PPS bistable processor
CPCS consists of: CPC rack consists of: CPC processor, auxiliary CPC processor, and CEAC racks 1 and 2 CEAC racks 1 and 2 each consists of: CEAC and a CPP	(1) CPP (2) CPP (3) CEAC	(1) CPP and CEAC processor within the same channel and other channels (2) CPC within the same channel (3) CPC	SDL	(1) TX: sends CEA position signals (2) TX: sends target CEA position signals (3) TX: sends penalty factors and target CEA position signals

Systems	From	To	Network Type	Purpose
ESF-CCS	ESF-CCS group controller	MTP, ITP	SDN	TX: Sends status data to receiving systems
ESF-CCS	ESF-CCS loop controller	MTP	SDN	TX: Sends ESF component status data to receiving system
ESF-CCS	ESF-CCS group controller	ESF-CCS loop controller	SDL	TX: group controller sends control signals to loop controller
ESF-CCS	Safety Console: ESF Actuation manual switches hardwired to CPM	ESF-CCS group controller	SDL	TX: CPM sends commands to group controllers for system level and component level
ESF-CCS	Safety Console: Minimum inventory manual switches hardwired to CPM	ESF-CCS loop controller	SDL	TX: group controller sends component control signals to LCs
QIAS-P	QIAS-P processor	(1) To IPS: QIAS-P processor to MTP via SDN, to IPS via one-way Ethernet to DCS Gateway Server, then through DCN-I Network (2) To QIAS-N processor: QIAS-P processor to ITP via SDN, then to QIAS-N via one-way SDL	(1) MTP via SDN, IPS via Ethernet (2) ITP via SDN, QIAS-N processor via SDL	TX: Sends the value and system status data; MTP and ITP serves as data communication isolation function and electrical isolation function between safety-related and non-safety systems unidirectional

Systems	From	To	Network Type	Purpose
QIAS-P	QIAS-P processor	QIAS-P display	SDN	TX: Sends status data for display
ESCM	ESCM	CCG	Bidirectional SDN	TX: Sends component control signal RX: Equipment feedback signal
ITP	ITP	ITP	SDN	RX: status data
MTP	MTP	bistable processor, LCL, CPCS, ESF-CCS	Bidirectional SDN	TX: sends testing data and setpoint data RX: status data
Operator module	operator module	(1) bistable processor, LCL, ESF-CCS (2) CPCS	Bidirectional SDN	(1) RX: status data TX: sends testing data and setpoint data (2) TX: send setpoint data
CPM of MCR	CPM	(1) bistable processor in the PPS (2) ITP (3) ESF-CCS group controller (4) ESF-CCS loop controller	SDN	RX: receive status information
CPM of the RSR	CPM	(1) CCG (2) group controllers	SDL	TX: CPM sends MCR/RSR master transfer switch signals to CCG and group controllers

Systems	From	To	Network Type	Purpose
CCG	CCG	ESF-CCS loop controller	Bidirectional SDN	TX: sends component control signal RX: receives feedback data

The SDL is used to interface between ITP to QIAS-N but data flow is unidirectional from safety to non-safety. According to Section C.4.1.5 of the Safety I&C System TeR, “the QIAS-N is programmed only to receive data and the transmission of any raw data is not allowed via the ITP. Any failure of this data link will not prevent the safety-related systems from performing their intended safety functions.”

Ethernet is used to interface between MTP to IPS, but data flow is unidirectional from safety to non-safety. Section 4.2.3.4 of the Safety I&C System TeR, states:

> The MTP provides the capability to modify the PPS setpoints and CPCS addressable constants. Also the MTP displays process variables, system setpoints, CPC-CWP status and various system statuses. The MTP also provides an interface to initiate and support testing. It is located in the MTC and is shared with other [safety-related] I&C systems within the division. The MTP provides the interface to the IPS through a non-safety network. The MTP only transmits data to the IPS using the unidirectional protocol for functional separation. There is no handshaking in the protocol. Fiber optic cabling is used for the link between the MTP and IPS for electrical isolation.

Section 4.3.1.5 of the Safety I&C System TeR, states “[t]his MTP interface is a unidirectional point-to-point Ethernet datalink from the MTP to the DCN-I gateway." In addition, Figure 4-22 of the technical report shows that the MTP to IPS link is a one way fiber optic cable. According to Section C.4.2 of the Safety I&C System TeR, “the MTP does not receive the data from the IPS (no receiving connection). The MTP processor acts as a CP providing a buffer circuit between the safety processor modules and the non-safety systems.” The staff issued RAI 348-8279, Question 07.09-11, to request the applicant to clarify what is meant by “no receiving connection” since a typical Ethernet connectors have 4 pairs of wires. It was not clear to staff if a standard Ethernet cable is used or a modified cable/connectors with TX pairs/pins on the non-safety end removed and RX pairs/pins on the safety end removed. In the August 25, 2016, supplemental response to RAI 348-8279, Question 07.09-11 (ML16238A434), the applicant provided additional markups to address staff’s concerns and also committed to incorporating the response into the Safety I&C System TeR. The applicant explained that a special converter is used to implement one way data transmission. The staff finds the supplemental response acceptable since it is clear that the connection between MTP and DCS/IPS is one-way data transmission. The verification that the proposed markups are incorporated into the next revision of the FSAR was a confirmatory item. Also, Section 7.9.1.4 of the DCD Tier 2 states “the MTP sends data to the IPS through the DCS gateway server using fiber-optic cable unidirectional... The DCS gateway server receives data from safety-related systems with fiber-optic isolation.” Besides the MTP, it was not clear to the staff if there are any other safety-related systems that

send data to the DCS gateway. The staff issued RAI 348-8279, Question 07.09-10 to request the applicant to clarify, and update the FSAR as appropriate. In the July 13, 2016, supplemental response to RAI 348-8279, Question 07.09-10, the applicant provided additional markups to address staff's concerns and also committed to incorporating the response into DCD Tier 2 Section 7.9.1.4. The staff finds the supplemental response acceptable since it is clear that only the MTP sends data to the DCS gateway server, and it is a one-way data transmission with acceptable fiber optic isolation. The verification that the proposed markups are incorporated into the next revision of the FSAR was a confirmatory item. The staff verified that the proposed markups have been incorporated into the Revision 1 of DCD Tier 2 Section 7.9 and Revision 1 of the Safety I&C System TeR, Section 4.3.1.5. As such, these confirmatory items have been satisfied.

Section C.4 of the Safety I&C System TeR states interdivisional communications conform to DI&C-ISG-04 Interdivisional Communication guidance:

- SDL between bistable processor and LCL – Table 7.9-3.
- SDL between LCL and group controller – Table 7.9-3.
- SDL between ITPs – Table 7.9-3.
- SDL between CPCS CPP and CEAC/CPP – Table 7.9-4.
- Ethernet between IFPD and ESCM – Table 7.9-5.

The following tables evaluate these interfaces for conformance to DI&C-ISG-04's interdivisional communication guidance.

Table 7.9-4: Evaluation of SDL Interdivisional Communication Between (1) bistable processor and LCL, (2) LCL and group controller, (3) ITPs

Point	Acceptable?	Basis
1	Yes	Section C.5.1 of the Safety I&C System TeR, states, compliance of the platform is provided in Reference 12 [Common Q Platform Topical Report]. Voting logic supports reactor trip and ESF safety functions. Since a voting scheme is used for these safety functions, and any partial trigger or ESF actuation function is accomplished prior to the voting function, the staff concludes that a safety division is not dependent on information from outside its safety function to accomplish the safety function.
2	Yes	Section C.5.1 of the Safety I&C System TeR, states, compliance of the platform is provided in Reference 12 [Common Q Platform Topical Report]. For the PPS, since each division receives data from redundant divisions for voting purposes, the division is protected from any spurious or missing data received from outside its division. In addition, communications failures will be detected, as described in Section 7.9.4.5 of this SER and will be accommodated through identifying invalid signals received in the communications processor and using voting logic modification to accommodate the identified invalid signals. Therefore, each PPS division will not be adversely influenced by information received outside its safety divisions.
3	Yes – PPS, Yes - ITP	Section C.5.1 of the Safety I&C System TeR, states, compliance of the platform is provided in Reference 12 [Common Q Platform Topical Report]. PPS: Interdivisional communication between the redundant divisions of the PPS is for voting purposes only. 2oo4 and 2oo3 voting protects against the effects of a single failure in a division. As such, the staff finds that interdivisional communication between redundant portions of the PPS enhances safety functions by supporting voting function, which is used to ensure that the PPS can perform its safety function given a single failure of one PPS division concurrent with another PPS division out of service for testing/maintenance.

Point	Acceptable?	Basis
		ITP: The staff issued RAI 45-7883, Question 07.09-4, to request the applicant to discuss how the ITP communications to display CIV positions support or enhance the performance of the safety functions. In the September 28, 2015, response to RAI 45-7883, Question 07.09-4 (ML15266A521), the applicant did not address the staff's concerns. The response did not describe how the ITP interdivisional communications support or enhance the performance of the safety function. The staff found that the applicant's proposal to use the ITAAC process for providing the human factors analysis to demonstrate that this data communication supports safety is not acceptable since the staff needs to base the safety finding on the information in the design certification. The ITAAC process is only a verification that the as-built system meets design requirements. As such, the staff requested supplemental information from the applicant to provide analysis demonstrating how displaying CIV status on one display benefits safety, potentially involving human factors and probabilistic risk assessment insights. The requested analysis should describe in detail the plant critical safety function that the control room operators would need to take to confirm isolation of all 160 containment penetrations. In the September 28, 2016, supplemental response to RAI 45-7883, Question 07.09-4 (ML16272A488), the applicant provided a HFE analysis demonstrating how displaying CIV status on one display benefits safety. The applicant stated, "Confirming the isolation status of all containment penetrations is a plant critical safety function because these indications are Type B AMI variables. In order for the control room operators to confirm the isolation of all containment penetrations, information regarding the positions of all 160 CIVs in divisions A, B, C and D is provided to both divisions A and B of the QIAS-P." The RAI response states that there are 160 CIVs that isolate containment at various containment penetrations. Figure 6.2.4-1, "Containment Isolation Valve Arrangement," in DCD Tier 2 Chapter 6, shows the different CIV arrangements used to isolate containment at the various containment penetrations. Some penetrations are isolated by a single CIV, and others are isolated by two CIVs in series. As stated in the RAI response, when two CIVs are provided in series, they are generally powered from different safety trains. To determine whether containment is isolated, the operator must determine the status of containment isolation at each penetration. The APR1400 design credits the Class 1E QIAS-P Division A and the QIAS-P Division B displays on the Safety Console with providing the operator information about the

