7. INSTRUMENTATION AND CONTROLS

7.0 Instrumentation and Controls - Introduction

This chapter of the safety evaluation report (SER) provides the U.S. Nuclear Regulatory Commission (NRC) staff's review of the instrumentation and control (I&C) portion of the General Electric Hitachi Nuclear America, LLC (GEH), economic simplified boiling-water reactor (ESBWR) application as part of the design certification review conducted by the NRC staff under Part 52, "Licenses, Certifications, and Approvals for Nuclear Power Plants," of Title 10 of the *Code of Federal Regulations* (10 CFR Part 52). This review is conducted in accordance with NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants," (hereafter referred to as the SRP) Chapter 7, "Instrumentation and Controls" Revision 5. Consistent with SRP Chapter 7, the review used Section 50.55a(h) of 10 CFR Part 50, "Domestic Licensing of Production and Utilization Facilities", which requires that applications for design certification filed on or after May 13, 1999, meet the requirements for safety systems in IEEE Standard (Std) 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations", and the correction sheet dated January 30, 1995. Guidance on applying the safety system criteria to computer-based systems is provided in IEEE Std 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations", as endorsed by Regulatory Guide (RG) 1.152, Revision 2, "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants," issued January 2006.

7.0.1 Method of Review

Consistent with SECY-92-053, "Use of Design Acceptance Criteria (DAC) During 10 CFR Part 52 Design Certification Reviews," dated February 19, 1992, Tier 2 of the ESBWR Design Control Document (DCD), provides limited design details for I&C systems. Accordingly, ESBWR DCD Tier 1, provides associated DAC, (a type of inspections, tests, analyses, and acceptance criteria (ITAAC) marked with {{Design Acceptance Criteria}} labels), that a combined license (COL) applicant or licensee would follow to complete the design detail.

The DAC are a set of prescribed limits, parameters, procedures, and attributes upon which the NRC relies, in a limited number of technical areas (digital I&C, human factors engineering, and piping), in making a final safety determination to support a design certification. The acceptance criteria for the DAC should be measurable, testable, or subject to analysis using preapproved methods, and should be verified as part of the ITAAC used to demonstrate that the as-built facility conforms to the certified design. Thus, the acceptance criteria for DAC are specified, together with the related ITAAC, in Tier 1, and both are part of the design certification. The DAC and the ITAAC, when met, ensure that the completed design and as-built plant conform to the design certification.

The safety basis of I&C systems in the ESBWR design can be divided into hardware and software aspects.

The hardware aspects are as follows:

- The applicant committed to comply with IEEE Std 603 and other applicable requirements.

- The applicant identified high level functional requirements.

- The applicant provided DAC to verify and confirm that the completed design meets IEEE Std 603 requirements.

The software aspects are as follows:

- The applicant identified and committed to a program to implement a software development process.

- The applicant provided DAC to verify and confirm the following:

  - Acceptable plans were prepared to control software development activities.
  - The plans were followed in an acceptable software life cycle.
  - The process produced acceptable design outputs.

The software and hardware design process is discussed below.

When a DCD includes DAC instead of providing design detail, the DCD should include the associated design processes that the COL applicant will use to complete the design. For software, the design includes a software design process described in NEDO-33226 (NEDE-33226P), "ESBWR I&C Software Management Program Manual" (SMPM), and NEDO-33245 (NEDE-33245P), "ESBWR I&C Software Quality Assurance Program Manual" (SQAPM). For hardware, the design process consists of commitments that the safety I&C systems are designed to follow IEEE Std 603 as documented in DCD, Tier 1, Section 2.2.15, and that the safety I&C systems are qualified to meet the requirements documented in DCD Tier 2, Sections 3.10 and 3.11 and DCD, Tier 1, Section 3.8.

Sections 7.1 through 7.8 of this report document the NRC staff's evaluation of the I&C design. The evaluation includes a verification of aspects of the design against the criteria in the respective SRP sections. The evaluation also includes verification that I&C system functions are compatible with the applicant's accident analyses. This involved NRC staff verification that the system events described in DCD, Tier 2, Chapter 15, are consistent with the initiating actions described in Chapter 7. In the necessary sections of this report, the evaluation will refer to IEEE Std 603, Section 5.5, as required by 10 CFR 50.55a(h)(3). This criterion requires that the safety system accomplish its safety functions under the full range of applicable conditions enumerated in the design basis. As explained below, the NRC staff finds that I&C system functions are consistent with the events described in the accident analyses.

7.0.2 Documents for Instrumentation and Control Review

The staff's evaluation is for Tier 1 and Tier 2 of the ESBWR Design Control Document (DCD), Revision 8.

- DCD, Tier 2, Chapter 7, "Instrumentation and Controls," contains the description of the DCD pertaining to the primary I&C systems of the design.

- DCD, Tier 2, Section 7.1, "Introduction," describes the I&C system architecture-a distributed control and information system (DCIS). Section 7.1 also discusses the conformance with regulatory requirements, industry codes, and standards.

- DCD, Tier 2, Section 7.2, “Reactor Trip System (RTS),” discusses the I&C aspects of the reactor trip function.

- DCD, Tier 2, Section 7.3, “Engineered Safety Features (ESF) Systems,” addresses the I&C aspects of the ESF actuation.

- DCD, Tier 2, Section 7.4, “Safety-Related Safe-Shutdown and Non-Safety-Related Cold Shutdown Systems,” discusses the systems in the design that are required for safe shutdown.

- DCD, Tier 2, Section 7.5, “Safety-Related and Non-Safety-Related Information Systems,” discusses post accident monitoring (PAM), containment monitoring, and radiation monitoring systems.

- DCD, Tier 2, Section 7.6, “Interlock Logic,” discusses interlocks important to safety.

- DCD, Tier 2, Section 7.7, “Control Systems,” describes control systems in the design.

- DCD, Tier 2, Section 7.8, “Diverse Instrumentation and Control Systems,” addresses the Anticipated Transient without Scram (ATWS) mitigation function and common cause failures (CCFs) defense within safety system designs.

- DCD, Tier 2 data communications for the design are addressed in Sections 7.1, 7.2, and 7.3.

- The software quality program for software design and development is discussed in NEDE-33226P and NEDE-33245P.

In DCD Tier 1, the following sections address the I&C-related design commitments including the DAC/ITAAC:

- DCD, Tier 1, Section 2.2, “Instrumentation and Control Systems” (includes Sections 2.2.1 through 2.2.16)

- DCD, Tier 1, Section 3.2, “Software Development”

- DCD, Tier 1, Section 3.3, “Human Factors Engineering”

- DCD, Tier 1, Section 3.7, “Post Accident Monitoring Instrumentation”

- DCD, Tier 1, Section 3.8, “Environmental and Seismic Qualification of Mechanical and Electrical Equipment”

The applicant also submitted the following LTRs to support the design certification review:

- NEDO-33251, “ESBWR I&C Defense-in-Depth and Diversity Report”

- NEDO-33304 (NEDE-33304P), “GEH Advanced Boiling-Water Reactor (ABWR)/ESBWR Setpoint Methodology”

- NEDO-33295 (NEDE-33295P), “ESBWR Cyber Security Program Plan”

7.1 Introduction

This section documents the NRC staff’s general evaluation of the DCIS (Section 7.1.1). It also documents the NRC staff’s evaluation of nonsystem-based topics, including (1) software development activities (Section 7.1.2), (2) assessment of diversity and defense-in-depth (D3) (Section 7.1.3), (3) setpoint methodology (Section 7.1.4), (4) data communication systems (Section 7.1.5), and (5) secure development and operational environment (SDOE) (Section 7.1.6). The specific SRP section and the associated review criterion used for each review are identified in each section.

7.1.1 General Distributed Control and Information System Description

The I&C system uses the distributed digital system to perform plant-protection and safety monitoring functions, as well as control functions. The NRC staff reviewed the DCIS in accordance with SRP Section 7.1. The NRC staff used acceptance criterion in SRP Table 7-1 and SRP Appendix 7.1-A to verify compliance with the applicable regulations, as directed by SRP Section 7.1. The NRC staff also used SRP Appendix 7.1-C and SRP Appendix 7.1-D to verify that DCD Tier 2 addressed all the criteria listed in IEEE Std 603, as required by 10 CFR 50.55a(h)(3).

As identified in SRP Table 7-1 and in Sections 7.1 to 7.8 of this report, not all regulations and acceptance criteria listed below are applicable to each I&C system important to safety. However, Section 7.1.1 of this report lists and evaluates each regulation and acceptance criteria applicable to the DCIS. Sections 7.2 to 7.8 of this report focus on those acceptance criteria that the corresponding SRP section indicates should be emphasized. Sections 7.2 to 7.8 of this report may also address system-specific criteria.

7.1.1.1 Regulatory Criteria

SRP Table 7-1, Section 1, identifies the following regulations as being applicable to I&C systems important to safety:

- 10 CFR 50.55a(a)(1) - Quality Standards for Systems Important to Safety
- 10 CFR 50.55a(h)(3) - Safety Systems (IEEE Std 603)
- 10 CFR 50.34(f)(2)(v) - Bypass and Inoperable Status Indication
- 10 CFR 50.34(f)(2)(xi) - Direct Indication of Relief and Safety Valve Position
- 10 CFR 50.34(f)(2)(xiv) - Containment Isolation System
- 10 CFR 50.34(f)(2)(xvii) - Accident Monitoring Instrumentation
- 10 CFR 50.34(f)(2)(xviii) - Instrumentation for the Detection of Inadequate Core Cooling
- 10 CFR 50.34(f)(2)(xix) - Instruments for Monitoring Plant Conditions following Core Damage

- 10 CFR 50.34(f)(2)(xxiv) - Central Reactor Vessel Water Level Recording

- 10 CFR 50.62 - Requirements for Reduction of Risk from ATWS

- 10 CFR 52.47(b)(1) - ITAAC for Standard Design Certification

SRP Table 7-1, Section 2, identifies the following 10 CFR Part 50, Appendix A, "General Design Criteria (GDC) for Nuclear Power Plants," as being applicable to I&C systems important to safety:

- GDC 1, "Quality Standards and Records"
- GDC 2, "Design Bases for Protection Against Natural Phenomena"
- GDC 4, "Environmental and Dynamic Effects Design Bases"
- GDC 10, "Reactor Design"
- GDC 13, "Instrumentation and Control"
- GDC 15, "Reactor Coolant System Design"
- GDC 16, "Containment Design"
- GDC 19, "Control Room"
- GDC 20, "Protection System Functions"
- GDC 21, "Protection System Reliability and Testability"
- GDC 22, "Protection System Independence"
- GDC 23, "Protection System Failure Modes"
- GDC 24, "Separation of Protection and Control Systems"
- GDC 25, "Protection System Requirements for Reactivity Control Malfunctions"
- GDC 28, "Reactivity Limits"
- GDC 29, "Protection Against Anticipated Operational Occurrences (AOOs)"
- GDC 33, "Reactor Coolant Makeup"
- GDC 34, "Residual Heat Removal"
- GDC 35, "Emergency Core Cooling"
- GDC 38, "Containment Heat Removal"
- GDC 41, "Containment Atmosphere Cleanup"
- GDC 44, "Cooling Water"

SRP Table 7-1, Section 3, identifies the NRC staff requirements memorandum (SRM) on SECY-93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Design," dated April 2, 1993, (1) Item II.Q, "Defense Against Common-Mode Failure in Digital Instrumentation and Control Systems," and (2) Item II.T, "Control Room Annunciator (Alarm) Reliability," as being applicable to I&C systems important to safety.

SRP Table 7-1, Section 4, discusses RGs that provide acceptable methods for implementing the regulatory requirements for hardware and software features of digital systems important to safety. The RGs identified as being applicable to I&C systems important to safety are the following:

- RG 1.22, "Periodic Testing of Protection System Actuation Functions," issued February 1972

- RG 1.47, “Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems,” issued February 2010
- RG 1.53, “Application of the Single-Failure Criterion to Safety Systems,” issued November 2003
- RG 1.62, “Manual Initiation of Protective Actions,” issued June 2010
- RG 1.75, Revision 3, “Criteria for Independence of Electrical Safety Systems,” issued February 2005
- RG 1.97, Revision 4, “Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants,” issued June 2006
- RG 1.105, Revision 3, “Setpoints for Safety-Related Instrumentation,” issued December 1999
- RG 1.118, Revision 3, “Periodic Testing of Electric Power and Protection Systems,” issued April 1995
- RG 1.151, Revision 1, “Instrument Sensing Lines,” issued July 2010
- RG 1.152, Revision 2, “Criteria for Digital Computers in Safety Systems of Nuclear Power Plants,” U.S. Nuclear Regulatory Commission, January 2006.
- RG 1.168, Revision 1, “Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants,” issued February 2004
- RG 1.169, “Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants,” issued September 1997
- RG 1.170, “Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants,” issued September 1997
- RG 1.171, “Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants,” issued September 1997
- RG 1.172, “Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants,” issued September 1997
- RG 1.173, “Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants,” issued September 1997
- RG 1.180, Revision 1, “Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems,” issued October 2003

- RG 1.189, Revision 2, “Fire Protection for Nuclear Power Plants,” issued October 2009

- RG 1.204, “Guidelines for Lightning Protection of Nuclear Power Plants,” issued November 2005

In addition to the RGs identified in SRP Table 7-1, Section 4, the following RG provides acceptable methods for implementing the regulatory requirements for hardware and software features of digital systems important to safety.

- RG 1.209, “Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants,” issued March 2007

The following industry standards/documents are generally applicable to I&C systems that are important to safety but have not been incorporated into SRP Table 7-1:

- Electric Power Research Institute (EPRI) TR-107330, “Generic Requirements Specification for Qualifying a Commercially Available PLC [Programmable Logic Controller] for Safety-Related Applications in Nuclear Power Plants,” approved by the NRC on July 30, 1998

- EPRI TR-102323-R1, “Guidelines for Electromagnetic Interference Testing in Power Plants,” approved by the NRC on April 17, 1996

- EPRI TR-106439, “Guideline on Evaluation and Acceptance of Commercial - Grade Digital Equipment for Nuclear Safety Applications,” approved by the NRC in April 1997

SRP Table 7-1, Section 5, identifies the applicability of SRP Branch Technical Positions (BTPs). DCD, Tier 1 Table 7.1-1, I&C Regulatory Requirements Applicability Matrix, listed that the design is in conformance with SRP Revision 4, BTP JOCB-1 to -21. The staff has compared the technical requirements between SRP Revision 4, BTP HICB-1 to -21 and SRP Revision 5, BTP 7-1 to BTP 7-21. The staff finds that conformance with BTP HICB-1 to -21 is equivalent to conformance with BTP 7-1 to BTP 7-21 in Revision 5 of SRP Table 7-1.

7.1.1.2 Summary of Technical Information

7.1.1.2.1 Instrumentation and Control Systems Overview

The I&C system for the design is a DCIS. It is subdivided into the safety DCIS (Q-DCIS) and the non-safety DCIS (N-DCIS). The Q-DCIS includes the reactor protection system (RPS), the neutron monitoring system (NMS), the independent control platform (ICP), and the safety system logic and control for the engineered safety features actuation system (SSLC/ESF). The N-DCIS includes the diverse protection system (DPS), the balance of plant (BOP), the plant investment protection (PIP) systems, the plant computer and workstations, and the severe accident mitigation system (Deluge system). The safety category, the system architecture, and the subsystems in that family are summarized in Tables 7-1 and 7-2 below.

Table 7-1 Q-DCIS Overview

System Families	Divisions	Subsystems	Platform

(RTIF-NMS)
 	
Reactor Trip & Isolation Function - Neutron Monitoring System
	4 Independent Divisions	• RPS
		• (LD&IS) - Leak Detection and Isolation System
		  ○ Main Steam Isolation Valve (MSIV) Logic
		• NMS
		  ○ (SRNM) - Startup Range Monitoring System
		  ○ (PRNM) - Power Range Monitoring System
		• (CMS) - Containment Monitoring System
		  ○ (SPTM) - Suppression Pool Temperature Monitoring Function
			RTIF-NMS Platform

SSLC/ESF	4 Independent Divisions	<u>(ECCS)</u> - <u>Emergency Core Cooling System</u>
		• (ADS) - Automatic Depressurization System
		  ○ Safety Relief Valves (SRVs), Depressurization Valves (DPVs)
		• (GDCS) - Gravity-Driven Cooling System
		• (ICS) - Isolation Condenser System
		• (SLC) - Standby Liquid Control System
		
		<u>Non-ECCS</u>
		• LD&IS
		  ○ Non-MSIV Logic
		• (CRHS) - Control Room Habitability System
			SSLC/ESF Platform

Independent Logic Controllers	4 Independent Divisions	• ATWS Mitigation by SLC System • (VBIF) - Vacuum Breaker Isolation Function • High Pressure Control Rod Drive (HP CRD) Isolation Bypass Function (IBF) • ICS DPV Isolation Function	Independent Control Platforms
Safety-Related Information Systems	As required per RG 1.97	• PAM Instrumentation • CMS • (PRMS) - Process Radiation Monitoring System	Independent Platform

Table 7-2 N-DCIS Overview

System Families	Redundancy	Subsystems	Platform
DPS	Triple Redundant	• Diverse RPS Logic • Diverse ECCS Logic • Diverse Containment Isolation • ATWS Mitigation Logic	Diverse DCIS Platform

Control Systems	Triple or Dual Redundant	• (NBS) - Nuclear Boiler System
		• (RC&IS) - Rod Control and Information System
		• (FWCS) - Feedwater Control System
		• (PAS) - Plant Automation System
		• (TGCS) - Turbine Generator Control System
		• (SB&PC) - Steam Bypass and Pressure Control System
		• NMS
		  o (AFIP) - Automatic Fixed In-Core Probe
		  o (MRBM) - Multichannel Rod Block Monitor
		• (CIS) - Containment Inerting System	

BOP DCIS Systems	Dual Redundant	BOP for Power Generator PIP-A & PIP-B	
Plant Computer	Multiple Stations	• (SPDS) - Safety Parameter Display System • (MCRP) - Main Control Room Panel System • (AMS) - Alarm Management System • (OLPs) - Online Procedures • Technical Specification (TS) Monitoring • (3D-Monicore) - three-dimensional Monicore	Independent Platform
Non-Safety Information Systems	As required per RG 1.97	• PRMS • (ARMS) - Area Radiation Monitoring System • CMS	Independent Platform
Severe Accident Mitigation	Multiple PLCs	• Deluge System (a GDCS Subsystem)	PLC

7.1.1.2.2 Q-DCIS Overview

The Q-DCIS performs the safety control and monitoring functions. The Q-DCIS is organized into four physically and electrically isolated divisions. Each division is segmented into systems; segmentation allows, but does not require, the systems to operate independently of each other. The Q-DCIS major cabinets, systems, and functions are listed below.