Point	Acceptable?	Basis
		status of each CIV following an accident. The interdivisional communication of the ITP allows the operator to access information about the CIVs at each penetration from either division of the QIAS-P. This means that the operator can look at either the QIAS-P Division A display or the QIAS-P Division B display to determine the position of all of the CIVs even though the CIVs are powered from different safety trains. Both QIAS-P displays show the operator a picture of the CIVs as they are arranged at each penetration, and they also show the operator the position of each CIV by using different colors for valves that are open and valves that are closed (e.g., red is for open valves and green is for closed valves). Following an accident, if one or more CIV(s) fail(s) to close, then the operator will be able to determine this by looking at the QIAS-P display because the display will show the operator the position of each valve. Any CIVs that failed to close will be red. The operator will then be able to assess whether containment is isolated at that penetration because the display will also show the operator whether there is a CIV in series with any CIVs that failed to close and the position of the CIV that is in series with the CIV that failed to close. If the operator sees that there is a green (i.e., closed) CIV in series with any CIV(s) that failed to close, then he or she will be able to determine that containment is isolated at that penetration. If there is not another CIV in series with any CIVs that failed to close, then he or she will be able to determine that containment is not isolated and take appropriate actions. Therefore, the operator only needs to look at either QIAS-P display to determine whether containment is isolated. Without the interdivisional communication of the ITP, the QIAS-P Division A display would show only the CIVs powered by its associated safety trains and the QIAS-P Division B display would only show the CIVs powered by its associated safety trains. Thus, although the QIAS-P Division A display would show the position of the CIVs in its safety trains and the QIAS-P Division B display would show the position of its CIVs in its safety trains, neither display would show the operator the arrangement of all of the CIVs at each penetration. To determine whether containment is isolated, the operator would need to look at both displays to ensure that all CIVs were closed. If all CIVs do close, they will all be green, and the operator will be able to determine this with as much effort and time as it would take using a single QIAS-P display (i.e., with interdivisional communication). However, if one or more CIV(s) fail(s) to close, then the operator will need to determine (1) whether there is a CIV in series with the CIV

Point	Acceptable?	Basis
		that failed to close and (2) the position of the CIV in series with the CIV that failed to closed. The QIAS-P displays would not tell the operator whether there is a CIV in series with any CIV(s) that failed to close. Therefore, the operator will need to find that information from another source. For example, as discussed in the RAI response, if CIV Feedwater-131, which is in series with CIV Feedwater-132 and powered from safety train A, fails to close, then the operator would see Feedwater-131 as red on the QIAS-P Division A display. Because the operators are not required or expected to memorize the arrangement of each CIV at each penetration, the operator would need to consult another source of information to discover that (1) another CIV is in series with CIV Feedwater-131, and (2) CIV Feedwater-132 is the identification number of the CIV that is in series with Feedwater-131. Then, because Feedwater-132 is powered from safety train B, the operator would need to navigate to the correct page of the QIAS-P Division B display to see whether Feedwater-132 was open or closed. It is possible that the operator could make a human performance error when trying to determine if any other CIVs are in series with any CIVs that failed to close or when looking at the status of any CIVs in series with the CIVs that failed to close. Such a human performance error could cause the operator to think that containment was isolated when it is actually not. The staff notes that unless there has been a loss of the non-safety displays concurrent with an accident, the operator will most likely use the LDP or the displays at the operator consoles to determine the status of containment isolation. The operator must use the QIAS-P display at the Safety Console only if the LDP and operator consoles are unavailable, which is expected to be an infrequent occurrence. Thus, the applicant has chosen to reduce the independence of the two QIAS-P divisions in order to minimize human performance errors that could occur during an event that is not expected to occur frequently. However, the displays on the Safety Console are a backup to the normal or non-safety displays, and the operators will primarily interact with the LDP and operator consoles. As a result, the operators may be less familiar with using the QIAS-P displays. Having clear and succinct indications on the QIAS-P displays helps to minimize human performance errors that could occur as a result of an operator being less familiar with using the QIAS-P displays. This becomes even

Point	Acceptable?	Basis
		more important when considering performance-shaping factors, such as stress on the operator, that are likely to impact human performance following an accident. Accordingly, the staff concludes that having both QIAS-P displays show the operators the position of each CIV and the arrangement of the CIVs at each penetration is an effective and efficient method of providing information to the operator about the status of containment isolation that also minimizes the likelihood of human performance errors. Based on supplemental response and HFE's analysis, the staff finds that ITP interdivisional communications support or enhance the performance of the safety functions. The applicant proposed to include the justification and the supporting analysis in the Safety I&C System TeR. As such, the incorporation of the proposed markups in the next revisions to this technical report was a confirmatory item. The staff verified that the proposed markups have been incorporated into the Revision 1 of the Safety I&C System TeR. As such, this confirmatory item has been satisfied.
4	Yes	Section C.5.1 of the Safety I&C System TeR, states, compliance of the platform is provided in Reference 12 [Common Q Platform Topical Report]. The platform uses separate communications modules from function processors that operate asynchronously to each other. In addition, the function processor only accesses shared information with the communications module only through the DPRAM.

Point	Acceptable?	Basis
5	Yes	Applicant is to address PSAI 6.6 of the Common Q Platform Topical Report SER, which states "when implementing a Common Q safety system the licensee must review Westinghouse's timing analyses and validation tests for the Common Q system in order to verify that it satisfies its plant-specific requirements for system response and display response time presented in the accident analysis in Chapter 15 of the safety analysis report." The staff issued RAI 43-7887, Question 07.01-25, to request the applicant to confirm the CPU load limit of 70 percent (as stated in the Common Q Platform Topical Report) and to provide timing analyses and validation tests for the Common Q system in order to verify that it satisfies its plant-specific requirements for system response and display response time presented in the accident analysis in Chapter 15 of the safety analysis report. The staff's evaluation of this RAI is in Section 7.1.4.9 of this SER.
6	Yes	Section C.5.1 of the Safety I&C System TeR, states, compliance of the platform is provided in Reference 12 [Common Q Platform Topical Report]. The communication protocol does not require any handshaking between the safety function processor and the communications processor. Handshaking is only performed within the DPRAM of the communications processor which is acceptable based on Section 1, Staff Position 6 of DI&C-ISG-04.
7	Yes	Section C.5.1 of the Safety I&C System TeR, states, compliance of the platform is provided in Reference 12 [Common Q Platform Topical Report]. The function processor only accepts predefined data sets, and uses a CRC check to ensure the integrity of the data. Faulted messages are flagged and ignored in subsequent logic.
8	Yes	Section C.5.1 of the Safety I&C System TeR, states, compliance of the platform is provided in Reference 12 [Common Topical Report]. Data exchange between redundant safety divisions is done using a separate communications processor that interfaces with the safety function processor through a shared DPRAM. The staff has determined that data exchange between redundant divisions of the safety-related I&C systems is processed in a manner that does not

Point	Acceptable?	Basis
		adversely affect the safety function of the sending divisions, the receiving division, or any other independent division.
9	Yes	Section C.5.1 of the Safety I&C System TeR, states, compliance of the platform is provided in Reference 12 [Common Qualified Topical Report]. In the safety-related I&C systems, DPRAM locations for storing incoming messages are predefined during application software generation. Separate, fixed memory locations are used for input (receive) and output (send) messages.
10	Yes	Section C.5.1 of the Safety I&C System TeR, states, conformance to DI&C-ISG-04, Section 1, Staff Position 10, and that "software is loaded into the processor module by a serial connection between the portable workstation and the processor module. This loading cable is always disconnected on each end to prevent inadvertent programming during plant operation...The compliance of the platform is provided in Reference 12 [Common Q Platform Topical Report]." Section 5.6.10 of the Common Q Platform Topical Report states that "When the reboot occurs, the Windows operating system is started up in order to be able to use the tool that connects to the AC160 for maintenance...When the tool is connected and the execution of the application program in the safety function processor is halted in order to change software...." It was not clear to the staff if the MTP is used for maintenance and software loading as discussed in the Common Q Platform Topical Report. The staff issued RAI 348-8279, Question 07.09-8, to request the applicant update the Safety I&C Technical Report with information regarding whether the MTP will be used for software loading. In the March 3, 2016, response to this RAI (ML16063A177), the applicant stated that the Safety I&C System TeR will be revised by the response to RAI 317-8271, Question 14.03.05-18 to indicate the MTP is not used for software loading. In the June 30, 2016, response to RAI 317-8271, Question 14.3.5-18, the applicant proposed to modify the Safety I&C System TeR to state that the MTP will not be used to load software for safety-related I&C systems. The staff finds that the proposed commitment to not use the MTP to load software and that instead, a normally disconnected portable workstation will be used to load software is acceptable because it conforms to the guidance of DI&C-ISG-04, Section 1, Staff Position 10. The evaluation of RAI 314-8271, Question 14.3.5-18 along with the confirmatory item tracking the

Point	Acceptable?	Basis
		proposed changes is documented in Section 14.3.5 of this SER. Thus, RAI 348-8279, Question 07.09-8, is closed and resolved.
11	Yes	Section C.5.1 of the Safety I&C System TeR, states, compliance of the platform is provided in Reference 12 [Common Q Platform Topical Report]. As discussed in Common Q Platform Topical Report SER, the platform does not propose any provision for sending or receiving software instructions from other divisions.
12	Yes	Section C.5.1 of the Safety I&C System TeR, states, compliance of the platform is provided in Reference 12 [Common Q Platform Topical Report]. Sections C.5.1.1, C.5.1.2, C.5.1.3, and C.5.1.4 of the Safety I&C System TeR stated "[t]he compliance of the platform is provided in Reference 12 [Common Qualified Topical Report]." for DI&C-ISG-04, Section 1, Staff Position 12. The staff issued RAI 348-8279, Question 07.09-16, to request the applicant to discuss if there any data communication failures that are APR1400 I&C architecture specific. See staff's evaluation in Section 7.9.4.5 of this SER for the evaluation of the response to this RAI.
13	Yes	Section C.5.1 of the Safety I&C System TeR, states, compliance of the platform is provided in Reference 12 [Common Topical Report]. As discussed in Common Q Platform Topical Report SER, "when errors are detected the systems are designed to flag data as failed and to enter into a state that would not compromise the safety functions of the system. The Common Q Platform Topical Report does not propose any inter-channel/interdivisional communications or input from any external systems that would be required for performance of the system safety functions. Therefore, each safety processor is not dependent upon any information or resource originating from outside processor's own safety division to perform its assigned safety functions."
14	Yes	Section C.5.1 of the Safety I&C System TeR, states, compliance of the platform is provided in Reference 12 [Common Q Platform Topical Report].

Point	Acceptable?	Basis
		As discussed in Common Q Platform Topical Report SER, “transmission of data over the Common Q HSL [SDL] is unidirectional and does not rely on acknowledgement from the receiving processor. The Common Q HSL [SDL] communications is designed to achieve a logical point-to-point configuration. No equipment outside of the divisions of the sending and receiving processors is relied upon to establish communications between these safety processors.”
15	Yes	Section C.5.1 of the Safety I&C System TeR, states, compliance of the platform is provided in Reference 12 [Common Q Platform Topical Report]. As discussed in Common Q Platform Topical Report SER, “the data transmission cycle time and the amount of data transferred during a cycle is determined by application-specific design. The data transmitted and the frequency of transmission remains fixed for any given configuration while the system is operable. The Common Q system also has provisions for identifying data as being updated even if it has not changed in value since the previous update.”
16	Yes	Section C.5.1 of the Safety I&C System TeR, states, compliance of the platform is provided in Reference 12 [Common Q Platform Topical Report]. As discussed in Common Q Platform Topical Report SER, “the protocols used for the HSL [SDL] interface include provisions for identifying a loss of connectivity. In addition, the processing section of the processor module functions independently from the communications section and is designed to accomplish all safety related function tasks independently of the communications processor. Even if the communications processor were to stall, there would be no loss of system safety functionality.”
17	Yes	Section C.5.1 of the Safety I&C System TeR, states, compliance of the platform is provided in Reference 12 [Common Q Platform Topical Report]. As discussed in Common Q Platform Topical Report SER, “NRC staff has determined that the Common Q platform meets the guidance provided by Section 1, Staff Position 17.
18		Section C.5.1 of the Safety I&C System TeR, states, compliance of the platform is provided in Reference 12 [Common Q Platform Topical Report].

Point	Acceptable?	Basis
		As discussed in Common Q Platform Topical Report SER, "the proposed functionality for the Common Q platform includes (1) Cross divisional communications for the purpose of coincidence voting over the HSL, (2) Communications to external non-safety systems. Neither of these functions is considered to be unneeded." These communications are analyzed in an FMEA in Section 7.2 and Section 7.3.
19	Yes	Section C.5.1 of the Safety I&C System TeR, states, "[t]he data communication systems are designed with a sufficient performance margin to perform its designed functions under conditions of maximum load. Real-time performance is determined by performing response time analysis for all safety functions. An analysis for each function is performed to demonstrate that the actual system response time is less than the response time requirements. The delays of data transport due to data communication in the data communication system are included in response time. The data communication system response time calculations are validated through sample tests, during system integration testing." DCD Tier 1, ITAAC Table 2.5., Item 10, provides response time analysis and testing acceptance criteria. This ITAAC requires the identification of the required response time to support the safety analysis response time. See Section 7.1.4.9 of this SER for the evaluation of the response to RAI 43-7887, Question 07.01-25 regarding CPU loading limits for additional considerations on response time.
20	Yes	Section C.5.1 of the Safety I&C System TeR, states, compliance of the platform is provided in Reference 12 [Common Q Platform Topical Report]. As discussed in Section 7.1.4.9 of this SER, the Common Q Supplemental TeR, states, in part, that the maximum load of the Common Q platform CPU (AC160) to be used for the APR1400 CPCS system needs to be raised to 75 percent, which exceeds the 70 percent CPU load limit as specified in the Common Q Platform Topical Report. In addition, many restrictions for configuration and programming have been proposed in the Common Q Supplemental TeR, so the task processing and communication in the CPCS could be deterministic. However, the above Common Q Platform Topical Report specifies that the maximum CPU load must not exceed a value of 70 percent to

Point	Acceptable?	Basis
		ensure the deterministic communication. See Section 7.1.4.9 of this SER for the evaluation of the response to RAI 43-7887, Question 07.01-25, regarding CPU load limits. DCD Tier 1 Table 2.5.1, Item 16, provides response time analysis and testing acceptance criteria. This response time test is used to verify that adequate throughput exists for the safety-related systems to satisfy the Chapter 15 response time requirements.

Table 7.9-5: Evaluation of SDL Interdivisional Communication Between CPCS CPP and CEAA/CPP

Point	Acceptable?	Basis
1	Yes	Section C.5.1 of the Safety I&C System TeR, states, "although each CPCS channel normally uses RSPT data from other channels to optimize the DNBR and LPD calculations, the safety function of each channel can be performed *if erroneous non-conservative inter-channel data is generated or if the inter-channel data is lost.* Therefore, it can be concluded that a CPCS channel is not dependent on any information or resource originating or residing outside its own safety channel to accomplish its safety function." See staff's evaluation for Point 2 below regarding undetectable failures.
2	Yes	Section C.5.1 of the Safety I&C System TeR, states, compliance of the platform is provided in Reference 12 [Common Q Platform Topical Report]. Section C.5.1.3.7 of the Safety I&C System TeR discusses failures modes for RSPT which are detectable by CPCS and through diagnostics. The staff issued RAI 348-8279, Question 07.09-19, to request the applicant to discuss failures which have been identified through analysis but cannot be detected through equipment or diagnostics, and how those undetectable failures are addressed. In the March 4, 2016, response to RAI 348-8279, Question 07.09-19, the applicant provided additional markups to address staff's concerns and also committed to incorporating the response

		into DCD Tier 2 Table 7.2-7, as part of response to another question, RAI 07.02-8. The staff finds the response acceptable since the APR1400 can withstand an undetectable single failure in one CEAC side including RSPTs, and still generate the DNBR and the LPD trips through the remaining CEACs to calculate the penalty factors and send penalty factors to the CPC. Also, PPS still remains in 2oo3 coincidence logic. The verification that the proposed markups are incorporated into the next revision of the FSAR was a confirmatory item. The staff verified that the proposed markups have been incorporated into the Revision 1 of DCD Tier 2 Table 7.2-7. As such, this confirmatory item has been satisfied.
3	Yes	DI&C-ISG-04, Section 1, Staff Position 3 states, in part, "A safety channel should not receive any communication from outside its own safety division unless that communication supports or enhances the performance of the safety function." It was not clear to the staff how the CPP and CEAC/CPP interdivisional communication as described in Section C.5.1.3 of the Safety I&C System TeR, meets DI&C-ISG-04, Section 1, Staff Position 3. Specifically, the staff requested the applicant to describe how the CPCS interdivisional communications support or enhance the performance of the safety functions. The staff issued RAI 348-8279, Question 07.09-18, to request the applicant to address this portion of DI&C-ISG-04 and update the FSAR accordingly. In the March 4, 2016, response to RAI 348-8279, Question 07.09-18 (ML16064A364), the applicant provided a justification for how the CPP and CEAC/CPP interdivisional communication enhance the safety function. However, the staff found the analysis supporting this justification is incomplete. Specifically, the applicant did not discuss the uncertainties and assumptions with regards to potential system failures if the CPCS channels cannot share data. The staff requested the applicant to supplement the RAI response to provide this information. Pending the resolution of this issue, RAI 348-8279, Question 07.09-18, was tracked as an open item. In the July 27, 2017 supplemental response to RAI 348-8279, Question 07.09-18 (ML17208B042), the applicant provided a description of how the interdivisional communication to share RSPT 1 and 2 values enhances the safety function. [

		]. Because the applicant demonstrated how the interdivisional communication for the CPCS enhances safety in accordance with DI&C-ISG-04, Section 1, Staff Position 3, the staff finds the open item associated with RAI 348-8279, Question 07.09-18, is closed and resolved. The staff verified that the incorporation of the proposed markups from this response in Revision 1 of the Safety I&C System TeR.
4	Yes	Section C.5.1 of the Safety I&C System TeR, states, compliance of the platform is provided in Reference 12 [Common Q Topical Report]. The platform uses separate communications modules from function processors that operate asynchronously to each other. In addition, the function processor only accesses shared information with the communications module only through the DPRAM.
5	Yes	As discussed in Section 7.1.4.8 of this SER, the Common Q Supplemental TeR states, in part, that the maximum load of the Common Q platform CPU (AC160) to be used for the APR1400 CPCS system needs to be raised to 75 percent, which exceeds the 70 percent CPU load limit as specified in the Common Q Platform Topical Report. In addition, many restrictions for configuration and programming have been proposed in the Common Q Supplemental TeR, so the task processing and communication in the CPCS could be deterministic. However, the above Common Q Topical Report specifies that the maximum CPU load must not exceed a value of 70 percent to ensure the deterministic communication. See Section 7.1.4.9 of this SER for the evaluation of the response to RAI 43-7887, Question 07.01-25, regarding CPU load limits.
6	Yes	Section C.5.1 of the Safety I&C System TeR, states, compliance of the platform is provided in Reference 12 [Common Q Platform Topical Report]. The communication protocol does not require any handshaking between the safety function processor and the communications processor. Handshaking is only performed within the DPRAM of the communications processor which is acceptable based on Section 1, Staff Position 6 of DI&C-ISG-04.

7	Yes	Section C.5.1 of the Safety I&C System TeR, states, compliance of the platform is provided in Reference 12 [Common Q Platform Topical Report]. The function processor only accepts predefined data sets, and uses a CRC check to ensure the integrity of the data. Faulted messages are flagged and ignored in subsequent logic.
8	Yes	Section C.5.1 of the Safety I&C System TeR, states, compliance of the platform is provided in Reference 12 [Common Q Platform Topical Report]. However, the APR1400 architecture specific data communication failures beyond what is stated have been evaluated– see staff evaluation of Staff Position 12 below.
9	Yes	Section C.5.1 of the Safety I&C System TeR, states, compliance of the platform is provided in Reference 12 [Common Q Platform Topical Report]. In the safety-related I&C systems, DPRAM locations for storing incoming messages are predefined during application software generation. Separate, fixed memory locations are used for input (receive) and output (send) messages.
10	Yes	See Table 7.9-3 and the evaluation of the response for RAI 348-8279, Question 07.09-8 in Table 7.9-3, Item 10.
11	Yes	Section C.5.1 of the Safety I&C System TeR, states, compliance of the platform is provided in Reference 12 [Common Q Platform Topical Report]. As discussed in Common Q Platform Topical Report SER, the platform does not propose any provision for sending or receiving software instructions from other divisions.
12	Yes	Section C.5.1 of the Safety I&C System TeR, states, compliance of the platform is provided in Reference 12 [Common Q Platform Topical Report]. Sections C.5.1.1, C.5.1.2, C.5.1.3, and C.5.1.4 of the Safety I&C System TeR state "The compliance of the platform is provided in Reference 12 [Common Qualified Platform Topical Report]." for DI&C-ISG-04, Section 1, Staff Position 12. Staff issued RAI 348-8279, Question 07.09-16, to request the applicant discuss if there any data

		communication failures that are APR1400 architecture specific. See the staff's evaluation in Section 7.9.4.5 of this SER.
13	Yes	Section C.5.1 of the Safety I&C System TeR, states, compliance of the platform is provided in Reference 12 [Common Q Platform Topical Report]. As discussed in Common Q Platform Topical Report SER, "when errors are detected the systems are designed to flag data as failed and to enter into a state that would not compromise the safety functions of the system. The Common Q Platform Topical Report does not propose any inter-channel/interdivisional communications or input from any external systems that would be required for performance of the system safety functions. Therefore, each safety processor is not dependent upon any information or resource originating from outside processor's own safety division to perform its assigned safety functions."
14	Yes	Section C.5.1 of the Safety I&C System TeR, states, compliance of the platform is provided in Reference 12 [Common Q Platform Topical Report]. As discussed in Common Q Platform Topical Report SER, "transmission of data over the Common Q HSL [SDL] is unidirectional and does not rely on acknowledgement from the receiving processor. The Common Q HSL [SDL] communications is designed to achieve a logical point-to-point configuration. No equipment outside of the divisions of the sending and receiving processors is relied upon to establish communications between these safety processors."
15	Yes	Section C.5.1 of the Safety I&C System TeR, states, compliance of the platform is provided in Reference 12 [Common Qualified Topical Report]. As discussed in Common Q Platform Topical Report SER, "the data transmission cycle time and the amount of data transferred during a cycle is determined by application-specific design. The data transmitted and the frequency of transmission remains fixed for any given configuration while the system is operable. The Common Q system also has provisions for identifying data as being updated even if it has not changed in value since the previous update."