The RTIF cabinets include the following:

- RPS
- MSIV functions of the LD&IS
- ATWS/SLC functions
- VB isolation function
- HP CRD isolation bypass function
- SPTM functions for RPS and CMS

The NMS includes the following:

- SRNM functions
- PRNM functions that include:
  - local power range monitor (LPRM) functions
  - average power range monitor (APRM) functions
  - oscillation power range monitor (OPRM) functions

The SSLC/ESF system includes the following:

- ECCS functions that include:
  - ADS functions
  - GDCS functions
  - ICS functions
  - SLC system ECCS functions
- LD&IS functions (except the MSIV functions)
- CRHS functions
- Safety information systems

The Q-DCIS major components include the following:

- fiber optic cable and hardwired network
- system control processors
- non microprocessor-based logic
- remote multiplexer units (RMUs)
- load drivers (discrete outputs)
- communication interface modules (CIMs)
- video display units (VDUs)
- main control room (MCR) wide-display/consoles that house the controls and monitoring
- hard controls/indicators (for monitoring)
- cabinets for housing devices such as power supplies

The RPS is the overall complex of instrument channels, trip logics, trip actuators, manual controls, and scram logic circuitry that initiate rapid insertion of control rods to shut down the reactor for situations that could result in unsafe operations. This action prevents or limits fuel damage, limits system pressure excursions, and thus minimizes the release of radioactive material. The RPS also establishes appropriate logic for different reactor operating modes, provides monitoring and control signals to other systems, and actuates alarms. The RPS hardware and logic are diverse from the SSLC/ESF logic, the ATWS mitigation logic, and the DPS logic. The RPS cabinet also houses the equipment that performs the SPTM functions for the CMS.

The NMS monitors neutron flux in the reactor core from the startup source range to beyond rated power. The NMS provides logic signals to the RPS to automatically shut down the reactor when a condition requires a reactor scram. The system provides an indication of neutron flux, which can be correlated with the thermal power level for the entire range of flux conditions that can exist in the core. The NMS comprises the following systems:

- The SRNM system monitors neutron flux levels from a very low-range power level to a power level above 15 percent of rated power. The SRNM system generates trip signals to prevent fuel damage resulting from abnormal positive reactivity insertion. The SRNM system generates both a high neutron flux trip and a high rate of neutron flux increase trip.

- The PRNM system includes the LPRM, APRM, and OPRM functions. The LPRM system provides the average power level of the reactor core and the OPRM system provides monitoring of neutron flux and core thermal hydraulic instabilities. In the low end of the power range (1 percent to 15 percent), the SPRM and PRNM monitoring overlap.

- The AFIP is a non-safety component of the NMS and does not provide information to the Q-DCIS. Its function is to calibrate the LPRMs by providing flux information to the 3D-MONICORE system.

- The MRBM is a non-safety component of the NMS and is completely isolated from the Q-DCIS by one-way optical fiber communications. Its function is to provide control rod blocks to the RC&IS to prevent violations of core thermal limits.

The SSLC/ESF system is the ESF actuation system for the design. SSLC/ESF is the overall complex of instrument channels, trip logic, trip actuators, manual controls, and actuation logic circuitry that initiate protective actions to mitigate the consequences of design-basis events (DBEs). Input signals from redundant channels of safety instrumentation are used to make trip decisions to initiate the following accident mitigating functions:

- ECCS operation
- leak detection, containment isolation, and radioactivity release barrier defense actuation
- MCR habitability functions

The ECCS provides emergency core cooling to respond to events that threaten the reactor coolant inventory. The ECCS comprises the ADS, the GDCS, the ICS, and the SLC system. The ADS resides within the NBS and comprises the SRVs, DPVs, and associated I&C. The ADS depressurizes the reactor to allow the low-head GDCS to provide makeup coolant to the

reactor. The ADS logic resides in the SSLC/ESF portion of the Q-DCIS. The GDCS provides emergency core cooling once the reactor has been depressurized. The GDCS is capable of injecting large volumes of water into the reactor pressure vessel (RPV) to keep the core covered for at least 72 hours following a loss-of-coolant accident (LOCA). The GDCS also performs a deluge function that drains the GDCS pools to the lower drywell in the event of a severe accident core-melt sequence. The GDCS deluge logic is separate and diverse from the Q-DCIS.

The ICS is designed to limit reactor pressure and prevent SRV operation following an isolation of the main steamlines. The ICS, together with the water stored in the RPV, provides sufficient reactor coolant volume to avoid automatic depressurization caused by a low reactor water level. The ICS is a safety system that removes reactor decay heat following reactor shutdown and isolation. The ICS logic resides on the SSLC/ESF portion of the Q-DCIS.

The SLC system performs dual functions. It provides additional coolant inventory to respond to a LOCA and it is a backup method to bring the nuclear reactor to subcriticality and to maintain subcriticality as the reactor cools. The SLC logic resides on the SSLC/ESF and the ATWS/SLC portions of the Q-DCIS.

The LD&IS monitors leakage sources from the reactor coolant pressure boundary (RCPB) and automatically initiates closure of the appropriate valves that isolate the source of the leak. This action limits a coolant release from the RCPB and the release of radioactive materials to the environment. The LD&IS logic for the MSIVs resides on the RPS portions of the Q-DCIS and the non-MSIV isolation valve logic resides on the SSLC/ESF. The MSIV isolation logic of the LD&IS is performed as part of the RPS logic platform. The non-MSIV isolation logic of the LD&IS is performed as part of the SSLC/ESF logic platform.

The CRHS provides a safe environment for the operators to control the nuclear reactor and its auxiliary systems during normal and abnormal conditions. The CRHS monitors the inlet ventilation air in the MCR habitability area and actuates logic to isolate and filter the CRHA on detection of hazardous environmental conditions. The CRHS logic resides on the SSLC/ESF portion of the Q-DCIS.

The ATWS/SLC system provides a diverse means of reducing power excursions from certain transients and a diverse means of emergency shutdown. The ATWS mitigation logic, which uses the soluble boron injection capability of the SLC system as a diverse means of negative reactivity insertion, is implemented as safety logic. The ATWS/SLC logic also provides a feedwater runback (FWRB) signal to attenuate power excursions. The SLC may be initiated manually or automatically using the ATWS mitigation logic or the SSLC/ESF logic as an ECCS function. The SLC logic resides on the SSLC/ESF and ATWS/SLC RPS portions of the Q-DCIS. The non-safety ATWS mitigation logic is implemented in the DPS.

The containment system wetwell-to-drywell VBIF prevents the loss of long-term containment integrity upon detection of excessive vacuum breaker leakage. The VBIF is implemented by independent logic controllers.

The HP CRD isolation bypass function automatically bypasses the HP CRD injection isolation (intended to prevent the over-pressurization of the containment and therefore loss of long-term containment integrity) to compensate for a failure of the GDCS to inject. The HP CRD isolation bypass function is implemented using the ICP, which is diverse from the RTIF-NMS platform and the SSLC/ESF platform and not susceptible to CCF.

The passive containment cooling system (PCCS) functions to cool the containment following a rise in containment pressure and temperature without requiring any component actuation. The PCCS needs no electric power and does not have instrumentation, control logic, or power-actuated valves.

The SPTM system is part of the CMS. The system operates continuously during reactor operation. Should the suppression pool temperature exceed established limits, the system provides input both for a reactor scram and for automatic initiation of the suppression pool cooling mode of the fuel auxiliary pool cooling system operation.

Other CMS functions, some of which are non-safety, include the monitoring of key containment fluid levels, radiation levels, pressures, concentrations, and dew point values. These parameters are monitored during both normal reactor operations and post accident conditions to evaluate the integrity and safe conditions of the containment. Abnormal measurements and indications initiate alarms in the MCR.

7.1.1.2.3 N-DCIS Overview

The N-DCIS components are redundant when they are needed to support power generation and are segmented into systems. The segmentation allows the systems to operate independently of each other. The N-DCIS cannot control any Q-DCIS component. The N-DCIS accepts one-way communication from the Q-DCIS so that the safety information can be monitored, archived, and alarmed seamlessly with the N-DCIS data.

The N-DCIS major systems and functions are described below.

The GENE systems include the following:

- Workstations
  - 3D MONICORE
  - SPDS

- Dual-Redundant Controllers
  - RC&IS (includes rod server processing channel (RSPC), rod action and position information (RAPI), file control module (FCM), Signal interface unit (SIU)),
  - ATLM, and
  - Rod worth minimizer (RWM)

- Triple-Redundant Controllers
  - DPS
  - SB&PC
  - FWCS
  - Feedwater temperature control system
  - TGCS

The PIP (Train A and Train B) includes the following:

- Control rod drive (CRD) system,
- Reactor water cleanup and shutdown cooling (RWCU/SDC) system,

- Fuel and auxiliary pool cooling system (FAPCS),
- Non-safety RSS,
- Reactor component cooling water system (RCCWS),
- Plant service water system (PSWS),
- PSWS cooling towers,
- Nuclear island chilled water system (NICWS),
- Drywell cooling non-safety electrical systems,
- Instrument air system (IAS),
- Non-safety PAM systems,
- Non-safety LD&IS systems,
- PCCS ventilation fans,
- Ancillary and standby diesel generators,
- 6.9-kilovolt (kV) plant electrical power system,
- Low voltage electrical system,
- Non-safety uninterruptible power supplies (UPS)

The BOP systems include the following:

- SB&PC
- FWCS
- Feedwater temperature control system
- TGCS
- Turbine auxiliary;
- Generator auxiliary controller;
- Electrical system main transformer/unit auxiliary transformer (UAT) controller;
- Main condenser controller;
- Electrical system reserve auxiliary transformer (RAT) controller;
- Normal heat sink controller;
- Condensate/feedwater/drains/extraction controller,
- including extraction and level control;
- Water systems controller;
- Service air/containment inerting/floor drains controller; and
- Miscellaneous HVAC controller.

The plant computer systems group includes the following:

- Performance monitoring and control (PMC) functions, prediction calculations, visual display control, point log and alarm processing, surveillance test support, and automation;

- Core thermal power/flow calculations;

- The plant AMS that alerts the operator to process deviations and equipment/instrument malfunctions;

- Fire Protection System (FPS) data through datalinks and gateways;

- The Historian function, that stores data for later analysis and trending;

- Control of the main mimic on the MCR wide display panel (WDP);

- Support functions for printers and the secure data communications to the technical support center (TSC), emergency operation facility (EOF), emergency response data system (ERDS), and potential links to the Simulator;

- Online procedures (OLP) to guide the operator during normal and abnormal operations, and to verify and record compliance;

- Transient recording;

- Non-safety PAM displays;

- Report generators to allow the operator, technician, or engineer to create historical or real time reports for performance analysis and maintenance activities;

- The plant configuration database (PCD) to document, manage, and configure components of the N-DCIS;

- Gateways to vendor-supplied non-safety systems such as seismic, meteorological, and radiation monitoring; and

- Non-safety process and area radiation monitoring

Plant computer functions (PCF) information display and control capability are provided by non-safety VDUs in the MCR and RSS panels.

The N-DCIS includes the following non segment-based equipment:

- Non-safety VDUs/MCRP
- Gateway
- Datalinks
- SPDS logic

The N-DCIS performs control functions with logic processing modules using signals acquired by the RMUs. The N-DCIS logic is implemented in triple-redundant control systems for core non-safety key systems such as the FWCS and the PAS, but it is always at least redundant for systems required for power generation, such that no single failure of an active DCIS component can cause or prevent a BOP trip or reactor scram.

The N-DCIS provides the control and monitoring operator interface on non-safety VDUs in the MCR and RSS panel. The VDUs operate independently of one another, yet each can normally access any component in the N-DCIS. This gives the RSS panels the same control and monitoring capability as the displays in the MCR. The N-DCIS components that are key for power generation are provided with two or three uninterruptible power sources with battery backup for at least 2 hours. For loss-of-offsite-power events or after battery backup power is lost, the N-DCIS can operate from either of the two diesel generators. The N-DCIS provides self-diagnostics that monitor communications, power, and other failures to the replacement card, module, or chassis level. Process diagnostics include system alarms (in the MCR) and the ability to identify sensor failures.

The non-safety DPS is designed to mitigate the possibility of digital protection system CCF discussed in Item II.Q of SECY-93-087. The DPS is a triple-redundant system, powered by redundant non-safety load group power sources. The DPS provides diverse reactor protection using a subset of the RPS scram signals. The DPS also provides diverse emergency core cooling by independently actuating the ECCS and selected containment isolation functions. The DPS processes the non-safety portions of the ATWS mitigation logic.

The RC&IS provides for normal monitoring of control rod positions and executing normal control rod movement commands. The RC&IS uses a dual-redundant architecture of two independent channels. The failure or malfunction of RC&IS has no impact on the hydraulic scram function of the CRD. The circuitry for normal insertion and withdrawal of control rods in RC&IS is completely independent of the RPS circuitry controlling the scram valves.

The FWCS is a power generation system for the purpose of maintaining proper vessel water. The FWCS uses a triple-redundant, fault-tolerant digital controller (FTDC). The FTDC consists of three parallel processing channels, each containing the hardware and software for execution of the control algorithms. The FWCS is not safety and is not required for safe shutdown of the plant. The FWCS initiates a runback of feedwater demand upon receipt of an ATWS trip signal from ATWS/SLC logic.

The PAS provides reactivity control, heatup and pressurization control, reactor power control, generator power control, and plant shutdown control. The PAS consists of triple-redundant process controllers. The PAS accomplishes different phases of reactor operations, which include approach to criticality, heatup, reactor power increase, automatic load following, reactor power decrease, and shutdown. The PAS interfaces with the operator's console to perform its designed functions. In the automatic mode, the PAS issues command signals to the turbine master controller, which contains appropriate algorithms for automated sequences of turbine and related auxiliary systems. The PAS does not perform or ensure any safety function.

The SB&PC system controls reactor pressure during plant startup, power generation, and shutdown modes of operation. This is accomplished through control of the turbine control valves (TCVs) and turbine bypass valves, (TBVs) such that susceptibility to reactor trip, turbine generator trip, main steam isolation, and SRV valve operation is minimized. The SB&PC system uses a triple-redundant microprocessor-based FTDC controller. With triple redundancy, the loss of one and/or two complete processing channels will not affect the system function.

The TGCS controls the turbine speed, load, and flow for startup and normal operations. The TGCS is a triple-redundant process control system. Only the operator can switch the turbine generator controller to Automatic (remote). The operator or the automatic power regulator can switch the turbine generator controller to Manual (local). The TGCS interfaces with the SB&PC system.

3D MONICORE provides core performance information and has two major components, the monitor and the predictor. Both components use a three-dimensional core model as the main calculation engine. 3D MONICORE is designed to periodically track current reactor parameters automatically with live plant data. This allows the user to study the effects of different rod patterns, core flows, and fuel burnups before performing reactor maneuvers to support plant operation.

In the event of a core-melt accident in which molten fuel reaches the lower drywell, the flow through the deluge line is required to flood the lower drywell region with a required deluge network flow rate assumed in the accident analyses. Deluge line flow is initiated by thermocouples, which sense high lower drywell region basement temperatures indicative of molten fuel on the lower drywell floor. Logic circuits actuate squib-type valves in the deluge lines upon detection of a basement temperature exceeding the setpoint value, provided that another set of dedicated thermocouples also senses the drywell temperature to be higher than a preset value. The deluge logic is completely separate from and independent of the Q-DCIS and the N-DCIS and is powered by dedicated batteries supported by battery chargers operating on non-safety power. Under a loss of power condition, including station blackout (SBO), the deluge system batteries provide power for 72 hours.

7.1.1.2.4 DCIS Design Features

The Q-DCIS is organized into four physically and electrically separate divisions. The Q-DCIS design basis is IEEE Std 603.

As discussed in probabilistic fire analysis, the Q-DCIS cabinet areas contain the control and information cabinets of the four safety divisions in the control building. Each of the four safety divisions is located in a separated fire area. These areas contain the equipment needed for the actuation of safety systems. A fire in a single fire area can only affect one safety system division.

There is no electrical system protection equipment (circuit breaker) in the MCR. The MCR fire will not actuate any DCIS controls, other than trip the main generator. The MCR fire does not result in the loss of offsite power or the loss of the diesels.

The Q-DCIS is designed in a way that no single failure (including a single fire event) can spuriously actuate the containment isolation valves or inadvertently actuate an ADS SRV or DPV. Typically, two load drivers are actuated simultaneously to actuate the component. Each of the trains (per division) of ADS start signals is sent to the load drivers/discrete output for the ADS SRV and DPV operated by that division. The load drivers/discrete outputs are wired in series for each valve, so that both are required for operation. This scheme makes the logic single-failure-proof against inadvertent actuation.

Each of the SRVs is equipped with four solenoid-operated pilot valves. Three solenoids receive a Q-DCIS signal; the fourth is part of the DPS. The solenoid-operated pilot valves are powered by a 120-volt alternating current (VAC) uninterruptible power supply. The divisional safety power sources are located in the divisional battery rooms. The power and control cables are physically separated from other divisions.

The N-DCIS design bases include the following:

- diversity where required from RPS and SSLC/ESF
- single-failure-proof for power generation-by redundant power and redundant communications
- triple redundancy where required by high reliability systems (SB&PC, PAS, FWCS, turbine-generator)

- segmentation of PIP A, PIP B, BOP, N-DCIS network (contains gateways and the DPS), and PCFs

Gateways are used to translate information from one platform to another. Normal gateways are used to put safety data onto the non-safety networks for use in monitoring, alarming, and recording. Gateways are also used between different N-DCIS components. Some components do not require gateways by being directly connected through fiber cables. Gateways are non-safety components and are not treated as isolators between safety and non-safety components. Gateways are designed to handle their required number of signals at their required speed. The single failure of any gateway or datalink will not cause a scram or loss of power generation.

PIP takes advantage of the network switch capability by segmenting specific DCIS functions. "A" and "B" PIP functions are segregated to different controllers. PIP-A controllers are connected to PIP-A network managed switches. PIP-B controllers are connected to PIP-B network managed switches. MCR displays are segregated into PIP-A, PIP-B, BOP, and network switches. Individual segments are still dual redundant.

The backbone of the N-DCIS is multiple network managed switches, which are highly reliable and very fast. In summary, the N-DCIS configuration is as follows:

- redundant
- segmented
- single-failure-proof
- able to handle data rates for both transient and steady states in control, alarming, monitoring, and recording

7.1.1.3 NRC Staff Evaluation

SRP Section 7.1 describes the procedures to be followed in reviewing any I&C system, including embedded computers and software necessary to support the operation of safety systems. All I&C systems important to safety are required to be identified in DCD Section 7.1 and discussed in subsequent sections of DCD, Tier 2, Chapter 7. The safety systems supported by I&C systems are described in other sections of DCD Tier 2 (particularly in Chapters 5, 6, 8, 9, 10, 15, and 18).

This section evaluates each regulation and acceptance criterion applicable to the DCIS using SRP Appendix 7.1-A supplemented by SRP Appendixes 7.1-C and 7.1-D, which provide additional guidance for evaluating IEEE Std 603 compliance. The evaluation is intended to allow cross-referencing by specific I&C systems since the basis for the DCIS conformance with the acceptance criteria typically is applicable to specific I&C systems. Sections 7.2 to 7.8 of this report focus on system-specific acceptance criteria identified in the corresponding SRP sections.

7.1.1.3.1 DAC Process for Compliance with Regulations

The NRC implements the policy (SECY-92-053) of accepting the use of DAC, considered a

special kind of ITAAC, in lieu of detailed design information in the digital I&C area. The applicant proposes and the NRC staff reviews, approves, and certifies sufficient ITAAC to ensure that the licensee will meet the DAC during construction before loading fuel. The NRC allows the use of the DAC process because providing detailed design information is not desirable for applicants using technologies that change so rapidly that the design may have become obsolete between the time the NRC certifies the design and the time a plant is eventually built. For this section and the remaining sections of this report, the use of the acronym DAC/ITAAC refers to DAC and any associated ITAAC.

An overview of the NRC staff's review of the digital I&C design, and how DAC are used to complete the design detail, follows. This section also describes the DAC/ITAAC associated with digital I&C design, which includes the DAC/ITAAC for the human factors engineering (HFE) design process in DCD, Tier 1, Section 3.3 and the ITAAC for PAM instrumentation and EQ in DCD, Tier 1, Sections 3.7 and 3.8, respectively. As these other ITAAC are referenced throughout Chapter 7 of this report, a brief description of each is provided for clarity.

(1) Compliance with IEEE Std 603 (DCD, Tier 1, Section 2.2.15)

The I&C system uses the distributed digital system to perform plant protection and safety monitoring functions, as well as control functions. To ensure that the digital I&C system is implemented properly, the NRC staff considered existing regulatory requirements, guides, and standards in the SRP. The NRC staff follows the guidance provided in SRP Chapter 7, Appendix 7.1-C and Appendix 7.1-D, to verify that DCD Tier 2 has addressed all the criteria listed in IEEE Std 603, as required by 10 CFR 50.55a(h)(3). In accordance with the NRC policy in SECY-92-053, the applicant has opted to use the DAC process in lieu of providing the design detail for the digital I&C system.

The NRC staff first performed a functional review at the simplified block diagram level. Sections 7.1.1, 7.1.2, and 7.1.3, and Figure 7.1.1 of the DCD Tier 2 provide references to applicable requirements for the design of the DCIS, which includes a simplified block diagram of the I&C system, a network diagram of the DCIS, and high level functional requirements for the DCIS. The high level system functional requirements for the DCIS, such as RTS, ESFAS, are described in subsequent sub-sections of the DCD Tier 2. The regulatory requirements referenced in the DCD for the digital I&C system establish the design criteria related to postulated single failures, CCFs, appropriate signal isolation, and so forth. These issues are discussed in more detail throughout chapter 7 of this report. The NRC staff finds that the DCD adequately supports the NRC staff's review at the simplified block diagram level.

The second part of the NRC staff's review addressed the implementation of the digital I&C system design to meet the functional system requirements. The IEEE Std 603 criteria provide the bases for the DAC/ITAAC for the digital I&C system development process. DCD Tier 2 specifies conformance to IEEE Std 603 throughout Chapter 7. DCD, Tier 1, Section 2.2.15, contains the DAC/ITAAC to confirm I&C system compliance with IEEE Std 603. DCD, Tier 2, Section 7.1.2.4, specifies conformance to applicable RGs and industry standards as described and evaluated in Sections 7.1.1.3.3, 7.1.1.3.6, and 7.1.1.3.8 of this report. These RGs and industry standards provide more detailed guidance for implementing the design criteria in IEEE Std 603. The DAC in DCD, Tier 1, Section 2.2.15, consist of block level failure modes and effects analyses (FMEAs) and inspections of simplified logic diagrams, system design specifications, safety analyses, P&IDs, electrical one-line diagrams, and the project design manual. These are standard I&C design practices which provide objective means to verify the design. NEDE-33226P describes the hardware development process integrated into the

software life cycle process, which provides a phased approach for completing the DAC/ITAAC. NEDE-33226P, Figure 5-11, provides a high level flow of the hardware design process alongside the software development process. NEDE-33226P, Section 5.7.4, describes the hardware/software specification produced during the requirements phase of the life cycle process. NEDE-33226P, Section 5.7.6, describes the system requirements specification which identifies additional hardware requirements. NEDE-33226P is evaluated in Section 7.1.2 of this report. Taken as a whole, the above constitutes an acceptable process for complying with IEEE Std 603.

The NRC staff's RAIs 7.1-9 to 7.1-30 concerned design compliance with IEEE Std 603. In response, the applicant created a new Section 2.2.15 in DCD, Tier 1, Revision 4, for I&C compliance with IEEE Std 603. Section 2.2.15 contains the DAC/ITAAC for IEEE Std 603 (Table 2.2.15-2) to confirm I&C system compliance with IEEE Std 603 and DCD, Tier 2, Table 2.2.15-1, which identifies the applicability of functional systems to IEEE Std 603 DAC/ITAAC. The NRC staff accepted the DAC approach to address compliance with IEEE Std 603 requirements but stated that only certain sections of IEEE Std 603 are addressed in DCD, Tier 1, Revision 4, Section 2.2.15. In RAI 14.3-265, the NRC staff asked the applicant to address all IEEE Std 603 sections in DCD, Tier 1, Section 2.2.15 (thus superceding RAIs 7.1-9 to 7.1-30) . For any IEEE Std 603 sections that are not provided with the DAC/ITAAC, the NRC staff requested that the applicant identify how compliance is substantiated or provide links to existing non system-based ITAAC. RAI 14.3-265 was being tracked as an open item in the SER with open items. With its response to RAI 14.3-265, Supplement 1, the applicant also submitted responses to RAIs 7.1-99, 7.1-100, and 7.1-101, all of which are incorporated in DCD Revision 6. DCD, Tier 1, Table 2.2.15-1, was updated to include all applicable IEEE Std 603 criteria for all safety I&C systems. The DCD, Tier 1, Section 2.2.15, design description identifies that some IEEE Std 603 criteria do not appear in Table 2.2.15-1 as some IEEE Std 603 criteria do not require ITAAC consistent with NRC guidance or because the criteria are covered by other non-system ITAAC. Table 2.2.15-2, identifies design commitments for each IEEE Std criterion for the software projects. The ITAAC acceptance criterion contain two phases: (a) DAC phase that specifies the software projects design requirements and (b) ITAAC implementation phase that specifies the methods to verify the as-built design has satisfied the IEEE Std 603 requirements.

To support DCD, Tier 1, Section 2.2.15 requirements, the applicant also updated DCD, Tier 2, Table 7.1-2. Table 7.1-2 provides detailed cross-references to the DCD Tier 2 sections that describes the specific design and methods to satisfy the IEEE Std 603 requirements. The staff determined the response to 14.3-265 was acceptable since the applicant revised DCD, Tier 1, Section 2.2.15, and the sections referenced by DCD, Tier 2, Table 7.1-2, to properly address compliance with the IEEE Std 603. Based on the applicant's responses RAIs 7.1-9 to 7.1-30 and 14.3-265 are resolved.

(2) Software Development Activities (DCD, Tier 1, Section 3.2)

In the software development area, the NRC staff's acceptance of the software for safety system functions is based on (1) confirmation that acceptable plans were prepared to control software development activities, (2) evidence that the plans were followed in an acceptable software life cycle, and (3) evidence that the process produced acceptable design outputs. As discussed in Section 7.1.1.3.1 of this report, the NRC implements the policy (SECY-92-053) of accepting the use of DAC in lieu of detailed design information in the digital I&C area during design certification stage. The NRC staff follows the guidance provided in BTP HICB-14, for evaluating software life cycle processes for digital computer-based I&C systems. Similar to the case of

hardware, the ESBWR has not completed the software life cycle processes for design certification. Rather, the applicant has provided a software development process in NEDE-33226P and NEDE-33245P, which are incorporated by reference into Tier 2 of the DCD. The NRC staff finds that the applicant's software development process is acceptable for the following reasons:

- The applicant's software development process is based on and commits to the guidance in BTP HICB-14. This BTP provides detailed guidelines for evaluating software life cycle processes for digital computer-based I&C systems. These guidelines are based on reviews of licensee submittals, EPRI's requirements for advanced reactor designs, and the analysis of standards and practices documented in NUREG/CR-6101, "Software Reliability and Safety in Nuclear Reactor Protection Systems". The structure of this BTP is derived from the review process described in the Standard Review Plan NUREG-0800, Appendix 7.0-A.

- RG 1.152, which endorses IEEE Std 7-4.3.2, is the primary guidance identified in BTP HICB-14 for complying with requirements for safety systems that use digital computer systems. However, there are numerous RGs that are also addressed and discussed in the various BTPs acceptance criteria sections. Additionally, while many standards exist that can be used to develop software for safety systems, the information in this BTP is generally based on the standards and reports referred to in Section 7.1.2.1 of this report. The combination of these standards and RGs set bounding limits which the NRC staff can rely upon to make the determination of acceptability at the design certification stage.

- NEDE-33226P and NEDE-33245P describe the applicant's commitment to and implementation of BTP HICB-14, including the standards and RGs referenced therein. The applicant identified deviations from BTP HICB-14, that the NRC staff evaluated in Section 7.1.2 of this report and found acceptable. DCD, Tier 1, Section 3.2, includes the DAC/ITAAC to verify that the software plans are developed and implemented consistent with the software development process and produce acceptable design outputs.

(3) Human Factors Engineering (DCD, Tier 1, Section 3.3)

Several IEEE Std 603 sections are related to HFE: Section 5.8 (information displays), Section 5.14 (human factor considerations), and Sections 6.2 and 7.2 (manual control). SRP Section 7.5 identifies two additional topics related to HFE alarms and PAM instrumentation. IEEE Std 603, Sections 5.8 and 5.14 (DCD, Tier 2, Sections 7.1.6.6.1.9, and 7.1.6.6.1.15) are addressed by the DAC/ITAAC for HFE in DCD, Tier 1, Section 3.3. As the design of human system interfaces has not been completed for the ESBWR, DCD, Tier 2, Chapter 18 describes the applicant's HFE design processes. Chapter 18 of this report evaluates whether accepted HFE practices and guidelines are incorporated into the applicant's HFE design processes using the acceptance criteria in NUREG-0711, "Human Factors Engineering Program Review Model". DCD, Tier 1, Section 3.3, includes the DAC/ITAAC for verifying the implementation the HFE design processes, which includes the topics listed above. Since the above topics have both HFE and I&C requirements and guidelines that should be addressed in an integrated manner, the DAC/ITAAC included in DCD, Tier 1, Section 3.3 are referenced throughout Chapter 7 of this report.

(4) Post Accident Monitoring Instrumentation (DCD, Tier 1, Section 3.7)

The PAM instrumentation is evaluated in Section 7.5.2.3 of this report. The selection of

accident monitoring variables is integrated with the HFE design process as described in DCD Chapter 18. DCD, Tier 1, Section 3.7, includes these criteria and the ITAAC to confirm that PAM instrumentation is installed consistently with the selected variable and is referenced throughout Chapter 7 of this report.

(5) Environmental and Seismic Qualification of Mechanical and Electrical Equipment (DCD, Tier 1, Section 3.8)

While there is no DAC for the environmental qualification (EQ) and seismic qualification of mechanical and electrical equipment, the ITAAC for EQ and seismic qualification in DCD, Tier 1, Section 3.8 confirms digital I&C system conformance to IEEE Std 603, Sections 5.4 and 5.5 (these criteria are described in DCD, Tier 2, Sections 7.1.6.6.1.5 and 7.1.6.6.1.6), and is referenced throughout Chapter 7 of this report. Thus the DCD, Tier 1, Section 3.8, ITAAC is associated with the DAC/ITAAC for IEEE Std 603 discussed in Item (1) above. In DCD, Tier 2, Sections 3.10 and 3.11 describe the EQ programs for safety electrical and digital I&C equipment and are evaluated in Chapter 3 of this report.

(6) DAC for other SRP Acceptance Criteria

As described in SRP Appendix 7.1-A, compliance with SRP acceptance criteria (e.g., certain GDC requirements) is dependent on compliance with some or all of the IEEE Std 603 requirements. Accordingly, the evaluation of the SRP acceptance criteria depends upon DAC for the IEEE Std 603 requirements.

7.1.1.3.2 General Conformance of the Distributed Control and Information System with SRP Criteria

10 CFR 52.47(a)(9), requires that the application include an evaluation of the design against the SRP revision in effect 6 months before the docket date of the application and identify all differences in design features, analytical techniques, and procedural measures proposed for the design and those corresponding features, analytical techniques, and procedural measures given in the SRP acceptance criteria. SRP Table 7-1 provides a matrix identifying the regulatory requirements, acceptance criteria, and guidance and their applicability to the various sections of Chapter 7 of the safety analysis report (SAR) (DCD for design certification). DCD, Tier 2, Table 7.1-1, has identified all of the applicable regulatory requirements, acceptance criteria, and guidance for each I&C system in the design. Table 7.1-2, provides detailed cross-references to the DCD Tier 2 section that describes the specific design and method to satisfy IEEE Std 603 requirements. This assisted the NRC staff in identifying the related documentation within the DCD to address compliance with the regulatory requirements for I&C systems important to safety.

DCD, Tier 2, Table 7.1-1, identifies applicable regulatory requirements and guidelines for I&C systems. The NRC staff performed its review with SRP Table 7.1, Revision 5 and SRP Appendix 7.1-A, Revision 5, while the applicant was required to address Revision 4, which was in effect 6 months before the docketing of the design certification. SRP Table 7.1, Revision 5 and SRP Appendix 7.1-A, Revision 5, provide an expanded list of GDC applicable to I&C systems compared to SRP Appendix 7.1-A, Revision 4. Revision 5 of the SRP explicitly addresses several GDC that were implicitly included in Revision 4 through the table associated with GDC 13, so Revision 5 does not represent a change in regulatory requirements with respect to the GDC. While the applicant does not include all GDC from SRP Table 7.1, Revision 5, in DCD, Tier 2, Table 7.1-1, the NRC staff verified that all of the applicable GDC

were addressed in other parts of the DCD as described below.

The applicant has agreed to meet the SRP guidance with a few exceptions. These exceptions are noted in DCD, Tier 2, Section 1.9, "Conformance with Standard Review Plan and Applicability of Codes and Standards," and Section 3.1, "Conformance with NRC General Design Criteria," as well as the applicable sections of this report. In DCD, Tier 2, Table 1.9-7, the applicant provided clarifications with respect to six BTPs. Because of its unique design features related to being a passive ESBWR, BTPs HICB-2, HICB-3, HICB-4, HICB-5, HICB-6, and HICB-13 are not applicable to the design. The NRC staff finds these clarifications acceptable.

SRP Chapter 7, Appendix 7-A, provides an agenda for the station site visit related to the I&C systems and includes a verification of layouts, separation and isolation, test features, and the potential for damage resulting from fire, flooding, or other environmental effects. The review described in SRP Chapter 7, Appendix 7-A, will be accomplished as part of the testing and inspections done by the COL licensees referencing the design certification.

7.1.1.3.3 Compliance with 10 CFR 50.55a(a)(1)

10 CFR 50.55a(a)(1) requires that structures, systems, and components must be designed, fabricated, erected, constructed, tested, and inspected to quality standards commensurate with the importance of the safety function to be performed. The NRC staff evaluated whether 10 CFR 50.55a(a)(1) has been adequately addressed for the DCIS per SRP Appendix 7.1-A. SRP Appendix 7.1-A states that the applicant should commit to conformance with the RGs and industry standards referenced in SRP Sections 7.1 through 7.9 and the BTPs in SRP Appendix 7-A. SRP Appendix 7.1-A identifies the applicable RGs and standards in its discussion of the RGs. SRP Table 7.1 identifies that 10 CFR 50.55a(a)(1) applies to all I&C systems and components (all DCD Chapter 7 sections) and also specifies the applicability of specific RGs to particular Chapter 7 sections.