16	Yes	Section C.5.1 of the Safety I&C System TeR, states, compliance of the platform is provided in Reference 12 [Common Q Platform Topical Report]. As discussed in Common Q Platform Topical Report SER, “the protocols used for the HSL [SDL] interface include provisions for identifying a loss of connectivity. In addition, the processing section of the processor module functions independently from the communications section and is designed to accomplish all safety related function tasks independently of the communications processor. Even if the communications processor were to stall, there would be no loss of system safety functionality.”
17	Yes	The evaluation of overall equipment qualification requirements is in Section 7.1.4.8 of this SER.
18	Yes	Section C.5.1 of the Safety I&C System TeR, states, compliance of the platform is provided in Reference 12 [Common Q Platform Topical Report]. As discussed in Common Q Platform Topical Report SER, “the proposed functionality for the Common Q platform includes (1) Cross divisional communications for the purpose of coincidence voting over the HSL, (2) Communications to external non-safety systems. Neither of these functions is considered to be unneeded.” These communications are analyzed in an FMEA in Section 7.2 and Section 7.3.
19	Yes	See the evaluation of Position 20 below.
20	Yes	Section C.5.1 of the Safety I&C System TeR, states, compliance of the platform is provided in Reference 12 [Common Q Platform Topical Report]. As discussed in Common Q Platform Topical Report SER, “to ensure that the Common Q system meets its application system response time requirements, the execution time for all of the systems tasks is calculated and measured during system development. This calculation includes terms to address the response time of the memory processing and associated circuits. Westinghouse has imposed a CPU load limit of 70 percent in order to avoid control module overruns which could adversely affect the deterministic behavior and response time of the system. The Common Q system is also designed such that the processing section of the processor module does not depend on any of the data that originates outside of its division to perform its safety functions or to meet its time response requirements. Therefore, data errors and

		error rates will not affect the deterministic performance or response time of the safety function processor." As discussed in Section 7.1.4.8 of this SER, the Common Q Supplemental TeR states, in part, that the maximum load of the Common Q platform CPU (AC160) to be used for the APR1400 CPCS system needs to be raised to 75 percent, which exceeds the 70 percent CPU load limit as specified in the Common Q Platform Topical Report. In addition, many restrictions for configuration and programming have been proposed in the above the Common Q Supplemental TeR, so the task processing and communication in the CPCS could be deterministic. However, the above Common Q Platform Topical Report specifies that the maximum CPU load must not exceed a value of 70 percent to ensure the deterministic communication. See the evaluation of RAI 43-7887, Question 07.01-25 in Section 7.1.4.9 of this SER regarding how deterministic operations will be ensured in the CPCS. DCD Tier 1 Table 2.5.1, Item 16, provides response time analysis and testing acceptance criteria. This response time test is used to verify that adequate throughput exists for the safety-related systems to satisfy the Chapter 15 response time requirements.

Because the applicant demonstrated conformance to DI&C-ISG-04, Section 1 for data communications between redundant portions of safety, and identified all interfaces between safety-related and non-safety systems and their interface type, the staff finds the APR1400 I&C system design meets the requirements of IEEE Std 603-1991, Clause 5.6.1.

Functional Independence

Functional independence is derived from IEEE Std 603-1991, Clause 5.6, requirements to ensure that redundant portions of a safety system are independent from each other to the degree necessary to retain the capability to accomplish the safety function. This is further clarified in Staff Position 1 in Section 1 of DI&C-ISG-04, which states:

> The safety system should not be dependent upon any information or resource originating or residing outside its own safety division to accomplish its safety function. This is a fundamental consequence of the independence requirements of [IEEE Std 603-1991]. It is recognized that division voting logic must receive inputs from multiple safety divisions.

The CSAS is used to actuate the CSS. The logic diagram for CSAS in Figure 7.3-5 in DCD Tier 2 shows four divisions. However, there are only two containment spray pumps. The staff issued RAI 348-8279, Question 07.09-9 to request the applicant to describe the control logic for the two spray pumps, identify the interconnections between Division A/B and C/D for shutdown cooling pump start on CSP trouble, and demonstrate that the functional dependency will not challenge the independence between the divisions. In the September 16, 2016, response to this RAI (ML16262A008), the applicant proposed to update DCD Tier 2 Section 7.6 to include a description and logic diagram of the ESFAS interlocks for both SCP and CSP. The applicant also proposed to include in the Safety I&C System TeR a complete list of interdivisional hardwired links (including those using fiber optic cabling). The applicant stated that SCPs can only be automatically started by an SIAS/CSAS signal when the SCP/CSP cross-connect valves are manually aligned for the CSS function and a CSP is inoperable. Therefore, the applicant concluded that when an SCP actuates concurrently with a single failure of the CSP spuriously actuating, there is no effect on the safety analysis. Based on the proposed modifications to the FSAR to include the description and logic diagram of the interlocks for both SCP and CSP, and the inclusion of the list of interdivisional hardwired links in the ESF-CCS to the Safety I&C System TeR, as well as the justification of why a SCP actuation concurrent with a single failure of the CSP would not have an effect on the safety analysis, the staff finds the issues identified in RAI 348-8279, Question 07.09-9, is closed and resolved. The incorporation of the proposed markups into the FSAR and the Safety I&C System TeR was a confirmatory item. The staff verified that the proposed markups have been incorporated into the Revision 1 of DCD Tier 2 Section 7.6.1.6 and Revision 1 of the Safety I&C System TeR. As such, this confirmatory item has been satisfied.

In the PPS, voting logic is used to support reactor trip and ESF safety functions. Since a voting scheme is used for these safety functions, and any partial trip or ESF actuation function is accomplished prior to the voting function, the staff concludes that a safety division is not dependent on information from outside its safety function to accomplish the safety function. As such, the staff finds that the safety-related I&C systems design has met the functional independence requirements of IEEE Std 603-1991, Clause 5.6.1.

7.9.4.6.2 Independence between Safety Systems and Design Basis Events

IEEE Std 603-1991, Clause 5.6.2, requires safety system equipment required to mitigate the consequences of a specific DBE to be independent of and physically separated from the effects of the DBE to the degree necessary to retain the capability to meet the requirements of this standard. This clause specifies that equipment qualification in accordance with IEEE Std 603-1991, Clause 5.4, is one method that can be used to meet this requirement. In addition, 10 CFR Part 50, Appendix A, GDC 22, requires the protection system to be designed to assure that the effects of natural phenomena, and of normal operating, maintenance, testing, and postulated accident conditions on redundant channels do not result in loss of the protection function.

To meet the requirements of IEEE Std 603-1991, Clause 5.6.2, data communications systems in support of safety-related systems shall meet the equipment qualification requirements of IEEE Std 603-1991, Clause 5.4, and accordingly, provide sufficient diversity to prevent the loss of the PPS. DCD Tier 2 Section 7.1 states that "the [safety-related] systems are implemented by [safety-related] hardware and previously developed software components that are dedicated or qualified for use in nuclear power plants." Equipment qualification is discussed in Section 3.11 of DCD Tier 2. Integrated system testing is performed as part of the development process as described to verify that the performance requirements of the safety functions have been met. In the June 22, 2016, response to RAI 460-8554, Question 7.1-53 (ML16174A176), the applicant stated that DCD Tier 2 Section 3.1.18 describes how the APR1400 design conforms to the requirements of GDC 22. The applicant proposed to modify DCD Tier, Section 7.1.2.24 to reference DCD Tier 2 Section 3.1.18 with respect to how the design meets the functional diversity requirements of GDC 22. The evaluation for independence between safety-related systems and DBEs to meet the requirements of IEEE Std 603-1991, Clause 5.4, is documented in Section 7.1.4.8 of this SER. This evaluation is also supplemented by the evaluation for GDC 4, which requires structures, systems, and components important to safety to be designed to accommodate the effects of and to be compatible with the environmental conditions associated with normal operation, maintenance, testing, and postulated accidents, including LOCAs. This evaluation is documented in Section 7.1.4.8 of this SER.

7.9.4.6.3 Independence between Safety Systems and Other Systems

IEEE Std 603-1991, Clause 5.6.3, requires safety-related system design to be such that credible failures in and consequential actions by other systems do not prevent the safety-related systems from meeting the requirements of this standard. This clause is enumerated by several subclauses, as documented below. The evaluation of the APR1400 safety-related I&C systems design against the requirements of IEEE Std 603-1991, Clause 5.6.3, is completed as a part of the evaluation of each clause. In addition, 10 CFR Part 50, Appendix A, 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 of the protection system. Interconnection of the protection and control systems shall be limited so as to assure that safety is not significantly impaired.

Interconnected Equipment

For interconnected equipment, IEEE Std 603-1991, Clause 5.6.3.1, requires the following.

1) Equipment that is used for both safety-related and non-safety functions to be classified as part of the safety-related systems. Isolation devices used to effect a safety system boundary shall be classified as part of the safety-related system.

2) No credible failure on the non-safety side of an isolation device shall prevent any port of a safety-related system from meeting its minimum performance requirements during and following any DBE requiring that safety function. A failure in an isolation device shall be evaluated in the same manner as a failure of other equipment in a safety-related system.

To address the requirements of IEEE Std 603-1991, Clause 5.6.3, SRP Section 7.9 states that interconnections between safety-related systems and non-safety systems should be designed such that each safety-related system can perform its safety function with no input or influence from the interconnected system, and that any failure of the interconnected system, failure of communications from that system or faulty data transmitted by that system cannot prevent or influence that independent safety determination. This is further clarified by the guidance in DI&C-ISG-04, Section 1 which provides 20 staff positions for communications between safety-related and non-safety systems, and DI&C-ISG-04, Section 3, “Multidivisional Control and Display Stations,” which provides criteria for non-safety multidivisional display and control stations for controlling safety-related equipment.

As part of the evaluation of IEEE Std 603-1991, Clause 5.6.3, the staff also evaluated whether adequate functional independence exists between safety-related systems and non-safety systems. Functional independence is derived from IEEE Std 603-1991, Clause 5.6, requirements to ensure that redundant portions of a safety-related system are independent from each other to the degree necessary to retain the capability to accomplish the safety function. This is further clarified in Staff Position 2 in Section 1 to DI&C-ISG-04 quoted above.