DCD, Tier 2, Sections 7.1.2.4 and 7.1.4.4 specify conformance to RGs and industry standards for the Q-DCIS and the N-DCIS, respectively. DCD, Tier 2, Table 7.1-1 identifies the applicability of specific RGs to particular I&C systems. DCD, Tier 2, Table 1.9-22 specifies the versions of the industrial code and standards applicable to the ESBWR. Using the preceding listed DCD sections, the NRC staff verified that the I&C standards listed in the DCD are consistent with SRP Appendix 7.1-A with some limited exceptions. DCD, Tier 2, Table 1.9-22 specifies conformance to Instrumentation, Systems, and Automation Society (ISA)-S67.04-2006 instead of ISA-S67.04-1994 for setpoint methodology. The setpoint methodology is evaluated in Section 7.1.4 of this report. NEDE-33226P and NEDE-33245P identify deviations from BTP HICB-14, five RGs, and associated industry standards. These deviations are evaluated in Section 7.1.2.3.4 of this report and found to be acceptable. DCD, Tier 2, Table 7.1-1 excludes 4 RGs: 1.174, 1.177, 1.189, and 1.200 from its applicability matrix and DCD, Tier 2, Table 1.9-7, identifies differences with the SRPs with regard to RGs 1.22, 1.118, and 1.151. These exclusions and differences are evaluated in Section 7.1.1.3.8 of this report and found to be acceptable. However, in RAI 7.1-100 the NRC staff requested the applicant to consistently identify standards for specific systems used to conform to the IEEE Std 603 criteria. An example is provided in RAI 7.1-100, Part D. In RAI 7.1-136, the NRC staff requested the applicant to address in DCD, Tier 2, Section 7.1.6.6, the RGs and standards used to conform to the IEEE Std 603 criteria. RAIs 7.1-100 and 7.1-136 were being tracked as open items in the SER with open items. In it responses, the applicant addressed the safety I&C designs conformance to both RG 1.53 and IEEE Std 379-2000, "Application of the Single Failure

Criterion to Nuclear Power Generating Station Safety Systems". A discussion about conformance to IEEE Std 379 is added to DCD, Tier 2, Section 7.1.6.6, which is the basis for modifying the conformance statement for RG 1.53. The conformance statements for RG 1.53 are consistently documented in DCD, Tier 2, Subsections 7.1.6.4, 7.2.1.3.4, 7.2.2.3.4, 7.2.3.3.4, 7.3.1.1.3.4, 7.3.1.2.3.4, 7.3.3.3.4, 7.3.4.3.4, 7.3.5.3.4, 7.3.6.3.4, 7.4.1.3.4, 7.4.2.3.4, 7.4.4.3.4, 7.4.5.3.4, 7.5.2.3.4, 7.5.3.3.4, 7.6.1.3.3, and 7.8.3.4. of the staff confirmed that the DCD changes were incorporated into DCD Revision 6. The NRC staff determined the response was acceptable since the applicant properly addressed conformance to RGs and industry standards compliance. Based on the applicant's responses, RAIs 7.1-100 and RAI 7.1-136 are resolved. Based on the above, the staff finds that 10 CFR 50.55a(a)(1) is adequately addressed for the DCIS.

7.1.1.3.4 Compliance with 10 CFR 50.34(f), 10 CFR 50.62 and 10 CFR 52.47(b)(1)

The applicant identified the following TMI Action Plan items that are not applicable to the design because the ESBWR relies on passive plant design features and not on the active systems identified below:

- II.K.3.13 - high pressure coolant injection (HPCI) and reactor core isolation coolant (RCIC) initiation levels
- II.K.3.15 - isolation of HPCI and RCIC (turbine-driven)
- II.K.3.21 - automatic restart of low-pressure core spray (LPCS) and low-pressure coolant injection (LPCI)
- II.K.3.22 - RCIC automatic switchover of suction supply

The NRC staff agrees with the applicant's determination.

The following TMI Action Plan items are applicable to the design:

(1) 10 CFR 50.34(f)(2)(v) [I.D.3], Bypass and Inoperable Status Indication

The NRC staff evaluated whether 10 CFR 50.34(f)(2)(v) has been adequately addressed for the DCIS. According to SRP Table 7-1 and SRP Appendix 7.1-A, 10 CFR 50.34(f)(2)(v) applies to the protection systems (RTS and ESF), information systems important to safety, interlock logic, and supporting systems (DCD Sections 7.2, 7.3, 7.5, and 7.6). 10 CFR 50.34(f)(2)(v) [I.D.3] requires an applicant to provide an automatic indication of the bypassed and operable status of the safety systems. DCD, Tier 2, Table 7.1-1, identifies 10 CFR 50.34(f)(2)(v) as being applicable to the safety systems consistent with SRP Table 7-1. DCD, Tier 2, Table 1A-1, states that the design of I&C provides an automatic indication of the bypasses and inoperable status of safety systems. This table also identifies where the applicability of 10 CFR 50.34(f)(2)(v) is discussed in DCD Sections 7.2, 7.3, 7.5, and 7.8.

SRP Section 7.5 states that the acceptance criteria for bypass and inoperable status indication are addressed in part by conformance to RG 1.47. SRP Table 7-1 and SRP Appendix 7.1-A states that RG 1.47 is applicable to the same systems as 10 CFR 50.34(f)(2)(v). DCD, Tier 2, Table 7.1-1, identifies that RG 1.47 is applicable to the safety systems consistent with SRP Table 7-1. DCD, Tier 2, Section 7.1.6.4, states for RG 1.47 that bypass indications are

designed to satisfy the guidance of IEEE Std 603, Section 5.8.3 and RG 1.47. This section also states that bypass indications use isolation devices that preclude the possibility of any adverse electrical effect of the bypass indication circuits on the plant's safety systems. DCD, Tier 2, Section 7.1.6.6.1.9, addresses the information display criterion (IEEE Std 603, Section 5.8) that requires information displays for the referencing platform be designed to be accessible to the operators, display variables for manually controlled actions, display system status information, provide indication of bypasses, and display the PAM variables in accordance with the HFE design process. DCD, Tier 1, Section 3.3, includes DAC/ITAAC for HFE design process. Based on the above and RG 1.47 being included in the applicable safety system design bases, the NRC staff finds that conformance to RG 1.47 has been adequately addressed.

In SRP Appendix 7.1-A, 10 CFR 50.34(f)(2)(v) is addressed by conformance to IEEE Std 603, Sections 5.6, 5.8, 5.12, and 6.3. The NRC staff evaluation of IEEE Std 603, Sections 5.6, 5.8, 5.12, and 6.3, is in Section 7.1.1.3.10 of this report. The NRC staff finds that Sections 5.6, 5.8, 5.12, and 6.3 of IEEE Std 603 are adequately addressed, based on their inclusion in the safety systems design bases and in DCD, Tier 1, Section 2.2.15, including the DAC/ITAAC for the applicant to verify conformance to these IEEE Std 603 sections. Information displays are designed using the HFE design process, as described in DCD, Tier 2, Chapter 18 and evaluated in Chapter 18 of this report. DCD, Tier 1, Section 3.3, includes the DAC/ITAAC for implementing the HFE design process, which includes the design and verification of controls and information displays for monitoring variables and systems in the control room. This verification is applicable to all safety systems and includes bypasses and inoperable status indications. Accordingly, based on the inclusion of 10 CFR 50.34(f)(2)(v) and associated criteria and guidelines in the safety systems design basis and their confirmation in the DAC/ITAAC, the NRC staff finds that the requirements of 10 CFR 50.34(f)(2)(v) have been adequately addressed for the DCIS.

(2) 10 CFR 50.34(f)(2)(xi) [II.D.3], Direct Indication of Relief and Safety Valve Position

10 CFR 50.34(f)(2)(xi) [II.D.3] requires an applicant to provide direct indication of relief and safety valve positions (open or closed) in the control room.

DCD, Tier 2, Table 1A.1, specifies that a direct indication of SRV and DPV positions (open or closed) be provided in the MCR. DCD, Tier 2, Section 7.3.1.1.5, also specifies that the ADS I&C indicates the status of the SRV and DPV in the MCR in conformance with IEEE 603 Section 5.8. DCD, Tier 2, Section 7.1.6.6.1.9 identifies that information display design is part of the HFE design process as described in DCD, Tier 2, Chapter 18 and evaluated in Chapter 18 of this report. DCD, Tier 1, Section 3.3, includes the DAC/ITAAC for implementing HFE design process, which includes the design and verification of controls and information displays for monitoring variables and systems in the control room. This verification is applicable to all safety systems and includes verifying the inventory of displays for system status indications. Accordingly, based on the display of the status of the SRV and DPV being included in the ADS I&C design basis and their confirmation in the DAC/ITAAC, the NRC staff finds that the requirements of 10 CFR 50.34(f)(2)(xi) [II.D.3] have been adequately addressed for the DCIS.

(3) 10 CFR 50.34(f)(2)(xvii) [II.F.1], Accident Monitoring Instrumentation

10 CFR 50.34(f)(2)(xvii) [II.F.1] requires the applicant to provide instrumentation to measure, record, and read out 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, as well as to provide for

continuous sampling of radioactive iodine and particulates in gaseous effluents from all potential accident release points and to provide for an onsite capability to analyze and measure these samples.

In DCD, Tier 2, Section 7.5.2, the applicant stated that the CMS provides the instrumentation to monitor the following:

- the atmosphere in the containment for high gross gamma radiation levels
- the pressure of the drywell and wetwell
- the drywell/wetwell differential pressure
- the lower and upper drywell water level (post-LOCA)
- the temperature of the suppression pool water
- the suppression pool water level
- the drywell/wetwell hydrogen/oxygen concentration
- the containment area radiation

These parameters are monitored during both normal reactor operations and post accident conditions to evaluate the integrity and safe conditions of the containment. Abnormal measurements and indications initiate alarms in the MCR.

DCD, Tier 2, Section 7.5.1, describes the PAM instrumentation, including the process to identify the post accident plant parameters to be displayed in the MCR. The PAM instrumentation has the following safety design basis:

- provide instrumentation to monitor variables and systems over their anticipated ranges for accident conditions, as appropriate, to ensure adequate safety

- provide the appropriate MCR instrumentation and displays to provide the information from which actions are taken to maintain a safe plant condition under accident conditions, including LOCAs

- provide equipment (including the necessary instrumentation) at appropriate locations outside the MCR with the capability for prompt hot shutdown of the reactor

- provide the means for monitoring the reactor containment atmosphere, spaces containing components that recirculate LOCA fluids, effluent discharge paths, and plant environs for radioactivity that may be released as a result of accidents

As discussed above, the PAM instrumentation and the CMS provide the accident monitoring instrumentation functions required by 10 CFR 50.34(f)(2)(xvii) [II.F.1]. As described in Section 7.5 of this report, the acceptability of the PAM instrumentation and the CMS and their conformance to 10 CFR 50.34(f)(2)(xvii) [II.F.1] are dependent upon (1) the inclusion of the accident monitoring instrumentation functions in the systems design bases, (2) the inclusion of IEEE Std 603 criteria in the systems design bases, (3) DCD, Tier 1, Section 2.2.15, including the DAC/ITAAC for the applicant to verify conformance to these IEEE Std 603 criteria, (4) the description in the DCD of the performance-based criteria the ESBWR uses for the selection, performance, design, qualification, display, and quality assurance of accident monitoring variables consistent with RG 1.97 and IEEE Std 497, (5) DCD, Tier 1, Section 3.7, including the performance-based criteria in the ITAAC to confirm that the PAM instrumentation is installed consistent with the selected variables, and (6) DCD, Tier 1, Section 3.3, including the

DAC/ITAAC to confirm that the HFE design is implemented based on the process described in DCD Chapter 18. Items (1) to (5) are evaluated and found acceptable in Section 7.5 of this report. DCD, Tier 1, Section 3.7 specifies that the scope of instrumentation relied upon to fulfill the PAM function is determined through the HFE design process. For each variable and type the process determines additional characteristics appropriate to that variable based on the guidelines provided in RG 1.97. PAM instrumentation software is developed in accordance with the software development program described in DCD, Tier 1, Section 3.2. Based on the review of DCD, Tier 1, Sections 2.2.15, 3.2, 3.3, and 3.7 DAC/ITAAC documentation, the NRC staff finds that the requirements of 10 CFR 50.34(f)(2)(xvii) have been adequately addressed for the DCIS.

(4) 10 CFR 50.34(f)(2)(xviii) [II.F.2], Inadequate Core Cooling Instrumentation

10 CFR 50.34(f)(2)(xviii) [II.F.2] requires an applicant to have instruments that provide, in the control room, an unambiguous indication of inadequate core cooling, such as primary coolant saturation meters in pressurized-water reactors (PWRs) and a suitable combination of signals from indicators of coolant level in the reactor vessel and in-core thermocouples in PWRs and boiling-water reactor (BWRs).

To address the requirement, SRP Appendix 7.1-A states that instrumentation for the detection of inadequate core cooling should provide the operator with sufficient information during accident situations to take planned manual actions and to determine whether safety systems are operating properly. In addition, the instrumentation should provide sufficient data for the operator to be able to evaluate the potential for core uncover and gross breach of protective barriers, including the resultant release of radioactivity to the environment.

For the design, the RPV water level is the only issue to be considered, because BWRs operate at saturation pressure and saturation monitors are not required. The detection of conditions indicative of inadequate core cooling in the design is provided by the direct RPV water level instrumentation. The RPV water level is measured by four physically separate level (differential pressure) transmitters mounted on separate divisional local racks in the safety envelope within the reactor building. Each transmitter is on a separate pair of instrument lines and is associated with a separate RPS electrical division. The instruments for monitoring the RPV water level from the sensor to the control room display are classified as safety instrumentation. Water level measurements include fuel zone, wide range, narrow range, and shutdown range. Each division has its own set of RPV sensing line nozzle connections.

The NRC staff reviewed the RPV water level measurement in the design. DCD, Tier 2, Table 1A-1, identifies that the RPV water level instrumentation system design includes a constant metered addition of purge water from the CRD hydraulic system to prevent the build-up of dissolved gasses in the fixed leg. DCD, Tier 2, Section 7.7.1.2.2, identifies that the Control Rod Drive Hydraulic Subsystem provides a purge flow that keeps the RPV water level reference leg instrument lines full. These lines are filled to address the effects of non condensable gases in the instrument lines and to prevent erroneous reference information after a rapid RPV depressurization event. DCD, Tier 2, Section 7.7.1.3.3, states that the instrument sensing lines for the NBS are in conformance with the guidelines in RG 1.151 and the associated guidance in ISA-S67.02.01, “Nuclear Safety-Related Instrument-Sensing Line Piping and Tubing Standard for Use in Nuclear Power Plants”.

DCD, Tier 2, Section 7.7.1.4, identifies that water level instruments are located outside the drywell so that calibration and test signals can be applied during reactor operation in

conformance with IEEE 603, Section 5.7. DCD, Tier 1, Table 2.2.15-2, includes the DAC/ITAAC for the applicant to verify that maintenance bypasses are implemented in the software development process to provide the capability for the testing and calibration of the safety systems. This provision will verify the ability of RPV level measurements to accomplish their safety functions. Based on the applicant's documentation of the TMI Action Plan item and DCD Tier 1 and Tier 2 updates, the NRC staff considers that the RPV water level measurement issues are resolved.

DCD, Tier 2, Section 7.7.1.2.2, describes the measurement of reactor coolant temperatures. The reactor coolant temperatures are measured at the mid-vessel inlet to the RWCU/SDC system and at the bottom head drain. Coolant temperatures can also be determined in the steam-filled parts of the RPV and steam-water mixture by measuring the reactor pressure. In the saturated system, reactor pressure connotes saturation temperature. Coolant temperatures (core inlet temperature) can normally be measured by the redundant core inlet temperature sensors located in each LPRM assembly below the core plate elevation. The RPV outside surface temperature is measured at the head flange and at the bottom head locations. Temperatures needed for operation and for compliance with the TS operating limits are obtained from these measurements. The NRC staff finds this approach acceptable.

Accordingly, based on the RPV water level and the reactor coolant temperature measurement instrumentation being included in the NBS I&C design basis and its confirmation in the DCD Tier 1, DAC/ITAAC, the NRC staff finds that requirements of 10 CFR 50.34(f)(2)(xviii) [II.F.2] have been adequately addressed for the DCIS.

(5) 10 CFR 50.34(f)(2)(xiv) [II.E.4.2], Containment Isolation Systems

10 CFR 50.34(f)(2)(xiv) [II.E.4.2] requires an applicant to provide containment isolation systems that do the following:

- ensure that all non essential systems are isolated automatically by the containment isolation system
- for each non essential penetration (except instrument lines), have two isolation barriers in series
- do not result in reopening the containment isolation valves on resetting of the isolation signal
- use a containment setpoint pressure for initiating containment isolation as low as is compatible with normal operation
- include automatic closing on a high radiation signal for all systems that provide a path to the environs

As described in DCD, Tier 2, Section 7.3.3, the LD&IS is used to detect and monitor leakage from the RCPB and to initiate the appropriate safety action to isolate the source of the leak. The system is designed to automatically initiate the isolation of certain designated process lines penetrating the containment, to prevent the release of radioactive material from the RCPB. DCD, Tier 2, Table 5.2-6, identifies the fluid lines designated for closure for each monitored variable. DCD, Tier 2, Section 6.2.4, describes the containment isolation functions and

specifies that information on containment isolation valves is provided in DCD, Tier 2, Tables 6.2-15 to 6.2-45. The evaluation of the second bullet above concerning two isolation barriers in series is provided in Section 6.2.4 of this report.

DCD, Tier 2, Section 5.2.5, identifies that diverse signals are provided for the containment isolation function. The signals, high drywell pressure, low reactor water level (Level 2), and the backup reactor water level (Level 1), are included in the list of monitored variables in DCD, Tier 2, Table 5.2-6, and in the list of sensor parameters in DCD, Tier 2, Table 7.3-5. The LD&IS functions are performed in two separate safety platforms. The MSIV isolation logic functions are performed in the RTIF-NMS platform, while all other containment isolation logic functions are performed in the SSLC/ESF platform.

DCD, Tier 2, Section 7.3.3.3, identifies that the LD&IS logic is designed to seal-in the isolation signal once the trip has been initiated. The isolation signal overrides any control action to trigger the opening of isolation valves. Reset of the isolation logic is required before any isolation valve can be opened manually. Manual valve override capability is provided for valves that are required to operate following a design basis event on a valve-by-valve or line-by-line basis. The valve override requires at least two deliberate operator actions and is under administrative controls. The override status is alarmed in the MCR. The NRC staff finds this acceptable.

DCD, Tier 2, Table 1A-1, in the discussion for 10 CFR 50.34(f)(2)(xiv), identifies that the alarm and initiation setpoints of the LD&IS are set to initiate containment isolation at the minimum values compatible with normal operating conditions for containment penetrations containing process lines that are not required for emergency operation. The value for this setpoint is based on the analytical limit used in safety analyses. The NRC staff finds this acceptable.

DCD, Tier 2, Table 5.2-6, identifies that the pathways to the environs, including the containment purge lines and valves and the reactor building HVAC exhaust, isolate on containment isolation signals, refueling area air exhaust high radiation signal, and the reactor building exhaust high radiation signal. The NRC staff finds this acceptable.

As discussed above, the LD&IS provides the containment isolation I&C functions associated with 10 CFR 50.34(f)(2)(xiv) [II.E.4.2]. As described in Section 7.3 of this report, the acceptability of the LD&IS and its conformance to 10 CFR 50.34(f)(2)(xiv) [II.E.4.2] are dependent upon on (1) the inclusion of the containment isolation I&C functions in the system design bases, (2) the inclusion of IEEE Std 603 criteria in the systems design bases, (3) DCD, Tier 1, Section 2.2.15, including the DAC/ITAAC for the applicant to verify conformance to these IEEE Std 603 criteria, (4) DCD, Tier 1, Section 3.2, including the DAC/ITAAC to verify the implementation of the software development process, and (5) DCD, Tier 1, Section 3.3, including the DAC/ITAAC to confirm that the HFE design is implemented based on the process described in DCD Chapter 18. Based on the review of DCD, Tier 1, Sections 2.2.15, 3.2, and 3.3 DAC/ITAAC documentation and DCD, Tier 2, Sections 7.2 and 7.3 design descriptions, the NRC staff finds that the requirements of 10 CFR 50.34(f)(2)(xiv) have been adequately addressed for the DCIS.

(6) 10 CFR 50.34(f)(2)(xix) [II.F.3], Instruments for Monitoring Plant Conditions Following Core Damage

10 CFR 50.34(f)(2)(xix) [II.F.3] requires an applicant to provide instrumentation adequate for monitoring plant conditions following an accident that includes core damage. DCD, Tier 2,

Table 7.1-1 identifies that PAM, CMS, PRMS, and ARMS support conformance to this requirement. The monitoring of plant conditions following core damage is a subset of the PAM functions provided by these systems. In addition, DCD, Tier 2, Section 7.3.1.2.2, describes the design of the deluge system. The deluge system is designed to flood the containment floor in the event of a core breach that results in molten fuel on the containment floor. This system is made up of two individual and identical trains, both of which contain an automatic actuation and a manual actuation ability. There are 12 deluge valves, each with four squib initiators (each train has a manual and automatic initiator). Each of these valves feeds the Basemat-Internal Melt Arrest Coolability (BiMAC) system, which floods the containment floor following a severe accident. The logic for the deluge valves is executed in a pair of dedicated non-safety PLCs and a pair of dedicated safety temperature switches. Automatic actuation of the deluge valves is accomplished in concert with a lower drywell high temperature. The containment floor is divided into 30 equal-area cells, with two thermocouples installed in each cell. One thermocouple from each cell is monitored in one PLC, while the other thermocouple from each cell is monitored in a second PLC. When temperatures exceed the setpoint at one set of thermocouples, coincident with setpoints being exceeded at a second set of thermocouples in adjacent cells, a trip signal is generated in each PLC.

As discussed above, the PAM, CMS, PRMS, and ARMS provide the PAM functions associated with 10 CFR 50.34(f)(2)(xix) [II.F.3]. As described in Section 7.5 of this report, acceptability of the PAM, CMS, PRMS, and ARMS and their conformance to 10 CFR 50.34(f)(2)(xix) [II.F.3], is dependent upon (1) the inclusion of the PAM functions in the systems design bases, (2) the inclusion of IEEE Std 603 criteria in the systems design bases, (3) DCD, Tier 1, Section 2.2.15, including the DAC/ITAAC for the applicant to verify conformance to these IEEE Std 603 criteria, (4) the description in the DCD of the performance-based criteria the ESBWR uses for the selection, performance, design, qualification, display, and quality assurance of accident monitoring variables consistent with RG 1.97 and IEEE Std 497, (5) DCD, Tier 1, Section 3.7, including the criteria and the DAC/ITAAC to confirm that the PAM instrumentation is installed consistent with the selected variables, and (6) DCD, Tier 1, Section 3.3, including the DAC/ITAAC to confirm that the HFE design is implemented based on the process described in DCD Chapter 18. Based on the review of DCD, Tier 1, Sections 2.2.15, 3.2, 3.3, and 3.7, DAC/ITAAC documentation, the NRC staff finds that the requirements of 10 CFR 50.34(f)(2)(xix) have been adequately addressed for the DCIS.

(7) 10 CFR 50.34(f)(1)(vii) [II.K.3.18], ADS Modification That Would Eliminate the Need for Manual Activation

10 CFR 50.34(f)(1)(vii) [II.K.3.18] requires an applicant to perform a feasibility and risk assessment study to determine the optimum ADS design modification that would eliminate the need for manual activation to ensure adequate core cooling.

DCD, Tier 2, Section 7.3.1.1, describes the ADS. In the design, the ECCS provides emergency core cooling in response to events that threaten reactor coolant inventory. The ECCS comprises the ADS, the GDCS, the ICS, and the SLC system. The ADS resides within the NBS and comprises the SRVs and DPVs and associated I&C. The ADS actuation logic is implemented in four SSLC/ESF divisions, each of which can make a Level 1 trip vote. Each of the divisional trip votes is shared with the other divisions. Normally, each of the four divisions makes a two-out-of-four (2/4) trip decision from the four divisional votes. Each division of the SSLC/ESF has two trains of 2/4 trip logic (except the DPV logic, which has three trains) to support the requirement that single divisional failures cannot result in inadvertent opening of any ADS valve (SRV or DPV). The ADS depressurizes the reactor to allow the low-head GDCS to

provide makeup coolant to the reactor. The ADS logic resides on the SSLC/ESF portion of the Q-DCIS. The GDCS provides emergency core cooling once the reactor has been depressurized. The GDCS is capable of injecting large volumes of water into the RPV to keep the core covered for at least 72 hours following a LOCA.

As discussed above, the ADS and the GDCS provide the automatic ADS I&C functions associated with 10 CFR 50.34(f)(1)(vii) [II.K.3.18]. As described in Section 7.3 of this report, acceptability of the ADS and the GDCS and their conformance to 10 CFR 50.34(f)(1)(vii) [II.K.3.18] are dependent upon (1) the inclusion of the automatic ADS I&C functions in the systems design bases, (2) the inclusion of IEEE Std 603 criteria in the systems design bases, (3) DCD, Tier 1, Section 2.2.15, including the DAC/ITAAC for the applicant to verify conformance to these IEEE Std 603 criteria, (4) DCD, Tier 1, Section 3.2, including the DAC/ITAAC to verify the implementation of the software development process, and (5) DCD, Tier 1, Section 3.3, including the DAC/ITAAC to confirm that the HFE design is implemented based on the process described in DCD Chapter 18. Based on the review of DCD, Tier 1, Sections 2.2.15, 3.2, and 3.3, DAC/ITAAC documentation, the NRC staff finds that the requirements of 10 CFR 50.34(f)(1)(vii) have been adequately addressed for the DCIS.

(8) 10 CFR 50.34(f)(2)(xxiv) [II.K.3.23], Central Reactor Vessel Water Level Recording

10 CFR 50.34(f)(2)(xxiv) [II.K.3.23] requires an applicant to provide the capability to record the reactor vessel water level in one location on recorders that meet normal post accident recording requirements.

DCD, Tier 2, Table 1A-1, shows that the recording of water levels is included in the MCR. Water level measurements are from the wide-range and fuel-range water level instruments. DCD, Tier 2, Section 7.5.1.3.4, includes a description of the process, with associated performance criteria, used to develop the PAM instrumentation. The description includes a list of the performance criteria with associated variables used to develop the PAM instrumentation. A recording requirement is included as a variable for the “Display Criteria.”

As discussed above, the PAM instrumentation provides the recording capability associated with 10 CFR 50.34(f)(2)(xxiv) [II.K.3.23]. As described in Section 7.5 of this report, acceptability of the PAM instrumentation and its conformance to 10 CFR 50.34(f)(2)(xxiv) [II.K.3.23], are dependent upon on (1) the inclusion of the recording capability in the system design bases, (2) the inclusion of applicable IEEE Std 603 criteria in the systems design bases, (3) DCD, Tier 1, Section 2.2.15, including the DAC/ITAAC for the applicant to verify conformance to these IEEE Std 603 criteria, (4) the description in the DCD of the performance-based criteria the ESBWR uses for the selection, performance, design, qualification, display, and quality assurance of accident monitoring variables consistent with RG 1.97 and IEEE Std 497, (5) DCD, Tier 1, Section 3.7, including the criteria and ITAAC to confirm that the PAM instrumentation is installed consistent with the selected variables, and (6) DCD, Tier 1, Section 3.3, including the DAC/ITAAC to confirm that the HFE design is implemented based on the process described in DCD Chapter 18. Based on the review of DCD, Tier 1, Sections 2.2.15, 3.2, 3.3, and 3.7, DAC/ITAAC documentation, the NRC staff finds that the requirements of 10 CFR 50.34(f)(2)(xxiv) have been adequately addressed for the DCIS.

(9) 10 CFR 50.34(f)(2)(xxiii) [II.K.2.10], Anticipatory Reactor Trip

10 CFR 50.34(f)(2)(xxiii) [II.K.2.10] requires, as part of RPS, an anticipatory reactor trip that would be actuated on a loss of main feedwater or on a turbine trip.

While 10 CFR 50.34(f)(2)(xxiii) states that it is applicable to only Babcock & Wilcox (B&W) plants, it is identified as applicable to the ESBWR on a generic issues basis since the ESBWR has an anticipatory trip. DCD, Tier 2, Section 7.2.1.2.4.2 includes anticipatory reactor trips that would be actuated on a loss of main feedwater or on a turbine trip. These are designated respectively in DCD, Tier 2, Section 7.2.1.2.4.2 as, "Power generation bus loss (Loss of feedwater flow)(Run mode only)" and "Turbine stop valve (TSV) closure." Corresponding trips are designated as initiators (as designated in Tier 1) and are included in DCD, Tier 1, Table 2.2.7-2, "RPS Automatic Functions, Initiators, and Associated Interfacing Systems." Based on the inclusion of the identified trips in the RPS design, the NRC staff finds that the requirements of 10 CFR 50.34(f)(2)(xxiii) [II.K.2.10] have been adequately addressed for the DCIS.

(10) 10 CFR 50.62, Requirements for Reduction of Risk from ATWS

The NRC staff evaluated whether 10 CFR 50.62 has been adequately addressed for the DCIS. 10 CFR 50.62 requires that BWR plants have (1) an ARI system that is diverse from the RPS and the ARI must be designed to perform its function in a reliable manner and be independent from the RPS [10 CFR 50.62(c)(3)], (2) an SLC system whose initiation must be automatic and which must be designed to perform its function in a reliable manner [10 CFR 50.62(c)(4)], and (3) an automatic recirculation pump trip (RPT) [10 CFR 50.62(c)(5)]. 10 CFR 50.62(c)(5) is not applicable to the ESBWR because the design does not have a recirculation pump. SRP Table 7.1 identifies that 10 CFR 50.62 applies to the DPS (DCD Section 7.8). DCD, Tier 2, Table 7.1-1, identifies that 10 CFR 50.62 is applicable to relevant safety and non-safety I&C systems.

Section 7.8 of this report provides a detailed evaluation of 10 CFR 50.62. As described in Section 7.8 of this report, the diverse ATWS mitigation logic includes the ARI functions required by 10 CFR 50.62(c)(3), the ATWS mitigation logic includes the SLC functions required by 10 CFR 50.62(c)(4), and both of the ATWS mitigation logics have acceptable diversity from the RPS and provide reasonable assurance of functioning in a reliable manner. Accordingly, the NRC staff finds that 10 CFR 50.62 has been adequately addressed for the DCIS.

(11) 10 CFR 52.47(b)(1), ITAAC for Standard Design Certification

The NRC staff evaluated whether the requirements of 10 CFR 52.47(b)(1) are addressed for I&C systems for the DCIS. This regulation requires that the application (for design certification) contain proposed ITAAC that are necessary and sufficient to provide reasonable assurance that, if the inspections, tests, and analyses are performed and the acceptance criteria are met, a plant that references the design certification has been constructed and will operate in accordance with the design certification, the Atomic Energy Act, and the Commission's rules and regulations. The NRC staff reviewed the applicable DCD, Tier 1, Sections 2.2.15, 3.2, 3.3, and 3.7, DAC/ITAAC documentation and the NRC staff finds that the requirements of 10 CFR 52.47(b)(1) have been adequately addressed for the DCIS. Details of the staff evaluation are provided in Section 14.3 of this report.

7.1.1.3.5 Resolution of I&C-Related Generic Issues

(1) A-19, "Digital Computer Protection Systems"

Generic issue A-19 was raised in 1978. NUREG-0933, "Resolution of Generic Safety Issues,"

issued August 2008, Table 2, identifies A-19 as a licensing issue, not a generic safety issue. In Generic Issue A-19, the NRC staff identified a need to standardize the safety review of RPS incorporating digital computers. Since 1978, the NRC has developed SRP Chapter 7 which includes the following:

- SRP Appendix 7.0-A, "Review Process for Digital Instrumentation and Control Systems"
- SRP Appendix 7.1-A, "Acceptance Criteria and Guidelines for Instrumentation and Control Systems"
- SRP Appendix 7.1-C, "Guidance for Evaluation of Conformance to IEEE Std 603"
- SRP Appendix 7.1-D, "Guidance for Evaluation of Application of IEEE Std 7-4.3.2"
- BTP HICB-14, "Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems"
- BTP HICB-19, "Guidance for Evaluation of Diversity and Defense-In-Depth in Digital Computer-Based Instrumentation and Control Systems"
- BTP HICB-21, "Guidance on Digital Computer Real-Time Performance"
- SRP Section 14.3.5, "Instrumentation and Controls—Inspections, Tests, Analyses, and Acceptance Criteria"

The DCD addresses conformance to the guidance listed above. Throughout Chapter 7 of this report, the NRC staff documents its evaluation of the conformance of the design to the guidance. The NRC staff finds that Generic Issue A-19 is adequately addressed.

(2) A-34, "Instruments for Monitoring Radiation and Process Variables during Accidents"

Generic Issue A-34 was initiated to develop criteria and guidelines to be used by applicants, licensees, and NRC staff reviewers to support the implementation of RG 1.97. In 1980, the NRC staff decided that Generic Issue A-34 was resolved and that the implementation of this item would be carried out under TMI Action Plan Item II.F.3, which is discussed in Section 7.1.1.3.4, Item (6) above. Accordingly, the NRC staff finds that Generic Issue A-34 is adequately addressed.

(3) A-47, "Safety Implications of Control Systems"

Generic Issue A-47 identified the need to perform an in-depth review of the non-safety control systems and to assess the effect of control system failures on plant safety. To this end, tasks were established to identify potential control system failures that, either singly or in selected combinations, could cause overpressure, overcooling, overheating, overfilling, or reactivity events.

DCD, Tier 2, Section 7.7, addresses the I&C systems for normal plant operation that do not perform plant safety functions. However, these systems do control plant processes that can have an impact on plant safety. These systems can affect the performance of safety functions either through normal operation or through inadvertent operation. Consistent with SRP

Section 7.7, Section 7.7 of this report documents the NRC staff confirmation that the failure of the control systems themselves or as a consequence of supporting system failures, such as loss of power sources, does not result in plant conditions more severe than those described in the analysis of design basis accidents and AOOs.

A specific example raised in A-47 was the automatic reactor vessel overfill protection. In the design, the automatic reactor vessel overfill protection is a feature of the FWCS described in DCD, Tier 2, Section 7.7.3. If the reactor water level rises to Level 8, then equipment protective actions will trip the main turbine and reduce feedwater demand to zero. The reactor water level rising to Level 8 results in the shutdown of the reactor by the RPS. The feedwater pumps will be tripped if the water level continues to rise to Level 9. The trip logic for the FWCS overfill protection is part of the RPS instrumentation. This example illustrates that a failure of the control system does not result in plant conditions more severe than those described in the analysis of the design basis accidents and AOOs. The standard plant TS (DCD, Tier 2, Chapter 16) provide surveillance requirements for the reactor vessel water high Level 8 function of the RPS instrumentation.

Based on the above, the NRC staff finds that Generic Issue A-47 is adequately addressed.

(4) New Generic Issue 45, "Inoperability of Instrumentation Due to Extreme Cold Weather"

New Generic Issue 45 involves ensuring that safety process, instrument, and sampling lines do not freeze during extreme cold weather. In response to this issue, the acceptance criteria for the design of protective measures against freezing in instrument lines of safety systems were included in RG 1.151. DCD, Tier 2, Section 7.1.6.4, states that instrument sensing lines are designed to conform to the guidance in RG 1.151, Revision 1. Section 7.1.6.6.1.5 states that safety components are designed to be qualified to operate in the normal and abnormal environments (including temperature, humidity, pressure, radiation, seismic, and electromagnetic interference (EMI) conditions) in which they are located; therefore, inoperability of instrumentation due to extreme cold would only be applicable to the instrument sensing lines.