In RAI 45-7883, Question 07.09-5, staff requested the applicant to clarify what is meant by "[QIAS-N] network is implemented by the [SDN]." In the August 5, 2015, response to this RAI (ML15217A252), the applicant stated “[QIAS-N] is the backup system for the [IPS] which is the primary indication and alarm system for operation. The QIAS-N is implemented with the common PLC platform, even though it is a non-safety system, because it displays the important plant parameters and maintains diversity from the IPS…QIAS-N network is implemented with the [Advant Field] 100 communication network.” The staff finds the response acceptable since the non-safety QIAS-N network is designed such that it will not affect the safety network as shown in Figure 7.9-5-1. The applicant committed to updating DCD Tier 2 Section 7.9.1.4 with the clarification. The staff finds this clarification and proposed change to the FSAR is acceptable. The incorporation of the proposed markups in the next revision of the FSAR was a confirmatory item. The staff verified that the proposed markups have been incorporated into the Revision 1 of DCD Tier 2 Section 7.9.1.4. As such, this confirmatory item has been satisfied.

Plant Protection System Interfaces with Non-Safety Systems

For the PPS, the applicant did not provide a complete list of interfaces between safety-related and non-safety I&C systems. As such, the staff issued RAI 45-7883, Question 07.09-2 to request a complete list of interfaces between safety-related and non-safety systems to be included in the FSAR or its referenced technical reports. In the September 28, 2016 response

to this RAI (ML16272A488), the applicant provided a list of interfaces between safety-related I&C systems and non-safety systems and equipment and proposed to include the list in the Safety I&C System TeR. The staff reviewed the identified interfaces and found that several non-safety standalone system interfaces to safety-related I&C systems were not included. The staff requested the applicant to address this issue in a supplemental response to this RAI. RAI 45-7883, Question 07.09-2, was tracked as an open item.

In the August 21, 2017, supplemental response to RAI 45-7883, Question 07.09-2 (ML17233A372), the applicant provided a description of all interfaces between safety-related and non-safety systems, including the interface type. The applicant committed to include this description in the Safety I&C System TeR. In addition, the applicant stated that Section 4.4.4.12 of the Safety I&C System TeR will be revised to include additional clarification that the non-safety signals cannot block the operation of the ESF-actuation signals and will reference Section 7.3.1.9 of DCD Tier 2. To address external interfaces, the applicant provided a modified Figure 4-1 of the Safety I&C System TeR which depicts the interfaces between the I&C systems to external networks (i.e., emergency offsite facility, nuclear emergency response center, and NRC operations center). The applicant also added a description of these interfaces in Section 4.6.2.7 of the Safety I&C TeR and described how the interface is uni-directional between the I&C systems and external networks. [

].
Because the applicant provided additional information to (1) identify all interface between safety-related and non-safety I&C systems and (2) demonstrate how I&C system interfaces to external networks are uni-directional, the staff finds the applicant has addressed the guidance of DI&C-ISG-04, and thus meets the requirements for IEEE Std 603-1991, Clause 5.6. As such, the open item associated with RAI 45-7883, Question 07.09-2, is closed and resolved.

The applicant provided a supplemental response to RAI 45-7883, Question 07.09-2 (ML18124A110), on May 4, 2018, to provide additional details regarding on the one way interface is implemented between the I&C systems to external networks. The applicant provided a new Figure 4-25 for the Safety I&C System TeR depicting how the signal flow and interface between IPS/DCN-I and external interfaces are implemented. The applicant provided a description of the design features that secure the communication to these remote interfaces and included this description in proposed markups to Section 4.6.2.7 of the Safety I&C System TeR. The applicant also provided corresponding markups to Figure 4-1 of the Safety I&C System TeR, Figure 4-1 in the D3 and CCF Coping Analysis TeRs, and Figure 4.1-1 of the Control System CCF Analysis TeR. The staff finds the response and proposed markups are acceptable because the applicant provided sufficient information regarding the design and implementation of the safety I&C system external interfaces to meet the requirements for IEEE Std 603-1991, Clause 5.6. The incorporation of the proposed markups into the next revision of Section 4.6.2.7 of the Safety I&C System TeR, Figure 4-1 of the Safety I&C System TeR, Figure 4-1 in the D3 and CCF Coping Analysis TeRs, and Figure 4.1-1 of the Control System CCF Analysis TeR was a confirmatory item. The staff verified the proposed markups have been incorporated into Section 4.6.2.7 of the Safety I&C System TeR, Revision 3, Figure 4-1 of the Safety I&C System TeR, Revision 3, Figure 4-1 in the D3 TeR, Revision 3, and CCF Coping Analysis TeRs, Revision 3, and Figure 4.1-1 of the Control System CCF Analysis TeR, Revision 3. As such, this confimatory item has been resolved.

Evaluation of Independence Between Safety Systems and Other Systems

Figure C.5-1, “ESCM Interface Diagram,” in the Safety I&C System TeR shows the connections between the ESCM internals components and the IFPD. The Ethernet processor of the ESCM processes data from the IFPD by checking the integrity of the data through error checking mechanism such as CRC. Erroneous data are discarded and not written to the buffer memory of the ESCM. Otherwise, Ethernet processor writes the valid information to the buffer memory. The function processor reads the data from the buffer memory, and checks data integrity through checking parity bit. Erroneous data is not written to the RAM of the CPU section of ESCM. The function processor writes the verified data to a predefined memory location in the RAM of the ESCM. Based on the verified component identification data in the RAM, the function processor reads data of system software and application software from their respective FPROM, and brings up the control template on ESCM FPD for that component. Finally, the operator can manually initiate the control signal for that component.

Table 7.9-6: Evaluation of Data Communication Between Safety and Non-safety Systems		
Point	**Acceptable?**	**Basis**
1	Yes	IFPD (non-safety) only sends component data ESCM (safety-related) to populate data on the control template of the ESCM display; IFPD is not sending any control signal that would operate a safety component. As a result, the ESCM is not depending on any data from the IFPD to perform manual component control of equipment. Also, APR1400 credits system-level actuations for safety functions, and not component control. Operator's manual action is required to activate the component control signal on the ESCM FPD.
2	Yes	IFPD sends data to ESCM the ESCM's Ethernet Communication Module (ECM). The Ethernet processor of the ECM checks the integrity of the IFPD data by error checking code. Erroneous data is dropped and it is not written to the buffer memory. Also, the function processor checks the integrity of the IFPD data in the buffer memory prior to writing the valid data to the RAM. These two verification steps help address Point 2 with regards to the IFPD to ESCM interface not adversely affecting the ESCM safety-related system. As another measure of mitigating possible communication faults due to the non-safety IFPD system, the applicant should address DI&C-ISG-04, Section 1, Staff Position 12, in which the applicant says is not applicable. See RAI for DI&C-ISG-04, Section 1, Staff Position 12 below.
3	Yes	The staff found that additional information is needed to determine if the IFPD to ESCM interdivisional communication conforms to the guidance in DI&C-ISG-04, Section 1, Staff Position 3. Specifically, the applicant needed to demonstrate how the IFPD to ESCM data communication support or enhance the performance of safety functions. The staff issued RAI 348-8279, Question 07.09-13, to request the applicant to address this portion of DI&C-ISG-04 and update the FSAR accordingly In the April 16, 2016 response to this RAI (ML16107A023), the applicant stated that if this communication interface did not exist, operators would need to frequently execute the same screen navigation commands on the IFPD and successively on all four ESCMs. In Revision 1 of the Safety I&C System TeR, the applicant also made additional changes to compare the use of the ESCMs with IFPDs to control safety related equipment versus using the ESCMs by themselves. In Table C.5.1-2, "Operating Step When the IFPD to ESCM Interface Exists" of Revision 1 to the Safety I&C System TeR, the applicant listed each action the operator performs to operate a safety component when the IFPD

Table 7.9-6: Evaluation of Data Communication Between Safety and Non-safety Systems		
Point	**Acceptable?**	**Basis**
		communicates to the ESCM. To operate one safety component, the applicant showed that the operator must perform five actions. In Table C.5.1-3, "Operating Step When the IFPD to ESCM Interface Does Not Exist" of the Safety I&C System TeR, the applicant listed each action the operator would need to perform to operate a safety component if the IFPD did not communicate with the ESCM. To operate one safety component, the applicant showed that the operator must perform eight actions. Furthermore, in the case where the IFPD does not communicate with the ESCM, the operators must select the correct ESCM to use from all four of the possible ESCMs. It is possible that an operator could select the wrong ESCM and operate the wrong component. When the IFPD does communicate with the ESCM, the controls for the equipment automatically appears on the correct ESCM, and the operator does not need to select which ESCM to use. This helps to reduce human error when operating safety components. The staff finds that the applicant should define some terms used to describe Steps 3, 9, 17 and 23 in Table C.5.1-3 so that the staff can evaluate the justification for safety enhancement provided in the April 16, 2016 response. Additionally, the staff requested the applicant clarify a statement in the April 16, 2016 response about how timing analysis would be used. Pending the resolution of these issues, RAI 348-8279, Question 07.09-13, was tracked as an open item. On November 2, 2016, the applicant revised its response to RAI 348-8279, Question 07.09-13 (ML16320A228). The applicant defined the terms used to describe Steps 3, 9, 17 and 23 in Table C.5.1-3. Also, the applicant explained that the steps were necessary because the operators rely on the IFPD to provide information that is needed to operate safety components and is not provided by the ESCM. Therefore, the staff finds the November 2, 2016 response adequately addresses RAI 348-8279, Question 07.09-13, because it describes why the IFPD/ESCM interface enhances safety and conforms to the guidance of DI&C-ISG-04, Section 1, Staff Position 3. The incorporation of the proposed markups into the next revision of the Safety I&C System TeR was a confirmatory item. The staff reviewed Revision 1 of the Safety I&C System TeR and found that most of the information from the proposed markups provided in the November 2, 2016 response to RAI 348-8279, Question 07.09-13 have been

Table 7.9-6: Evaluation of Data Communication Between Safety and Non-safety Systems		
Point	**Acceptable?**	**Basis**
		adequately incorporated. However, the staff identified a typo with the labeling Figure C.5-2. On August 16, 2017, the applicant submitted a supplemental response to this RAI (ML17228A749) to provide proposed markups with correct labeling of this figure. The incorporation of the proposed markups in Revision 2 of the Safety I&C System TeR was a confirmatory item. The staff verified the proposed markups have been incorporated into the Safety I&C System TeR, Revision 2. As such, this confirmatory item has been satisfied.
4	Yes	The Ethernet processor processes IFPD component identification data by checks the data's integrity and writing the data to a shared memory, Buffer Memory. The function processor processes the checked data in the shared Buffer Memory, and checks the data's integrity prior to writing data to the RAM. The Ethernet processor and function processor operate independently of one another – the read (function processor) and write (Ethernet processor) cycles are asynchronous. ESCM is safety-related and its application is developed according to the SPM TeR as ITS class software.
5	Yes	See Table 7.9-3 and the evaluation of the response to RAI 43-7887, Question 07.01-25, in Section 7.1.4.9 of this SER.
6	Yes	Section C.5.1 of the Safety I&C System TeR, states, compliance of the platform is provided in Reference 12 [Common Q Platform Topical Report]. The communication protocol does not require any handshaking between the safety function processor and the communications processor. Handshaking is only performed within the DPRAM of the communications processor which is acceptable based on Section 1, Staff Position 6 of DI&C-ISG-04.
7	Yes	Section C.5.1 of the Safety I&C System TeR, states, compliance of the platform is provided in Reference 12 [Common Q Platform Topical Report].