DCD, Tier 1, Section 3.8 ITAAC covers the EQ program. Safety-related equipment can perform its safety function under normal, abnormal, and design basis accident conditions.

As DCD Tier 2 specifies that the design conforms to RG 1.151, the NRC staff finds that New Generic Issue 45 is adequately addressed.

(5) New Generic Issue 64, "Identification of Protection System Instrument Sensing Lines"

New Generic Issue 64 involves identifying the protection system equipment that is part of the protection system subject to the regulations. The NRC staff decided that RG 1.151 and ISA-S67.02.01 address this issue.

DCD, Tier 2, Section 7.1.6.4, states that instrument sensing lines are designed to conform to the guidance in RG 1.151, Revision 1. ISA-S67.02.01, Section 5.3, "Identification and Channel Coding," states that the instrument sensing tubing or piping runs pertaining to safety instrument channels shall be identified and coded so as to identify its channel. Each instrument sensing line and associated valves in this channel shall have an identification tag showing the channel and unique line or valve identification number.

The identification of safety equipment is addressed by IEEE Std. 603, Section 5.11, which is evaluated in section 7.1.1.3.10 of this report. DCD, Tier 1, Table 2.2.15-2, includes the DAC/ITAAC for IEEE Std. 603, Section 5.11, to verify that distinct identification of each redundant portion of safety systems.

As DCD Tier 2 specifies that the design conforms to RG 1.151, the NRC staff finds that New Generic Issue 64 is adequately addressed.

(6) New Generic Issue 142, "Leakage through Electrical Isolators in Instrumentation Circuits"

New Generic Issue 142 involves the concern that isolation devices subjected to failure voltages or currents at less than maximum credible fault levels passed significant levels of voltage or current, but the same devices performed acceptably at maximum credible levels. The safety system on the Class 1E side of the isolation device may be affected by the passage of small levels of electrical energy, depending on the design and function of the safety system.

DCD, Tier 2, Section 7.1.3.3, describes the interfaces between electrical divisions for logic voting, between divisional and non divisional circuits for annunciations, and so on. However, these interfaces are accomplished through a fiber optic medium that is non conductive and thus provides full safety isolation. No interlocking is provided, nor required, for these interfaces. The electrical hardware is not affected significantly by noise because of the combination of digital transmission and fiber optics incorporated in the design.

The electrical isolation of safety equipment is addressed by IEEE Std. 603, Section 5.6, which is evaluated in section 7.1.1.3.10 of this report. DCD, Tier 1, Table 2.2.15-2, includes the DAC/ITAAC for IEEE Std. 603, Section 5.6, to verify the applicable independence of safety systems, which includes electrical isolation.

Based on the review of DCD Tier 2 information, the NRC staff finds that New Generic Issue 142 is adequately addressed.

(7) New Generic Issue 67.3.3, "Steam Generator, Staff Actions-Improved Accident Monitoring"

New Generic Issue 67.3.3 resulted from lessons from a January 1982 steam generator tube rupture event. Since the ESBWR does not have steam generators, New Generic Issue 67, is not applicable to the design. However, one recommendation, New Generic Issue 67.3.3, "Improved Accident Monitoring," is applicable to both PWRs and BWRs. New Generic Issue 67.3.3, involves addressing accident monitoring weaknesses by fully implementing RG 1.97. DCD, Tier 2, Table 1.11-1 states that New Generic Issue 67.3.3 is addressed by conformance with RG 1.97, as described in DCD, Tier 2, Section 7.5. The NRC staff evaluated PAM instrumentation conformance to RG 1.97 in Section 7.5 of this report and found it acceptable.

DCD, Tier 1, Section 3.7 provides ITAAC to confirm that the installed PAM instrumentation conforms to the guidance of RG 1.97.

The NRC staff finds this treatment of New Generic Issue 67.3.3 acceptable. Accordingly, New Generic Issue 67.3.3 is adequately addressed.

(8) New Generic Issue 120, "On-Line Testability of Protection Systems"

New Generic Issue 120 addresses requirements for conducting at-power testing of safety system components without impairing plant operation. The staff raised this issue because it found, in the review of several plant TS in 1985, that some older plants did not provide as complete a degree of on-line testing as other plants. GDC 21, "Protection System Reliability and Testability," includes the requirements for on-line testing of protection systems. These requirements apply to both the RPS and the engineered safety features actuation system (ESFAS). A protection system with two-out-of-four logic that can operate with one channel in bypass, and the remaining three channels in a two-out-of-three logic configuration meets this requirement. This issue was resolved with no new requirements.

Guidance for this issue is provided in RG 1.22, "Periodic Testing of Protection System Actuation Functions," RG 1.118, "Periodic Testing of Electric Power and Protection Systems," and IEEE Std 338. Conformance to these documents ensures that the ESBWR protection systems (including logic, actuation devices, and associated actuated equipment) will be designed to permit testing while the plant is at power without adversely affecting plant operation.

DCD, Tier 2, Section 7.1.6.6.1 states that the ESBWR protection system has a two-out-of-four logic configuration that can operate with one channel in bypass, and the remaining three channels in a two-out-of-three logic configuration. This meets the requirements in GDC 21 for on-line testing. The ESBWR's design provision for testing of the protection system conforms to the guidelines in RGs 1.22 and 1.118

The on-line testability of protection systems is addressed by IEEE Std. 603, Sections 5.7 and 6.5, which are evaluated in section 7.1.1.3.10 of this report. DCD, Tier 1, Table 2.2.15-2, includes the DAC/ITAAC for IEEE Std. 603, Sections 5.7 and 6.5, to verify that maintenance bypasses allow test and calibration of one out of four divisions, that the divisions not in bypass status will accomplish their safety functions, that bypassed divisions alarm in the MCR, and that the division logic automatically becomes a two-out-of-three voting scheme.

The NRC staff finds this treatment of New Generic Issue 120 acceptable. Accordingly, New Generic Issue 120 is adequately addressed.

(9) NRC Office of Inspection and Enforcement (IE) Bulletin 80-06, "Engineered Safety Feature (ESF) Reset Controls"

IE Bulletin 80-06, dated March 13, 1980, requires all operating plant licensees to review plant design drawings at the schematic or elementary diagram level to determine whether, upon the reset of an ESF actuation signal, all associated safety equipment remains in its emergency mode.

DCD, Tier 2, Section 7.3.1.1.2, calls for safety VDUs in the MCR to provide a display format allowing the operator to manually open each SRV and each DPV independently, using the primary SSLC/ESF logic function (IEEE Std 603, Sections 5.8, 6.2, and 7.2). Each non-safety VDU in the MCR provides a display format allowing the operator to manually open each SRV independently, using the DPS logic function. Each display uses an "arm/fire" configuration requiring at least two deliberate operator actions. Operator use of the "arm" portion of the display triggers a plant alarm. The two manual opening schemes from the SSLC/ESF and from the DPS are diverse. Each safety VDU provides a display with an "arm/fire" switch (one per division) to manually initiate ADS as a system, rather than initiating each valve individually (IEEE Std 603, Sections 5.8, 6.2, and 7.2). If the operator uses any 2/4 "arm/fire" switches, the

ADS sequence seals in and starts the ADS valve-opening sequence (IEEE Std 603, Section 5.2). This requires at least 2/4 deliberate operator actions.

DCD, Tier 1, Table 2.2.15-2, includes the DAC/ITAAC for verifying that the protection systems design was completed in compliance with IEEE Std 603.

Based on the design implementing the IEEE Std 603 requirement for actuation seal-in provisions and requiring two deliberate operations to perform a manual operation, such as the reset function, their verification in the DCD Tier 1, DAC/ITAAC, the NRC staff finds that the design acceptably addresses IE Bulletin 80-06.

7.1.1.3.6 Compliance with I&C - Related General Design Criteria

SRP Table 7.1 and SRP Appendix 7.1-A identify the following GDC as the acceptance criteria for I&C systems important to safety. This section provides a general evaluation of each GDC, while the remaining sections of Chapter 7 of this report evaluate the specific application of the GDC.

(1) GDC 1, "Quality Standards and Records"

GDC 1 requires quality standards and maintenance of appropriate records. The NRC staff evaluated whether GDC 1 has been adequately addressed for the DCIS per SRP Appendix 7.1-A. SRP Appendix 7.1-A for GDC 1 states that the NRC staff review should confirm that the appropriate regulatory guides and endorsed standards are identified as applicable for each I&C system important to safety. The discussion of conformance to RGs and standards for 10 CFR 50.55a(a)(1) in Section 7.1.1.3.3 applies to GDC 1. Based on the finding for 10 CFR 50.55a(a)(1), the NRC staff finds that the requirements of GDC 1 regarding RGs and standards have been adequately addressed for the DCIS.

GDC 1 also includes requirements for a quality assurance program and the maintenance of appropriate records. The evaluation of the applicant's quality assurance program and appropriate records is addressed in Chapter 17 of this report.

(2) GDC 2, "Design Bases for Protection Against Natural Phenomena"

GDC 2 requires design bases for protection against natural phenomena. The NRC staff evaluated whether GDC 2 has been adequately addressed for the DCIS. SRP Table 7.1 and SRP Appendix 7.1-A show that GDC 2 applies to all I&C safety systems (DCD Sections 7.2, 7.3, 7.4, 7.5, and 7.6). SRP Appendix 7.1-A for GDC 2 states that the design bases for protection against natural phenomena for I&C systems important to safety should be provided for the I&C system. DCD, Tier 2, Table 7.1-1, identifies the applicability of GDC 2 to I&C systems, including its applicability to all safety I&C systems. DCD, Tier 2, Section 7.1.6.6.1.5, states that the safety I&C systems are designed to meet the requirements of IEEE Std 603, Section 5.4, for EQ. In DCD, Tier 1, Section 3.8 includes the ITAAC for the applicant to confirm the EQ of safety electrical and digital I&C equipment, which is consistent with the requirements of IEEE Std 603, Section 5.4. Also, the safety I&C systems are designed to meet RG 1.100, Revision 3, September 2009, "Seismic Qualification of Electric and Mechanical Equipment for Nuclear Power Plants", and IEEE Std 344, "IEEE Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations", associated with seismic qualification.

SRP Appendix 7.1-A for GDC 2 also states that the design bases should identify those systems and components that should be qualified to survive the effects of earthquakes and other natural phenomena. DCD, Tier 2, Table 3.2-1, identifies that the safety I&C systems are designed as seismic Category I systems. DCD, Tier 2, Chapter 3, states that the I&C systems important to safety are qualified for protection against natural phenomena, consistent with the analysis of these events, and that they are located and housed in structures consistent with these requirements. Section 3.10 of this report evaluates the adequacy of qualification programs to demonstrate the capability of I&C systems to withstand the effects of natural phenomena. DCD, Tier 2, Section 3.11, specifies that instrumentation systems needed for severe accidents are designed to operate in the severe accident environment for which they are intended, and over the time span for which they are needed. DCD, Tier 2, Section 3.11, is evaluated in Section 3.11 of this report. DCD, Tier 1, Section 3.8, includes the ITAAC to verify the EQ and seismic qualification of instrumentation systems needed for severe accidents. Based on the above, the NRC staff finds that the requirements of GDC 2 have been adequately addressed.

(3) GDC 4, "Environmental and Dynamic Effects Design Bases"

GDC 4 requires environment and dynamic effects design bases. The NRC staff evaluated whether GDC 4 has been adequately addressed for the DCIS. SRP Table 7.1 and SRP Appendix 7.1-A show that GDC 4 applies to all I&C safety systems (DCD Sections 7.2, 7.3, 7.4, 7.5, and 7.6). SRP Appendix 7.1-A for GDC 4 states that the environmental and dynamic effects (e.g., missiles) design bases for I&C systems important to safety should be provided for each system. Environmental design bases are discussed in DCD, Tier 2, Chapter 7, but missile design bases are discussed in DCD Tier 2, Chapter 3, as described below. DCD Tier 2, Table 7.1-1, identifies the applicability of GDC 4 to I&C systems, including its applicability to all safety I&C systems. DCD, Tier 2, Section 7.1.6.6.1.5, describes the methods used for temperature and humidity, radiation, and EMI qualification. Safety I&C systems are designed to meet the EQ requirements in RG 1.89, "Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants", RG 1.100, and IEEE Std 323, "Qualifying Safety - Related Equipment for Nuclear Power Generating Stations", associated with EQ. In DCD, Tier 1, Section 3.8, includes the ITAAC for the applicant to confirm the EQ of safety electrical and digital I&C equipment, which is consistent with the requirements of IEEE Std 603, Section 5.4.

SRP Appendix 7.1-A for GDC 4 also states that the design bases should identify those systems and components that are qualified to accommodate the effects of environmental conditions and that are protected from the dynamic effects of missiles, pipe whipping, and discharging fluids. DCD, Tier 2, Chapter 3, specifies that safety I&C systems be protected from the dynamic effects of missiles, pipe whipping, and discharging fluids. DCD, Tier 2, Table 3.2-1, identifies the equipment classification of safety I&C systems. DCD, Tier 2, Table 3.11-1, identifies the qualification program and required operating times for electrical and mechanical equipment, including safety I&C systems. DCD, Tier 2, Appendix 3H, identifies the design bases environmental conditions by plant zone and typical equipment. Section 3.10 of this report evaluates the adequacy of qualification programs to demonstrate the capability of I&C systems to withstand dynamic effects. Section 3.11 of this report evaluates the adequacy of EQ programs. DCD, Tier 1, Section 3.8, provides the ITAAC for the EQ of the safety electrical equipment located in a harsh environment to verify that such equipment can perform its safety function under normal, abnormal, and design basis accident (DBA) environmental conditions.

SRP Appendix 7.1-A for GDC 4 also states that the I&C systems needed for severe accidents must be designed so there is reasonable assurance they will operate in the severe accident

environment for which they are intended and over the time span for which they are needed. Monitoring for severe accidents is evaluated in Section 7.5.2.3, Item (4), of this report and found to be acceptable.

Based on the above, the NRC staff finds that environmental and dynamic design bases are provided for the DCIS as a whole, that qualified systems are identified, and that the I&C systems needed for severe accidents are designed so there is reasonable assurance they will operate in the severe accident environment for which they are intended and over the time span for which they are needed. Accordingly, the NRC staff finds that the requirements of GDC 4 have been adequately addressed.

(4) GDC 10, "Reactor Design"

GDC 10 requires that the reactor core and associated coolant, control, and protection systems 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. The NRC staff evaluated whether GDC 10 has been adequately addressed for the DCIS. SRP Table 7.1 identifies that GDC 10 applies to I&C protection and control systems (DCD Sections 7.2, 7.3, 7.6, and 7.7). SRP Appendix 7.1-A for GDC 10 states that the NRC staff review should evaluate the I&C system contributions to design margin for reactor core and coolant systems. DCD, Tier 2, Table 15.1-6, identifies systems, including protection, and control systems, required to mitigate AOOs. DCD, Tier 2, Chapter 7, includes corresponding actions in the design bases of the protection and control systems to maintain the reactor core and reactor coolant systems within appropriate margins. In DCD, Tier 1, Sections 2.2.15, 3.2, 3.3, and 3.8 include the DAC/ITAAC for the applicant to verify that the protection and control system designs implement these design bases. The implementation of GDC 10 is further discussed in Sections 7.2, 7.3, 7.6, and 7.7 of this report. Accordingly, based on the applicant identifying necessary protection and safety actuations in the design bases for the protection and control systems, and their verification in the DCD Tier 1, DAC/ITAAC, the NRC staff finds that the requirements of GDC 10 have been adequately addressed for the DCIS.

(5) GDC 13, "Instrumentation and Control"

GDC 13 requires providing instrumentation to monitor variables and systems over their anticipated ranges for normal operation, AOOs, and accident conditions to assure adequate safety. GDC 13 also requires providing appropriate controls to maintain these variables and systems within prescribed operating ranges. The NRC staff evaluated whether GDC 13 has been adequately addressed for the DCIS. SRP Table 7.1 identifies that GCD 13 applies to all I&C systems, including supporting systems (all DCD Chapter 7 sections). DCD, Tier 2, Table 7.1-1, identifies that GDC 13 is applicable to all I&C systems important to safety. The applicant has identified interrelated processes to design the monitoring and control capabilities. NEDE-33226P and NEDE-33245P, as part of a software life cycle process, define a process by which plant performance requirements under various operational conditions will be specified, implemented, and tested. DCD, Tier 1, Section 3.2, includes the DAC/ITAAC for verifying that the software plans were developed and implemented consistent with this process and produce acceptable design outputs. DCD, Tier 1, Section 3.3, includes the DAC/ITAAC for implementing an HFE design process, which includes the design and verification of controls and information displays for monitoring variables and systems in the control room.

In addition, the NRC staff has evaluated the appropriate controls to maintain these variables and systems within prescribed operating ranges for specific systems throughout Chapter 7 of

this report and found them acceptable. Accordingly, based on the defined processes for designing the monitoring and control capability, their verification in the DCD Tier 1, DAC/ITAAC, and the appropriate controls provided for specific systems, the NRC staff finds that the requirements of GDC 13 have been adequately addressed for the DCIS.

(6) GDC 15, "Reactor Coolant System Design"

GDC 15 requires that the reactor coolant system and associated auxiliary, control, and protection systems shall be designed with sufficient margin to ensure that the design conditions of the RCPB are not exceeded during any condition of normal operation, including AOOs. The NRC staff evaluated whether GDC 15 had been adequately addressed for the DCIS. SRP Table 7-1 identifies that GDC 15 applies to I&C protection and control systems (DCD Sections 7.2, 7.3, 7.6, and 7.7). SRP Appendix 7.1-A for GDC 15 states that the NRC staff review should evaluate the I&C system contributions to design margin for reactor coolant systems. DCD, Tier 2, Table 15.1-6, identifies systems, including protection and control systems, required to mitigate AOOs. DCD, Tier 2, Chapter 7, includes corresponding actions in the design bases of the protection and control systems to maintain the reactor core and reactor coolant systems within appropriate margins. In DCD, Tier 1, Sections 2.2.15, 3.2, 3.3, and 3.8 include the DAC/ITAAC for the applicant to verify that the protection and control system designs implement these design bases. The implementation of GDC 15 is further discussed in Sections 7.2, 7.3, 7.6, and 7.7 of this report. Accordingly, based on the applicant's identification of necessary protection and safety actuations in the design bases for the protection and control systems, and their verification in the DCD Tier 1, DAC/ITAAC, the NRC staff finds that the requirements of GDC 15 have been adequately addressed for the DCIS.