Table 7.9-6: Evaluation of Data Communication Between Safety and Non-safety Systems		
Point	**Acceptable?**	**Basis**
		The function processor only accepts predefined data sets, and uses a CRC check to ensure the integrity of the data. Faulted messages are flagged and ignored in subsequent logic.
8	Yes	Section C.5.1 of the Safety I&C System TeR, states, compliance of the platform is provided in Reference 12 [Common Q Platform Topical Report]. IFPD sends pre-defined messages (data) to ESCM. The Ethernet processor checks the integrity of the data before writing it to a pre-determined address in the Buffer Memory. Additionally, the function processor checks the integrity of the pre-defined message prior to writing it to a pre-determined location in the RAM. Only pre-defined messages are ready by the function processor for bringing up the control template on the ESCM flat panel display. Based on the above discussion, the data exchanged between safety-related ESCM and the non-safety IFPD is processed in a manner that does not adversely affect the safety function of the sending divisions, the receiving divisions, or any other independent divisions.
9	Yes	Section C.5.1 of the Safety I&C System TeR, states, compliance of the platform is provided in Reference 12 [Common Q Platform Topical Report]. The incoming message data from the IFPD is stored in a fixed predetermined address in the Buffer Memory shared with the ESCM's function processor. This buffer memory is not used for any other purpose. The ESCM only reads the input data from IFPD in the Buffer Memory. The ESCM does not write to the buffer memory. There is no output data from the ESCM so it is not necessary to address memory allocations with regards to segregation of input and output data.
10	Yes	See Table 7.9-3 and the evaluation of the response to RAI 348-8279, Question 07.09-8 in Table 7.9-3, Item 10.
11	Yes	Section C.5.1 of the Safety I&C System TeR, states, compliance of the platform is provided in Reference 12 [Common Q Platform Topical Report].

Table 7.9-6: Evaluation of Data Communication Between Safety and Non-safety Systems		
Point	**Acceptable?**	**Basis**
		As discussed in Common Q Platform Topical Report SER, the platform does not propose any provision for sending or receiving software instructions from other divisions.
12	Yes	Section C.5.1 of the Safety I&C System TeR, states, compliance of the platform is provided in Reference 12 [Common Q Platform Topical Report]. DCD Tier 2 Section 7.1, Page 7.1-3, states, in part, “Data communications within or between I&C systems are designed to provide reasonable assurance that any error in data communication will not cause inadvertent actuations or prevent the safety functions from being performed.” The staff issued RAI 45-7883, Question 07.09-7, to request the applicant to clarify whether the applicant really meant “any” errors as this goal is typically difficult to achieve except on simple communication schemes. The RAI also requested that the applicant describe the potential data communication faults between IFPD and ESCM and the mitigating measures for each fault. In the November 3, 2015, response to this RAI (ML15307A679), the applicant stated, in part, “The use of “any error” in DCD Tier 2 Section 7.1 means the malfunctions that lead to detectable and undetectable failures of data communications. DCD Tier 2 Section 7.1, Page 7.1-3, sub-part, “Data Communication” will be updated as follows: “Data communications within or between I&C systems is provided with the communication independence to ensure that there will be no adverse impact on the safety-related systems. Data communication systems are composed of a qualified PLC data communication network, a non-safety DCS data communication network, a qualified serial data link, and Ethernet network. Communication independence is provided among safety divisions and between safety-related and non-safety data communication systems. The safety-related and non-safety data communication systems are diverse.” Based on the response provided, the staff finds that additional information is needed on how errors are detected and addressed by the ESCM and other portions of the ESF-CCS. As such, the staff requested the applicant to supplemental the response to provide this information. RAI 45-7883, Question 07.09-7, was tracked as an open item.

Table 7.9-6: Evaluation of Data Communication Between Safety and Non-safety Systems		
Point	**Acceptable?**	**Basis**
		In the May 23, 2017 response to RAI 45-7883, Question 07.09-7 (ML17143A240), the applicant provided additional analysis and justification on how certain communication errors will be addressed. Specifically, if these communication errors occur, the operator would be able recognize an error had occurred because the right template would not display on the ESCM. The operator will be able to recognize communication errors due to the additional confirmation step added to the design. Once this occurs, the operator would either move over to a different IFPD or to the ESCMs safety console which has no IFPD interface. Because the applicant demonstrated how these communication errors can be detected (via operator recognition or data communications error detection) and alternative means are provided to operate the components if these errors were to occur, the staff finds the response is acceptable. The applicant proposed to include the additional analysis in the Safety I&C System TeR. The verification that the proposed markups are incorporated into the next revision of the Safety I&C System TeR was a confirmatory item. The staff has verified the proposed markups have been incorporated into the Safety I&C System TeR, Revision 2. As such, this confirmatory item has been satisfied. For DI&C-ISG-04 Section 1, Staff Positions 12, 13, 14, 15, and 17, the applicant stated that these "position is not applicable to the communication between IFPD and the ESCM because communication between the IFPD and ESCM does not perform the safety function [or] because it is not vital communication." The staff disagree with the applicant since DI&C-ISG-04 states "vital communication as used are communications that are needed to support a safety function," and based on the discussions in the Safety I&C System TeR, the IFPD and ESCM connectivity supports a safety function. As such, the staff issued RAI 348-8279, Question 07.09-15, to request the applicant to address DI&C-ISG-04 Section 1, Staff Positions 12, 13, 14, 15 and 17 for the IFPD to ESCM interface. In the April 16, 2016 response to RAI 348-8279, Question 07.09-15 (ML16107A023), the applicant referred to the response to RAI 45-7883, Question 07.09-7, to address DI&C-ISG-04, Section 1, Staff Position 12, which the staff has found to be acceptable. See the staff's evaluation for the response to RAI 45-7883, Question 07.09-7, in the paragraph above.

Table 7.9-6: Evaluation of Data Communication Between Safety and Non-safety Systems		
Point	**Acceptable?**	**Basis**
13	Yes	Section C.5.1 of the Safety I&C System TeR, states, compliance of the platform is provided in Reference 12 [Common Q Platform Topical Report]. As discussed in Common Q Platform Topical Report SER, “when errors are detected the systems are designed to flag data as failed and to enter into a state that would not compromise the safety functions of the system. The Common Q Platform Topical Report does not propose any inter-channel/interdivisional communications or input from any external systems that would be required for performance of the system safety functions. Therefore, each safety processor is not dependent upon any information or resource originating from outside processor’s own safety division to perform its assigned safety functions.” The applicant states DI&C-ISG-04, Section 1, Staff Position 13, “is not applicable to the communication between the IFPD and ESCM because it is not vital communication.” Staff disagree, and request applicant to address the intent of this staff position to include provisions for ensuring that received messages are correct and are correctly understood. The applicant has, in part, provided information to meet the intent of this staff position. For DI&C-ISG-04, Section 1, Staff Positions 12, 13, 14, 15, and 17, the applicant stated that “position is not applicable to the communication between IFPD and the ESCM because communication between the IFPD and ESCM does not perform the safety function [or] because it is not vital communication.” Staff disagrees. DI&C-ISG-04 states "vital communication as used are communications that are needed to support a safety function," and based on the discussions in the Safety I&C System TeR, the IFPD and ESCM connectivity supports a safety function. Staff issued RAI 348-8279, Question 07.09-15, to request the applicant address DI&C-ISG-04 Interdivisional Communication positions 12, 13, 14, 15 and 17 for the IFPD to ESCM interface. In the July 16, 2016, response, to RAI 348-8279, Question 07.09-15 (ML16198A002), the applicant stated, in part, “errors in the IFPD to ESCM Ethernet communication interface are detected… While communication errors do not affect the operation of the ESCM function processor, these compliance descriptions describe the errors that would require the ESCM to be used in a

Table 7.9-6: Evaluation of Data Communication Between Safety and Non-safety Systems		
Point	**Acceptable?**	**Basis**
		standalone manner (i.e., with manual screen navigation to the desired control or function template). The IFPD to ESCM Ethernet communication interface does not include error correction." The staff finds the response acceptable since it conforms to staff guidance in DI&C-ISG-04, Section 1, Staff Position 13. The verification that the proposed markups are incorporated into the next revision of the Safety I&C System TeR was a confirmatory item. The staff verified that the proposed markups have been incorporated into the Revision 1 of the Safety I&C System TeR. As such, this confirmatory item has been satisfied.
14	Yes	Section C.5.1 of the Safety I&C System TeR, states, compliance of the platform is provided in Reference 12 [Common Q Platform Topical Report]. As discussed in Common Q Platform Topical Report SER, "transmission of data over the Common Q HSL [SDL] is unidirectional and does not rely on acknowledgement from the receiving processor. The Common Q HSL [SDL] communications is designed to achieve a logical point-to-point configuration. No equipment outside of the divisions of the sending and receiving processors is relied upon to establish communications between these safety processors." The applicant states DI&C-ISG-04, Section 1, Staff Position 14 "is not applicable to the communication between the IFPD and ESCM because communication between the IFPD and ESCM does not perform a safety function." Staff disagrees with that statement, and requests the applicant address this staff position. The applicant has, in part, provided information to meet the intent of this staff position. For DI&C-ISG-04, Section 1, Staff Positions 12, 13, 14, 15, and 17, the applicant stated that "position is not applicable to the communication between IFPD and the ESCM because communication between the IFPD and ESCM does not perform the safety function [or] because it is not vital communication." The staff disagrees. DI&C-ISG-04 states "vital communication as used are communications that are needed to support a safety function," and based on the discussions in the Safety I&C System TeR, the IFPD and ESCM connectivity supports a safety function. The staff issued RAI 348-8279, Question 07.09-15, to request the applicant to address

Table 7.9-6: Evaluation of Data Communication Between Safety and Non-safety Systems		
Point	**Acceptable?**	**Basis**
		DI&C-ISG-04, Section 1, Staff Positions 12, 13, 14, 15 and 17 for the IFPD to ESCM interface. In the July 16, 2016, response to RAI 348-8279, Question 07.09-15 (ML16198A002), the applicant stated, in part, that "the communication is "point-to point," which, "means that the message is passed directly from the sending node (i.e., IFPD) to the receiving node (i.e., ESCM), without the involvement of equipment outside the division of the sending or receiving node. For example, if there is a failure of the ESCM EPs for Divisions B, C and D, there would be no adverse impact to the communication between any of the four IFPDs at the operator console and the ESCM for Division A. Similarly, if there is a failure of the EPs for three of the four IFPDs, the fourth IFPD would still be able to communicate with all four ESCMs." The staff finds the response acceptable since it conforms to staff guidance in DI&C-ISG-04, Section 1, Staff Position 14. The verification that the proposed markups are incorporated into the next revision of the Safety I&C System TeR was a confirmatory item. The staff verified that the proposed markups have been incorporated into the Revision 1 of the Safety I&C System TeR. As such, this confirmatory item has been satisfied.
15	Yes	Section C.5.1 of the Safety I&C System TeR, states, compliance of the platform is provided in Reference 12 [Common Q Platform Topical Report]. As discussed in Common Q Platform Topical Report SER, "the data transmission cycle time and the amount of data transferred during a cycle is determined by application-specific design. The data transmitted and the frequency of transmission remains fixed for any given configuration while the system is operable. The Common Q system also has provisions for identifying data as being updated even if it has not changed in value since the previous update." The applicant states DI&C-ISG-04, Section 1, Staff Positions 15 "is not applicable to the communication between the IFPD and ESCM because does not perform a safety function." Staff disagrees with that statement, and requests applicant to address this staff position. The applicant has, in part, provided information to meet the intent of this staff position.

Table 7.9-6: Evaluation of Data Communication Between Safety and Non-safety Systems		
Point	**Acceptable?**	**Basis**
		For DI&C-ISG-04 Section 1, Staff Positions 12, 13, 14, 15, and 17, the applicant stated that these "position is not applicable to the communication between IFPD and the ESCM because communication between the IFPD and ESCM does not perform the safety function [or] because it is not vital communication." The staff disagrees with this statement. DI&C-ISG-04 states "vital communication as used are communications that are needed to support a safety function," and based on the discussions in the Safety I&C System TeR, the IFPD and ESCM connectivity supports a safety function. The staff issued RAI 348-8279, Question 07.09-15, to request the applicant address DI&C-ISG-04 Interdivisional Communication positions 12, 13, 14, 15 and 17 for the IFPD to ESCM interface. In the July 16, 2016, response to RAI 348-8279, Question 07.09-15 (ML16198A002), the applicant stated, in part, “the IFPD transmits information data to the ESCM based on event-driven transmission. So, the transmission of data between the IFPD and ESCM takes place when the operator selects the component on the IFPD. In response, the ESCM [Ethernet processor] receives and stores the data set in the predefined address of the buffer memory. Therefore, the operation of the ESCM [Ethernet processor] is also event driven. However, the ESCM [function processor] reads the data set in the buffer memory at regular intervals, whether data in the set has changed or not. In addition, all data from the ESCM [function processor] is transmitted to the ESF-CCS controllers every execution cycle periodically regardless of any data change from the [Ethernet processor].” The applicant proposed to include this description in the Safety I&C System TeR. The staff finds the response is acceptable since it conforms to DI&C-ISG-04, Section 1, Staff Position 15. The verification that the proposed markups are incorporated into the next revision of the Safety I&C System TeR was a confirmatory item. The staff verified that the proposed markups have been incorporated into the Revision 1 of the Safety I&C System TeR. As such, this confirmatory item has been satisfied.
16	Yes	Section C.5.1 of the Safety I&C System TeR, states, compliance of the platform is provided in Reference 12 [Common Q Platform Topical Report]. As discussed in Common Q Platform Topical Report SER, “the protocols used for the HSL [SDL] interface include provisions for identifying a loss of connectivity. In addition, the processing section of the processor module functions independently from

Table 7.9-6: Evaluation of Data Communication Between Safety and Non-safety Systems		
Point	**Acceptable?**	**Basis**
		the communications section and is designed to accomplish all safety related function tasks independently of the communications processor. Even if the communications processor were to stall, there would be no loss of system safety functionality." As discussed in the Safety I&C System TeR, the loss of connectivity between the IFPD and ESCM does not prevent the ESCM from initiating manual component control.
17	Yes	Applicant states DI&C-ISG-04, Section 1, Staff Position 17 "is not applicable to the communication between the IFPD and ESCM." Staff disagrees with that statement, and requests applicant to address this staff position. The applicant has, in part, provided information to meet the intent of this staff position, i.e., equipment qualification. For DI&C-ISG-04 Section 1, Staff Positions 12, 13, 14, 15, and 17, the applicant stated that these "position is not applicable to the communication between IFPD and the ESCM because communication between the IFPD and ESCM does not perform the safety function [or] because it is not vital communication." The staff disagrees with this statement. DI&C-ISG-04 states "vital communication as used are communications that are needed to support a safety function," and based on the discussions in the Safety I&C System TeR, the IFPD and ESCM connectivity supports a safety function. The staff issued RAI 348-8279, Question 07.09-15, to request the applicant address DI&C-ISG-04 Interdivisional Communication positions 12, 13, 14, 15 and 17 for the IFPD to ESCM interface. In the April 16, 2016, response to RAI 348-8279, Question 07.09-15 (ML16107A023), the applicant did not address adequately seismic and EMI. The staff requested the applicant supplement the response to this RAI to address how testing IFPD to ESCM interface to the same seismic and EMI criteria as safety-related systems will ensure that seismic and EMI won't induce spurious failures. The staff found that the applicant needed to document how the ESCM/IFPD interface is environmentally qualified. In the July 16, 2016, response to RAI 348-8279, Question 07.09-15 (ML16198A002), the applicant provided proposed markups to the FSAR to address the staff's concern (i.e., by adding the ESCM/IFPD will be environmentally qualified). The response is acceptable since it conforms to DI&C-ISG-04, Section 1, Staff Position 17. The verification that the proposed markups

Table 7.9-6: Evaluation of Data Communication Between Safety and Non-safety Systems		
Point	**Acceptable?**	**Basis**
		are incorporated into the next revision of the Safety I&C System TeR was a confirmatory item. The staff verified that the proposed markups have been incorporated into the Revision 1 of the Safety I&C System TeR. As such, this confirmatory item has been satisfied.
18	Yes	The evaluation of the FMEA provided in FSAR Sections 7.2 and 7.3 is documented in Sections 7.2 and 7.3 of this SER, respectively.
19	Yes	To comply with DI&C-ISG-04, Section 1, Staff Position 19, the applicant stated "…even if incorrect data are broadcasted or a broadcast data storm occurs on a network causing an excess of data traffic, this failure does not adversely affect the performance of the [function processor] because communication bandwidth is sufficient for the true data rate including overhead." The staff also request the applicant to demonstrate how the effects of data storms are addressed for this connectivity in order to provide reliable data transmissions to support safety-related system functions as required by GDC 13. See staff evaluation of RAI 348-8279, Question 07.09-12 in Section 7.9.4.3.4, "Effects of Data Storms," of this SER.
20	Yes	To conform to DI&C-ISG-04, Section 1, Staff Position 20, the applicant stated "…maximum delay time is calculated as total of network delay time and access cyclic time…based on mean response time plus a value that bounds 97.7 percent of responses for distribution of signal response time typical of an asynchronous signal path." The staff issued RAI 348-8279, Question 07.09-14, to request the applicant to discuss how these response times will be verified for IFPD to ESCM interdivisional communication. In the April 16, 2016, response to this RAI (ML 16107A023), the applicant stated the proposed system response times is 0.5s for control template to presented and 0.5s for dynamic data to be updated. The staff found that these proposed response times are slower by a quarter second than the preferred times the applicant committed to in Technical Report APR1400-E-J-NR-14011, "Basic Human-System Interfaces," (hereafter referred to as Basic Human-Systems Interfaces TeR) but well within the maximum times, and therefore, acceptable. The proposed verification of these times using the HSI test facility is acceptable since the same simulator is used to test all the other HFE design elements. The HFE design process requires an integrated system validation test on a simulator that represents the

Table 7.9-6: Evaluation of Data Communication Between Safety and Non-safety Systems		
Point	**Acceptable?**	**Basis**
		completed APR1400 control room design which should demonstrate that computer response times do not slow or confuse the operator. Based on the above discussion, the staff finds the response acceptable, and applicant conforms to this staff position since the applicant demonstrated that the maximum delay time is calculated in accordance with the guidance of DI&C-ISG-04, Section 1, Staff Position 20 and is bounded by maximum allowed response times. The applicant committed to updating the FSAR and the referenced technical reports. As such, the incorporation of the proposed markups into the next revision of the FSAR and referenced technical reports was a confirmatory item. The staff verified that the proposed markups have been incorporated into the Revision 1 of the Safety I&C System TeR and Revision 1 of Basic Human-Systems Interfaces TeR. As such, this confirmatory item has been satisfied.

DI&C-ISG-04, Section 3 presents guidance concerning operator workstations used for the control of plant equipment in more than one safety division and for display of information from sources in more than one safety division. This guidance also applies to workstations that are used to program, modify, or maintain safety-related systems that are not in the same safety division as the workstation. Multi-divisional control and display stations may themselves be safety-related or not safety-related, and they may include controls and displays for equipment in multiple safety divisions and for equipment that is not safety-related, provided they meet the conditions identified in DI&C-ISG-04.

Section C.5.3 of the Safety I&C System TeR states:

> The APR1400 has a divisionalized ESCM and the ESCM is not a multidivisional control and display station. Ethernet is used for communication from the IFPD to ESCM to send component identification data without sending a control signal that operates a safety component. The signal from the IFPD only provides information data to the ESCM to support operator's manual action. The information data is only used for bringing up the control template on the ESCM display but not for performing a safety function. The ESCM cannot send a control signal to the ESF-CCS [loop controller] unless distinctive operator actions are activated. Therefore, [loop controller] does not rely upon any information data from the IFPD to accomplish its safety function. In addition, a component-level signal of the ESCM does not perform the safety function. The design of the APR1400 does not credit component-level control of equipment to perform the safety function. All safety functions are carried out at the system-level actuations. Therefore, Section 3 of DI&C-ISG-04 is not applicable.

Although the ESCM may not be used to perform a credited safety function, it appears to the staff that the component data from IFPD (non-safety control) to ESCM (safety-related) may be used to control safety-related equipment. Section 3.1.1 of DI&C-ISG-04 provides guidance on the control of safety-related equipment from a non-safety workstation. Based on the staff's understanding of the interface between ESCM and the IFPD, the staff finds that the non-safety IFPD is used to indirectly control safety-related equipment. Thus, the guidance of DI&C-ISG-04 applies. The staff issued RAI 45-7883, Question 07.09-3, to request the applicant to address the staff positions in DI&C-ISG-04, Section 3, for this interface. The applicant was also requested to clarify whether it is possible to bypass or lockout any safety functions from the non-safety IFPD via the ESCM. In the September 16, 2016, response to this RAI (ML16263A023), the applicant provided markups to the Safety I&C System TeR to include the added acknowledgement design feature on the ESCM that requires operators to confirm that the correct component has been selected for control from the IFPD. The applicant also included markups to demonstrate how the IFPD/ESCM interface conforms to the guidance of DI&C-ISG-04, Section 3 and provided a list of components that can be controlled on the ESCMs. The response states that the ESCMs do not contain the capability to bypass and lockout of safety components. Based on (1) the proposed additional design feature that requires the operator to confirm the component selection on the ESCM, (2) the demonstration of how the IFPD/ESCM conforms to the guidance of DI&C-ISG-04, Section 3, and (3) the commitment that the ESCMs do not have the capability to lockout or bypass safety components, the staff finds this design conforms to the guidance of DI&C-ISG-04, Section 3. The incorporation of the proposed markups into the next revision of the Safety I&C System TeR was a confirmatory item. The staff verified that the proposed markups have been incorporated into the Safety I&C System TeR, Revision 1. As such, this confirmatory item has been satisfied.