(7) GDC 16, "Containment Design"

GDC 16 requires containment leak-tight barrier against the uncontrolled release of radioactivity. The NRC staff evaluated whether GDC 16 has been adequately addressed for the DCIS. SRP Table 7-1 identifies that GDC 16 applies to I&C ESF and interlock logic (DCD Sections 7.3 and 7.6). SRP Appendix 7.1-A for GDC 16 states that GDC 16 imposes functional requirements on ESF I&C systems to the extent that they support the requirement that the containment provide a leak tight barrier. SRP Appendix 7.1-A identifies several potential relevant I&C functions but the only one applicable to the ESBWR passive design is containment isolation. GDC 16 is not applicable to the ESBWR interlock logic, since the one interlock is associated with coolant injection into the reactor, not containment isolation. DCD, Tier 2, Section 7.3.2, describes the PCCS, which provides containment cooling. While the PCCS has no I&C functions, it does rely on I&C functions in the ICS to perform its safety functions, as described in DCD, Tier 2, Section 7.4.4.3. In DCD Tier 2, Sections 7.3.3 and 7.3.5 identify the containment isolation functions in the LD&IS and SSLC/ESF system design bases. In DCD, Tier 1, Sections 2.2.15, 3.2, 3.3, and 3.8 include the DAC/ITAAC for the applicant to verify that the ESF actuation and control systems, VBIF, and all subsystem designs implement these design bases. Accordingly, based on the applicant's identification of the necessary containment isolation functions in the design bases of the ESF actuation and control systems, VBIF, and all subsystems, and their verification in the DCD Tier 1, DAC/ITAAC, the NRC staff finds that the requirements of GDC 16 have been adequately addressed for the DCIS.

(8) GDC 19, "Control Room"

GDC 19 requires control room functionality, control room habitability, and remote shutdown capability. The NRC staff evaluated whether GDC 19 has been adequately addressed for the

DCIS. SRP Table 7-1 identifies that GDC 19 applies to all I&C systems and supporting systems (DCD Sections 7.2 through 7.8). The evaluation of the operation of specific I&C systems is included throughout Chapter 7 of this report. DCD, Tier 2, Table 7.1-1, identifies that GDC 19 is applicable to all I&C systems, consistent with SRP Table 7-1. The adequacy of the human factors aspects of the control room design is addressed in DCD, Tier 2, Section 18.1.5, which specifies that divisional separations for control, alarm, and display be maintained. In DCD, Tier 2, Sections 6.4.8 and 9.4.1.5, as examples, detail control room habitability area design features, including instrumentation for air flow, differential pressure (across the area envelope), and safety radiation monitoring. Control room habitability is evaluated in Section 6.4 of this report. Remote shutdown system (RSS) capability is identified in Section 7.4.2 of the DCD Tier 2 document. The RSS maintains Division I/II separation and isolation.

The I&C subsystems described in DCD, Tier 2, Sections 7.2 through 7.8, include details of control interfaces through either the Q-DCIS or the N-DCIS. In DCD, Tier 2, Sections 7.1.3.1 and 7.1.4.2 identify the design bases for these control systems and their conformity to IEEE Std 603. Full control functionality is included in the design. As an example, the Q-DCIS supports safety system monitoring and operator input to/from the MCR and RSS. Protective actions associated with RPS, neutron monitoring, and the SSLC/ESF can be manually initiated at the system level, in conformance with RG 1.62, and at the division level, in conformance with IEEE Std 603.

In DCD, Tier 1, Sections 2.2.15, 3.2, 3.3, and 3.8 include the DAC/ITAAC for the applicant to verify that the control room functionality is implemented. Accordingly, based on a review of the design bases for control room functions, I&C interfaces, and a review of Tier 1 ITAAC for these functions, the NRC staff finds that the requirements for GDC 19 have been adequately addressed.

(9) GDC 20, “Protection System Functions”

GDC 20 requires that the protection system be designed (1) to initiate automatically the operation of the appropriate systems, including reactivity control systems, to ensure that specified acceptable fuel design limits are not exceeded as a result of AOOs and (2) sense accident conditions and initiate the operation of systems and components important to safety. The NRC staff evaluated whether GDC 20 has been adequately addressed for the DCIS. SRP Table 7-1 identifies that GDC 20 applies to the protection systems (RTS and ESF) (DCD Sections 7.2 and 7.3). SRP Appendix 7.1-A states that GDC 20 is addressed for protection systems by conformance to IEEE Std 603, Sections 4, 5, 5.5, 6.1, 6.8, and 7.1. DCD, Tier 2, Table 7.1-1, identifies that GDC 20 is applicable to the protection systems consistent with SRP Table 7-1. The applicant has committed to following the guidance of RG 1.105 and has provided a setpoint methodology in NEDE-33304P, which is evaluated in Section 7.1.4 of this report. The NRC staff also evaluated, for the protection systems, design-basis requirements, general functional requirements, and system integrity, involving IEEE Std 603, Sections 4, 5, 5.5, 6.1, 6.8, and 7.1, in Sections 7.1.1.3.10, 7.2.3.1, and 7.3.3.1 of this report. DCD, Tier 1, Table 2.2.15-2, includes the DAC/ITAAC for verifying that setpoints of safety functions are defined, determined, and implemented based on the defined setpoint methodology and that the design was completed in compliance with IEEE Std 603. In response to RAI 14.3-265 Supplement 1, which was incorporated in DCD Revision 6, the applicant updated DCD, Tier 1, Tables 2.2.15-1 and 2.2.15-2 to cover applicable requirements of IEEE Std 603. As explained in Section 7.1.1.3.10 of this report, DCD, Tier 1, Section 2.2.15, design description identifies that some IEEE Std 603 criteria do not appear in Table 2.2.15-1 (and therefore do not appear in Table 2.2.15-2) as some IEEE Std 603 criteria do not require ITAAC consistent with NRC

guidance or because the criteria are covered by other non-system ITAAC. Based on the applicant's identification of the necessary protection safety actuation in the design bases for the protection and control systems, and their verification in the DCD Tier 1, DAC/ITAAC, the NRC staff finds that the requirements of GDC 20 have been adequately addressed for the DCIS.

(10) GDC 21, "Protection System Reliability and Testability"

GDC 21 requires that protection systems be designed for high functional reliability and in-service testability commensurate with the safety functions to be performed. The NRC staff evaluated whether GDC 21 had been adequately addressed for the DCIS. SRP Table 7-1 identifies that GDC 21 applies to the RTS and ESF systems and to the supporting systems (DCD Sections 7.2 and 7.3). SRP Appendix 7.1-A states that GDC 21 is addressed for protection systems by conformance to IEEE Std 603 criteria except Sections 5.4, 6.1, and 7.1. DCD, Tier 2, Table 7.1-1, identifies that the guidelines for periodic testing in RG 1.22 and RG 1.118 applies to the protection systems. DCD, Tier 2, Section 7.2.1, describes the conformance of the RPS to IEEE Std 603, which is evaluated in Section 7.2.3.1 of this report. DCD, Tier 2, Section 7.3, describes the conformance of ESF actuation and control systems, VBIF, and all subsystems to IEEE Std 603, which is evaluated in Section 7.3.3.1 of this report. DCD, Tier 1, Table 2.2.15-2, includes the DAC/ITAAC for verifying that the protection systems design was completed in compliance with IEEE Std 603. In particular, DCD, Tier 1, Table 2.2.15-2, includes the DAC/ITAAC for verifying that IEEE Std 603, Sections 5.7 and 6.5, "Capability for Test and Calibration," have been met. DCD, Tier 1, Section 3.2, includes the DAC/ITAAC to verify the implementation of the software development process. In response to RAI 14.3-265, Supplement 1, which was incorporated in DCD Revision 6, the applicant updated DCD, Tier 1, Tables 2.2.15-1 and 2.2.15-2 to cover applicable requirements of IEEE Std 603. As explained in Section 7.1.1.3.10 of this report, DCD, Tier 1, Section 2.2.15, design description identifies that some IEEE Std 603 criteria do not appear in Table 2.2.15-1 (and therefore do not appear in Table 2.2.15-2) as some IEEE Std 603 criteria do not require ITAAC consistent with NRC guidance or because the criteria are covered by other non-system ITAAC. Based on the applicant's identification of the necessary protection safety actuation in the design bases for the protection and control systems, and their verification in the DCD Tier 1, DAC/ITAAC, the NRC staff finds that the requirements of GDC 21 have been adequately addressed for the DCIS.

(11) GDC 22, "Protection System Independence"

GDC 22 requires, in the pertinent part, that protection systems 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. The NRC staff evaluated whether GDC 22 has been adequately addressed for the DCIS. SRP Table 7-1 identifies that GDC 22 applies to the protection systems (RTS and ESF) and supporting systems (DCD Sections 7.2 and 7.3). SRP Appendix 7.1-A states that GDC 22 is addressed for protection systems by conformance to IEEE Std 603, Sections 4, 5.1, 5.3, 5.4, 5.5, 5.6, 6.2, 6.3, 6.8, 7.2, and 8. DCD, Tier 2, Table 7.1-1, identifies that GDC 22 and RG 1.75 apply to the protection systems. DCD, Tier 2, Section 7.2.1, describes the conformance of the RPS to IEEE Std 603, which is evaluated in Section 7.2.3.1 of this report. DCD, Tier 2, Section 7.3, describes the conformance of ESF actuation and control systems, VBIF, and all subsystems to IEEE Std 603, which is evaluated in Section 7.3.3.1 of this report. DCD, Tier 1, Table 2.2.15-2, includes the DAC/ITAAC for verifying that the protection systems design was completed in compliance with IEEE Std 603. In particular, DCD, Tier 1, Table 2.2.15-2, includes the DAC/ITAAC for verifying that IEEE Std 603, Section 5.6, "Independence," has been met. In response to RAI 14.3-265 Supplement 1, which was incorporated in DCD Revision 6, the

applicant updated DCD, Tier 1, Tables 2.2.15-1 and 2.2.15-2 to cover applicable requirements of IEEE Std 603. As explained in Section 7.1.1.3.10 of this report, DCD, Tier 1, Section 2.2.15, design description identifies that some IEEE Std 603 criteria do not appear in Table 2.2.15-1 (and therefore do not appear in Table 2.2.15-2) as some IEEE Std 603 criteria do not require ITAAC consistent with NRC guidance or because the criteria are covered by other non-system ITAAC. Based on the applicant's identification of the necessary protection safety actuation in the design bases for the protection and control systems, and their verification in the DCD Tier 1, DAC/ITAAC, the NRC staff finds that the requirements of GDC 22 have been adequately addressed for the DCIS.

(12) GDC 23, "Protection System Failure Modes"

GDC 23 requires that protection systems be designed to fail into a safe state or into a state demonstrated to be acceptable on some other defined basis, if certain conditions (such as disconnection of the system, loss of energy, or postulated adverse environments) are experienced. The NRC staff evaluated whether GDC 23 has been adequately addressed for the DCIS. SRP Table 7-1 identifies that GDC 23 applies to the protection systems (RTS and ESF) and supporting systems (DCD Sections 7.2 and 7.3). SRP Appendix 7.1-A states that GDC 23 is addressed for protection systems by conformance to IEEE Std 603, Section 5.5. DCD, Tier 2, Table 7.1-1, identifies that GDC 23 applies to the protection systems. DCD, Tier 2, Section 7.1.6.6.1.6, states that the RTIF-NMS platform fails to a tripped state. Hardware and software failures detected by self-diagnostics cause a trip signal to be generated in the RPS division in which the failure occurs. DCD, Tier 2, Section 7.1.6.6.1.6, states that the SSLC/ESF fails to a state where the activated component remains "as-is" to prevent a control-system-induced LOCA. For the same reason, hardware and software failures detected by self-diagnostics do not initiate a signal in a failed SSLC/ESF division. IEEE Std 603, Section 5.5 is implemented in DCD Tier 1 DAC/ITAAC through the EQ DAC/ITAAC in DCD, Tier 1, Section 3.8 and the software development ITAAC in DCD, Tier 1 Section 3.2. Accordingly, based on the conformance to the applicable guidance and IEEE Std 603 and their verification in DCD Tier 1, DAC/ITAAC, the NRC staff finds that the requirements of GDC 23 have been adequately addressed for the DCIS.

(13) GDC 24, "Separation of Protection and Control Systems"

GDC 24 requires that the protection system 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. GDC 24 requires that the interconnection of the protection and control systems be limited so as to assure that safety is not significantly impaired. The NRC staff evaluated whether GDC 24 has been adequately addressed for the DCIS. SRP Table 7-1 identifies that GDC 24 applies to all I&C systems (DCD Sections 7.2 through 7.8). SRP Appendix 7.1-A states that GDC 24 is addressed for protection systems by conformance to IEEE Std 603, Sections 5.1, 5.6, 5.12, 6.3, 6.6, and 8, particularly Sections 5.6 and 6.3. SRP Section 7.7 states that for control systems isolated from safety systems, the applicable IEEE Std 603, Sections are 5.6.3 and 6.3.

DCD, Tier 2, Table 7.1-1, identifies that GDC 24 applies to all I&C systems. DCD, Tier 2, Section 7.1.6.6.1.2 for IEEE Std 603, Section 5.1 states that communication between safety control systems and non-safety control systems is electrically isolated and one-way (which references DCD, Tier 2, Section 7.1.3.3.6). DCD, Tier 2, Section 7.1.3.3 states that safety fiber

optic CIMs provide the safety isolation and separation and are qualified safety components. In RAI 7.1-65, the staff asked the applicant to describe the CIM safety-related functions and how they will be confirmed. RAI 7.1-65 was being tracked as an open item in the SER with open items. In its responses, the applicant clarified that CIMs are safety signal isolation devices and the applicant revised DCD, Tier 1, Table 2.2.15-2, Item 10, to provide DAC/ITAAC to verify that the software project's interdivisional communication systems have optically isolated fiber optical communication pathways. The NRC staff determined the responses were acceptable since the applicant clarified the CIM safety-related functions and how they will be confirmed. Based on the applicant's response, RAI 7.1-65 is resolved. In RAI 7.1-132, the NRC staff requested that the applicant clarify which system contains the trip circuit to cut off power to the N-DCIS and to add this safety trip to the appropriate section of DCD Tier 1. RAI 7.1-132 was being tracked as an open item in the SER with open items. In its response, the applicant clarified the function of the safety Control Room Habitability Area HVAC Subsystem (CRHAVS) emergency trip circuit for the N-DCIS equipment. DCD Tier 1, Tables 2.2.13-2 and 2.2.13-3, DCD, Tier 2, Subsections 6.4.8, 7.3.4.2, and 9.4.1.5 were updated and incorporated in DCD Revision 6. The NRC staff determined the responses were acceptable since the applicant clarified in the DCD the system that contains the trip circuit to cut off power to the N-DCIS. Based on the applicant's response, RAI 7.1-132 is resolved. DCD, Tier 2, Section 7.1.6.6.1, describes conformance to IEEE Std 603, Sections 5.1, 5.12, 6.6, 8.1, 8.2, and 8.3, respectively. In response to RAI 14.3-265, Supplement 1, which was incorporated in DCD Revision 6, the applicant updated DCD Tier 1, Tables 2.2.15-1 and 2.2.15-2 to cover applicable requirements of IEEE Std 603. As explained in Section 7.1.1.3.10 of this report, DCD, Tier 1, Section 2.2.15, design description identifies that some IEEE Std 603 criteria do not appear in Table 2.2.15-1 (and therefore do not appear in Table 2.2.15-2) as some IEEE Std 603 criteria do not require ITAAC consistent with NRC guidance or because the criteria are covered by other non-system ITAAC. Based on the applicant's identification of the necessary protection safety actuation in the design bases for the protection and control systems and their verification in the DCD Tier 1, DAC/ITAAC, the NRC staff finds that the requirements of GDC 24 have been adequately addressed for the DCIS.

(14) GDC 25, "Protection System Requirements for Reactivity Control Malfunctions"

GDC 25 requires that the protection system be designed to assure that specified acceptable fuel design limits are not exceeded for any single malfunction of the reactivity control systems, such as accidental withdrawal (not ejection or dropout) of control rods. The NRC staff evaluated whether GDC 25 has been adequately addressed for the DCIS. SRP Table 7-1 identifies that GDC 25 applies to the RPS and control system interlock logic (DCD Sections 7.2 and 7.6). SRP Appendix 7.1-A states that GDC 25 is addressed for protection systems by conformance to IEEE Std 603, Section 4, which is associated with safety system design-basis requirements. DCD, Tier 2, Section 7.2.1, provides the design bases for the RPS that include protection from abnormal operational occurrences, such as continuous control rod withdrawal. DCD, Tier 2, Chapter 15, includes an analysis for continuous rod withdrawal in several scenarios to show that the RPS is designed to prevent fuel design limits from being exceeded. In DCD, Tier 1, Tables 2.2.1-6 and 2.2.7-4 provide the ITAAC for verification of these reactor protection functions. In response to RAI 14.3-265 Supplement 1, which was incorporated in DCD Revision 6, the applicant updated DCD, Tier 1, Tables 2.2.15-1 and 2.2.15-2 to cover applicable requirements of IEEE Std 603. As explained in Section 7.1.1.3.10 of this report, DCD, Tier 1, Section 2.2.15, design description identifies that IEEE Std 603, Criteria 4.2, 4.3, 4.10, 4.11, and 4.12, are not included as ITAAC because NUREG 0800, Section 14.3.5, and RG 1.206, Section C.II.1, do not include these criteria as ITAAC. DCD, Tier 2, Section 7.1.6.6.1.1 describes how IEEE Std 603, Criteria 4.2, 4.3, 4.10, 4.11, and 4.12 are already addressed in the DCD. The NRC staff finds the explanation of IEEE Std 603, Criteria 4.2, 4.3, 4.10, 4.11, and

4.12 and their exclusion from the ITAAC acceptable. Based on the applicant's identification of the necessary protection safety actuation in the design bases for the protection and control systems and their verification in the DCD Tier 1, DAC/ITAAC, the NRC staff finds that the requirements of GDC 25 have been adequately addressed for the DCIS.