Subsequent to the September 16, 2016, response to RAI 45-7883, Question 07.09-3, the applicant provided another supplemental response to this RAI (ML17303A756) on November 16, 2017. This response provides additional markups to the Basic Human-System Interfaces TeR in order to ensure there is consistency between DCD Tier 2, Chapters 7 and 18. The staff finds this supplemental response is acceptable because the markups provided to the Basic Human-Systems Interfaces TeR are consistent with the markups provided in the previous response to this RAI for the Safety I&C System TeR, Revision 1. The incorporation of the proposed markups into the next revision of Basic Human-Systems Interfaces TeR was a confirmatory item. The staff verified the proposed markups have been incorporated into the Basic Human-Systems Interfaces TeR. As such, this confirmatory item has been satisified.

Because the applicant demonstrated conformance to DI&C-ISG-04 Sections 1 and 3 data communications between safety-related and non-safety systems, and identified all safety-related and non-safety interfaces and their interface type, the staff finds the APR1400 I&C system design meets the requirements of IEEE Std 603-1991, Clause 5.6.3.

Single Random Failure

For effects of a single random failure, IEEE Std 603-1991, Clause 5.6.3.3, stipulates that where a single random failure in a non-safety system can result in a DBE, and also prevent proper action of a portion of the safety-related system designed to protect against that event, the remaining portions of the safety-related system shall be capable of providing the safety function even when degraded by any separate single failure.

The staff's evaluation of the APR1400 I&C system design against the requirements of IEEE Std 603-1991, Clause 5.6.3.3, is documented in Section 7.1.4.10 of this SER.

7.9.4.6.4 Command Prioritization

DI&C-ISG-04, Section 2, "Command Prioritization," presents guidance applicable to a prioritization device or software function block, hereinafter referred to simply as a "priority module." A priority module receives device actuation commands from multiple safety and non-safety sources, and sends the command having highest priority on to the actuated device. The actuated device is a safety-related component such as a motor actuated valve, a pump motor, a solenoid operated valve, etc. The priority module must also be safety-related. The priority modules that combine the diverse actuation signals with the actuation signals generated by the digital system should not be executed in digital system software that may be subject to a CCF.

The Safety I&C System TeR, Section C.5.2.1, "Prioritization in Component Interface Module," states the following, in part.

> …the CIM only consists of discrete hardware components and does not use any software except diagnostic section of the CIM which is FPGA based. However, the diagnosis section only receives signals from the priority logic section and base section. Therefore, the diagnosis section does not adversely affect the priority logic section or base section of the CIM. The CIM is divided into three sections: priority logic section, diagnosis section and base section. The priority logic section is implemented by hardware device with no software such as TTL or CMOS. The diagnosis section is implemented by [a FPGA] device. For the base section, this section is implemented by solid switching power device. The

diagnosis section only receives signals from the priority logic section and base section, so there are no output interfaces from the FPGA to the priority logic section or base section of the CIM.

The CIM priority logic and base sections are designed, qualified, and fabricated in accordance with 10 CFR Part 50, Appendices A and B, and are qualified to the seismic Category I, environmental, and electromagnetic, and as a result, the priority module design conforms DI&C-ISG-04, Section 2, Staff Position 1.

The CIM priority logic module is independent from the ESF-CCS, DPS, and DMA switches, and hardwired to the output of the ESF-CCS, DPS, and DMA switches. The connections are prioritized based on the TTL/CMOS device. The failure of the digital system, ESF-CCS, does not adversely affect the priority function of the CIM, and as a result, the priority module design conforms to DI&C-ISG-04, Section 2, Staff Position 2.

The signals originating from the safety-related system has priority over signals from the non-safety system. The Safety I&C System TeR, Section C.5.2.1, “Prioritization in Component Interface Module,” states, in part, ”for each safety component, the priority logic in the CIM is delegated to the predefined safe state.” To address potential blocking of the priority logic performing a safety function, the priority logic gives priority to either the ESF-CCS or the DPS that demands the safety state. As a result, the priority module design conforms to DI&C-ISG-04, Section 2, Staff Position 3, since safety function can be performed.

Each CIM interfaces with a single component and has dedicated control, and as a result, the priority module design conforms to DI&C-ISG-04, Staff Section 2, Position 4.

The CIM is hardwired to ESF-CCS loop controller, DPS and DMA switches within the same division, and as a result, the priority module design conforms to DI&C-ISG-04, Section 2, Staff Position 5.

The priority logic section of the CIM is developed using a hardware-based non-digital technology (that is equivalent to implementation with relays), and as a result, DI&C-ISG-04, Section 2, Staff Positions 6 and 7 do not apply.

DI&C-ISG-04, Section 2, Staff Position 8, states, in part, “to minimize the probability of failures due to common software, the priority module design should be fully tested.” For the APR1400, the testing of the priority logic section involves all combinations of inputs with internal states. However, Section 7.8.4.2.3 of this SER has an open item, RAI 342-8291, Question 07.08-6, regarding the 100 percent testing. The staff evaluated the November 18, 2016 supplemental response to RAI 342-8291, Question 07.08-6 (ML16323A505), and found the response acceptable. The staff’s evaluation is in Section 7.8.4.2.3 of this SER. Therefore, the staff finds the applicant has demonstrated that the APR1400 priority module does not need to meet the requirements of DI&C-ISG-04, Section 2, Staff Position 8 because the priority module does not contain software within the portion that performs the priority function.

The priority logic section does not receive input from the diagnostic section, and as a result, failure of the diagnostic function does not adversely affect the priority logic safety function, and as a result, the priority module design conforms to DI&C-ISG-04, Section 2, Staff Position 9.

The priority logic section gives priority to safe state signals from either the ESF-CCS or the DPS as discussed above, and that the safety function cannot be interrupted based on the priority

logic. As a result, the priority module conforms to DI&C-ISG-04, Section 2, Staff Position 10, since the priority module ensure completion of protective action.

Based on demonstrating conformance to DI&C-ISG-04, Section 2, the staff finds the priority module meets the requirements of IEEE Std 603-1991, Clause 5.6.

7.9.4.7 Control Systems Data Communication Functions

10 CFR Part 50, Appendix A, GDC 13, requires instrumentation to be provided to monitor variables and systems over their anticipated ranges for normal operation, for AOOs, and for accident conditions as appropriate to assure adequate safety, including those variables and systems that can affect the fission process, the integrity of the reactor core, the reactor coolant pressure boundary, and the containment and its associated systems. Appropriate controls shall be provided to maintain these variables and systems within prescribed operating ranges. In addition, 10 CFR Part 50, Appendix A, GDC 19, requires a control room be provided from which actions can be taken to operate the nuclear power unit safely under normal conditions and to maintain it in a safe condition under accident conditions, including LOCAs. Furthermore, 10 CFR Part 50, Appendix A, GDC 20, requires, in part, that the protection system is designed to initiate automatically the operation of the appropriate systems, and to sense accident conditions and to initiate the operation of systems and components important to safety.

Section 4.1.2.7 of the Safety I&C System TeR states the IPS is:

> DCS-based data processing system and HSI system that serve to provide operational means for control and monitoring of the plant…the IFPD provides the operator with the HSI resource including process mimic displays, alarms, and historical data access…also, it provides the soft control templates for manual component controls…the soft control of the IFPD is used for control associated with P-CCS controllers directly attached to the non-safety DCS platform network. The [non-safety] IFPD also interfaces to the [safety related] ESCM to send safety component selection information through Ethernet network.

The DCD Tier 2 Section 7.1.1.5 states the “IPS displays all [accident monitoring instrumentation] AMI variables.” The non-safety DCS platform network is called Data Communication Network – Information. DCD Tier 2 Section 7.9.1.3 states, in part:

> an evaluation is performed to demonstrate that the throughput, capacity, response time, and data accuracy of DCN-I network meet the requirements of the supported I&C systems. Expected error rates and their effects on system safety, reliability, and performance are also evaluated.

DCD Tier 2 Section 7.9.1.4 states, in part:

> an evaluation is performed to demonstrate that the throughput, capacity, latency, and data accuracy of the QIAS-N network meet the requirements of the QIAS-N. Expected error rates and their effects on system safety, reliability, and performance are also evaluated. The error rates include errors in device addressing and signal data attributes.

The staff concludes that the proposed design criteria and performance characteristics for sufficient capacity and bandwidth for the DCN-I and QIAS-N networks in order to reliably

operate plant process systems are sufficient and adequate to meet the requirements of GDC 13 and 19.

7.9.5 Combined License Information Items

No applicable items were identified in the FSAR. No additional COL information items need to be included in DCD Tier 2 Table 1.8-2, "APR1400 Combined License Information Items," for data communication systems.

7.9.6 Findings and Conclusions

The staff reviewed DCD Tier 2 Section 7.9 and the associated technical and topical reports for conformance to the regulatory requirements of 10 CFR Parts 50 and 52 as related to data communications systems. The evaluation of the data communications design to the requirements of 10 CFR Part 50, Appendix B and GDC 1 is in Section 7.1.4.7 of this SER.

Based on the resolution of the open items associated with RAI 45-7883, Question 07.09-2; RAI 45-7883, Question 07.09-7; RAI 348-8279, Question 07.09-16; RAI 348-8279, Question 07.09-18, and RAI 43-7887, Question 07.01-25, regarding conformance to communications independence guidance of DI&C-ISG-04 and the staff's overall evaluation regarding conformance to DI&C-ISG-04 above, the staff has determined the design of the data communications system meets the relevant requirements of 10 CFR 50.55a(h)(3) and GDC 24.

The evaluation of the data communications system against the requirements of 10 CFR Part 50, Appendix A, GDC 22 is in Section 7.8 of this SER.

The data communications system conforms to the guidelines for periodic testing in RG 1.22, Revision 0, and RG 1.118, Revision 3. The BISI conforms to the guidelines of RG 1.47, Revision 1. The data communications system conforms to the guidelines on the application for the single failure criterion in RG 1.53, Revision 2. Based on the review, the staff concludes that the data communications system satisfies the requirement of IEEE Std 603-1991 with regard to the system reliability and testability. Therefore, the staff finds that the data communications system satisfies these requirements of GDC 21.

Based on the resolution of the open item associated with RAI 348-8279, Question 07.09-16, and the provision of information that demonstrate how communication failures are addressed by the design in accordance with DI&C-ISG-04, the staff concludes the data communications system failure modes were adequately identified, and thereby determined the data communications system satisfies the requirements of GDC 23.

Based on the applicant's commitment to have design criteria and performance characteristics for sufficient capacity and bandwidth for the DCN-I and QIAS-N networks in order to reliably operate plant process systems, the staff concludes the data communications system design meets the requirements of GDC 13 and 19.