(15) GDC 28, "Reactivity Limits"

GDC 28 requires that reactivity control systems be designed with appropriate limits on the potential amount and rate of reactivity increase. The NRC staff evaluated whether GDC 28 has been adequately addressed for the DCIS. SRP Table 7-1 identifies that GDC 28 applies to I&C interlock logic and control systems (DCD Sections 7.6 and 7.7). SRP Appendix 7.1-A states that GDC 28 imposes functional requirements on I&C interlock and control systems to the extent they are provided to limit reactivity increases to prevent or limit the effect of reactivity accidents. In DCD, Tier 2, Sections 7.7.2 and 7.7.6 state that the RC&IS and NMS conform to GDC 28. DCD, Tier 2, Sections 7.7.2 and 7.7.6 and DCD, Tier 2, Chapter 15, Table 15.1-5 and Table 15.1-6 identify RC&IS actuations and other actions that reduce the need for the actuation of protection and safety systems to mitigate AOOs. DCD, Tier 2, Section 7.7.2, includes corresponding actions in the design bases of the RC&IS to provide appropriate limits on the potential amount and rate of increase in reactivity. In particular, DCD, Tier 2, Section 7.7.2.2.7.4, identifies the control rod block functions performed by the RC&IS. DCD, Tier 2, Section 7.7.6, describes the MRBM, which monitors more than one region of the core and provides input to the RC&IS. DCD, Tier 1, Section 2.2.1, includes the ITAAC for the applicant to verify that the as-built RC&IS implements these actions. Accordingly, based on identified RC&IS actions and their verification in the ITAAC, the NRC staff finds that the requirements of GDC 28 have been adequately addressed for these non-safety systems.

(16) GDC 29, "Protection Against Anticipated Operational Occurrences"

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. The NRC staff evaluated whether GDC 29 has been adequately addressed for the DCIS. SRP Table 7-1 identifies that GDC 29 applies to the protection systems, control systems, and supporting systems (DCD Sections 7.2, 7.3, and 7.7). SRP Appendix 7.1-A states that GDC 29 is addressed by conformance, as applicable, to GDC 20–25 and GDC 28. In DCD, Tier 2, Table 7.1-1 and Sections 7.2 and 7.7 identify that GDC 29 applies to the applicable RPS and control systems. However, in DCD Tier 2, Table 7.1-1 and Section 7.3 do not identify that GDC 29 applies to the applicable ESF actuation and control systems, VBIF, and all subsystems. In RAI 7.3-14, the NRC staff asked the applicant to clarify the applicability of GDC 29. RAI 7.3-14 was being tracked as an open item in the SER with open items. In its response to RAI 7.3-14, the applicant stated that it would address conformance to GDC 29 in the response to RAI 7.1-99. Responses to RAI 14.3-265, RAI 14.3-265, Supplement 1, RAI 7.1-99, 7.1-100, and 7.1-101, that corrected the inconsistence's in DCD Tier 1 and Tier 2, were incorporated in DCD Revision 6. Table 7.1-1 was updated to cover all applicable criteria including GDC for all safety-related systems. The staff determined that the response to RAI 7.3-14 was acceptable, as augmented by the response to RAI 7.1-99, since the applicant clarified the applicability of GDC 29. Based on the applicant's responses, RAI 7.3-14 is resolved. Based on the applicant's identification of the necessary protection safety actuation in the design bases for the protection and control systems, their verification in the DCD Tier 1, DAC/ITAAC, and that the DCIS complies with GDC 20-25 and 28 as discussed above, the NRC staff finds that the requirements of GDC 29 have been adequately addressed for the DCIS.

(17) GDC 33, “Reactor Coolant Makeup”

GDC 33 requires a system to supply reactor coolant makeup for protection against small breaks in the RCPB. SRP Appendix 7.1-A states that GDC 33 imposes functional requirements on the ESF I&C systems provide to initiate, control, and protect the integrity of reactor coolant makeup systems for protection against small breaks in the RCPB. GDC 33 also requires that necessary I&C systems be operable using either onsite or offsite power (assuming only one source is available). DCD, Tier 2, Section 3.1.4.4, states that GDC 33 is applicable to the CRDHS, described in DCD, Tier 2, Section 4.6.1.2.4; the ICS, described in DCD, Tier 2, Section 5.4.6; and the ADS and GDCS, described in DCD, Tier 2, Section 6.3. The CRDHS is non-safety. In DCD, Tier 2, Sections 7.4.4 (ICS) and 7.3.1 (ADS and GDCS) identify the corresponding reactor coolant makeup initiation, control, and protection functions in the design bases. The performance and reliability requirements of GDC 33 are addressed by the applicability of IEEE Std 603 to the ICS, ADS, and GDCS. In particular, Sections 5.1, 5.7, and 6.5 of IEEE Std 603 provide requirements for single failures and testability. Conformance of these systems to IEEE Std 603 are evaluated in Sections 7.4 and 7.3 of this report. In DCD, Tier 1, Sections 2.2.15, 3.2, 3.3, and 3.8 include the DAC/ITAAC for the applicant to verify that the ICS, ADS, and GDCS designs implement these design bases and conform to IEEE Std 603. DCD, Tier 2, Section 8.1.3, states that the Q-DCIS, which includes the ICS, ADS, and GDCS I&C systems, is powered by the safety 250-volts direct current (VDC) power distribution system, normally, or by the safety batteries for 72 hours if normal power is lost. Therefore, these systems are operable using either onsite or offsite power (assuming only one source is available). The safety 250-VDC power distribution system, including batteries, is evaluated in Chapter 8 of this report. Accordingly, based on the applicant’s identification of necessary reactor coolant makeup functions in the design bases of the ICS, ADS, and GDCS and their verification in the DCD Tier 1, DAC/ITAAC, the NRC staff finds that the requirements of GDC 33 have been adequately addressed for the DCIS.

(18) GDC 34, “Residual Heat Removal”

GDC 34 requires a system to remove residual heat. SRP Appendix 7.1-A states that GDC 34 imposes functional requirements on the ESF, safe-shutdown, and interlock I&C systems provided to initiate, control, and protect the integrity of residual heat removal systems. GDC 34 also requires that the necessary I&C systems be operable using either onsite or offsite power (assuming only one source is available). DCD, Tier 2, Section 3.1.4.5, states that GDC 34 is applicable to the ICS, described in DCD, Tier 2, Section 5.4.6. DCD, Tier 2, Section 7.4.4, identifies the corresponding residual heat removal initiation, control, and protection functions in the design bases. The performance and reliability requirements of GDC 34 are addressed by the application of IEEE Std 603 to the ICS. In particular, Sections 5.1, 5.7, and 6.5 of IEEE Std 603, provide requirements for single failures and testability. Conformance of the ICS to IEEE Std 603 is evaluated in Section 7.4 of this report. In DCD, Tier 1, Sections 2.2.15, 3.2, 3.3, and 3.8 include the DAC/ITAAC for the applicant to verify that the ICS design implements these design bases and conforms to IEEE Std 603. DCD, Tier 2, Section 8.1.3, states that the Q-DCIS, which includes the ICS I&C system, is normally powered by the safety 250-VDC power distribution system, or, if normal power is lost, by the safety batteries for 72 hours. Therefore, these systems are operable using either onsite or offsite power (assuming only one source is available). The safety 250-VDC power distribution system, including batteries, is evaluated in Chapter 8 of this report. Accordingly, based on the applicant’s identification of the necessary residual heat removal functions in the design bases of the ICS and their verification in the DCD Tier 1, DAC/ITAAC, the NRC staff finds that the requirements of GDC 34 have been adequately addressed for the DCIS.

(19) GDC 35, “Emergency Core Cooling”

GDC 35 requires a system to provide abundant emergency core cooling. SRP Appendix 7.1-A states that GDC 35 imposes functional requirements on the ESF, safe-shutdown, and interlock I&C systems provided to initiate, control, and protect the integrity of ECCS. GDC 35 also requires that the necessary I&C systems be operable using either onsite or offsite power (assuming only one source is available). DCD, Tier 2, Section 3.1.4.6, states that GDC 35 is applicable to the ECCS, including the ICS, the SLC system, GDCS, and ADS, as described in DCD, Tier 2, Section 6.3. In DCD, Tier 2, Sections 7.4.4 (ICS), 7.4.1 (SLC System), and 7.3.1 (ADS and GDCS) identify the corresponding ECCS initiation, control, and protection functions in the design bases. The performance and reliability requirements of GDC 35 are addressed by the application of IEEE Std 603 to the ECCS. In particular, Sections 5.1, 5.7, and 6.5 in IEEE Std 603 provide requirements for single failures and testability. Conformance of the ECCS to IEEE Std 603 is evaluated in Sections 7.4 (ICS and SLC System) and 7.3 (ADS and GDCS) of this report. In DCD, Tier 1, Sections 2.2.15, 3.2, 3.3, and 3.8 include the DAC/ITAAC for the applicant to verify that the ECCS designs implement these design bases and conform to IEEE Std 603. DCD, Tier 2, Section 8.1.3, states that the Q-DCIS, which includes the ICS, the SLC system, GDCS, and ADS I&C systems, is normally powered by the safety 250-VDC power distribution system, or, if power is lost, by safety batteries for 72 hours. Therefore, these systems are operable using either onsite or offsite power (assuming only one source is available). The safety 250-VDC power distribution system, including batteries, is evaluated in Chapter 8 of this report. Accordingly, based on the applicant’s identification of the necessary ECCS functions in the design bases of the ICS, SLC system, ADS, and GDCS and their verification in the DCD Tier 1, DAC/ITAAC, the NRC staff finds that the requirements of GDC 35 have been adequately addressed for the DCIS.

(20) GDC 38, “Containment Heat Removal”

GDC 38 requires a system to remove heat from the reactor containment. SRP Appendix 7.1-A states that GDC 38 imposes functional requirements on the ESF, safe-shutdown, and interlock I&C systems provided to initiate, control, and protect the integrity of containment heat removal systems. GDC 38 also requires that the necessary I&C systems be operable using either onsite or offsite power (assuming only one source is available). DCD, Tier 2, Section 3.1.4.9, states that GDC 38 is applicable to the PCCS, described in DCD, Tier 2, Section 6.2.2. In DCD, Tier 2, Sections 6.2.2 and 7.3.2 state that the PCCS does not have instrumentation, control logic, or power-actuated valves and does not need or use electrical power for its operation in the first 72 hours after a LOCA. While the PCCS has no instrumentation and controls (I&C) functions, it does rely on I&C functions in other systems, namely the ICS, SSLC/ESF, and FAPCS to perform its safety functions. In RAI 7.1-140, the NRC staff requested the applicant to clarify the active components, electrical motive power, and I&C functions needed for the PCCS to perform its safety functions, including supporting functions provided by other systems. RAI 7.1-140 was being tracked as an open item in the SER with open items. In its response, the applicant clarified that the PCCS relies on the water in the Equipment Storage Pool and Reactor Well to perform its safety functions for 72 hours. Pool cross-connect valves are active components that open to allow water in the Equipment Storage Pool and Reactor Well to flow into the IC/PCCS pools. FAPCS provides four safety-related level sensors in each IC/PCCS inner expansion pool. The cross-connect valves are opened when a low level condition is detected by the sensors in either pool. FAPCS also provides four non-safety level sensors in each inner expansion pool which are used by DPS to open the cross-connect valves. The air operated cross-connect valves require pneumatic and electrical motive power to open, which is

provided by a pneumatic accumulator, and the safety-related Uninterruptible Power System. The squib cross-connect valves are opened pyrotechnically and need only electrical motive power to open, which is provided by the safety-related Uninterruptible Power System. The response modified multiple sections of the DCD Tier 2, including Sections 7.4.4.3, 7.5.5, and 7.8.1.2.5, to address these clarification. The staff determined the response was acceptable since the applicant identified the necessary support systems and function for the PCCS to perform its safety functions. Based upon the applicant's response, RAI 7.1-140 is resolved.

As noted above, the response to RAI 7.1-140 added containment heat removal initiation, control, and protection functions to the design bases in sections DCD, Tier 2, Sections 7.4.4.3 (ICS). The performance and reliability requirements of GDC 38 are addressed by the application of IEEE Std 603 to the ICS. In particular, Sections 5.1, 5.7, and 6.5 of IEEE Std 603, provide requirements for single failures and testability. Conformance of the ICS to IEEE Std 603 is evaluated in Section 7.4 of this report. DCD, Tier 1, Sections 2.2.15, 3.2, 3.3, and 3.8 include the DAC/ITAAC for the applicant to verify that the ICS design implements these design bases and conforms to IEEE Std 603. DCD, Tier 2, Section 8.1.3, states that the QDCIS, which includes the ICS I&C system, is normally powered by the safety 250-VDC power distribution system, or, if normal power is lost, by the safety batteries for 72 hours. Therefore, these systems are operable using either onsite or offsite power (assuming only one source is available). The safety 250-VDC power distribution system, including batteries, is evaluated in Chapter 8 of this report. Accordingly, based on the applicant's identification of the necessary containment heat removal functions in the design bases of the ICS and their verification in the DCD Tier 1, DAC/ITAAC, the NRC staff finds that the requirements of GDC 38 have been adequately addressed for the DCIS.

(20) GDC 41, "Containment Atmosphere Cleanup"

GDC 41 requires systems to control fission products, hydrogen, oxygen, and other substances which may be released into the reactor containment. SRP Appendix 7.1-A states that GDC 41 imposes functional requirements on the ESF and interlock I&C systems provided to initiate, control, and protect the integrity of containment atmosphere cleanup systems. GDC 41 also requires that the necessary I&C systems be operable using either onsite or offsite power (assuming only one source is available). The NRC staff evaluated whether GDC 41 has been adequately addressed for the DCIS. SRP Table 7-1 identifies that GDC 41 applies to the ESF and interlock I&C systems (DCD Sections 7.3 and 7.6). DCD, Tier 2, Section 6.5.4, states that the suppression pool performs a fission product cleanup function in conformance with GDC 41. However, this function does not require any I&C functions. DCD, Tier 2, Section 6.2.5.1, states that safety combustible gas control is provided by an inerted containment; therefore, GDC 41 is not applicable to the design for this function. The evaluation of the containment atmosphere cleanup systems with regard to GDC 41 is provided in Section 6.5 of this report. Accordingly, based on atmospheric cleanup systems not requiring any I&C functions, the NRC staff finds that the requirements of GDC 41 are not applicable to the I&C design.

(21) GDC 44, "Cooling Water"

GDC 44 requires a system to transfer heat from structures, systems, and components (SSC) important to safety, to an ultimate heat sink. According to SRP Appendix 7.1-A, GDC 44 imposes functional requirements on the ESF, interlock, and control I&C systems provided to initiate, control, and protect the integrity of cooling water systems important to safety that transfer heat to the ultimate heat sink. GDC 44 also requires that necessary I&C systems be operable using either onsite or offsite power (assuming only one source is available). In DCD,

Tier 2, Sections 3.1.4.15 and 9.2.5 state that the IC/PCCS pools are the ultimate heat sink. These sections also state that the IC/PCCS pools have no active components and do not require I&C functions to perform their safety function of transferring heat to the atmosphere. Accordingly, because the ultimate heat sink cooling water does not require any I&C functions, the NRC staff finds that the requirements of GDC 44 are not applicable to the I&C design.

7.1.1.3.7 NRC Staff Requirement Memorandum Issues

SECY-93-087, identified two digital I&C-related issues designated as SRM issues:

(1) SRM to SECY-93-087, Item II.Q, "Defense Against Common - Mode Failures in Digital Instrumentation and Control Systems"

(2) SRM to SECY-93-087, Item II.T, "Control Room Annunciator (Alarm) Reliability"

The NRC staff evaluated whether the guidelines of SRM to SECY-93-087, Item II.Q, have been adequately addressed for the DCIS. SRP Table 7-1 identifies that the SRM to SECY-93-087, Item II.Q, applies to the protection systems, ESF actuation systems, control systems, and the DPS (DCD Sections 7.2, 7.3, 7.7, and 7.8).

DCD, Tier 2, Table 7.1-1, identifies that the SRM to SECY-93-087, Item II.Q, applies to the applicable systems. NEDO-33251 provides the primary assessment of conformance to the guidelines of SRM to SECY-93-087, Item II.Q, along with BTP HCIB-19. The NRC staff positions on Item II.Q and NRC staff evaluation of the D3 assessment are documented in Section 7.1.3 of this report.

The NRC staff evaluated whether the guidelines of SRM to SECY-93-087, Item II.T, have been adequately addressed for the DCIS. SRP Table 7-1 identifies that the SRM to SECY-93-087, Item II.T, applies to information systems important to safety and supporting systems (DCD Section 7.5).

The NRC staff position in Item II.T is as follows: (1) The annunciator system is considered to consist of sets of alarms (which may be displayed on tiles, VDUs, or other devices) and sound equipment; logic and processing support; and functions to enable operators to silence, acknowledge, reset, and test alarms, (2) The MCR should contain compact, redundant operator workstations with multiple display and control devices that provide organized, hierarchical access to alarms, displays, and controls. Each workstation should have the full capability to perform MCR functions as well as support division of tasks between two operators, (3) The display and control features should be designed to satisfy existing regulations, for example, separation and independence requirements for Class 1E circuits (IEEE Std 384-1992, "IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits,") and specifications for manual initiation of protective actions at the systems level per RG 1.62. The designer should use existing defensive measures (e.g., segmentation, fault tolerance, signal validation, self-testing, error checking, supervisory watchdog programs), as appropriate, to assure that alarm, display, and control functions provided by the redundant workstations meet these criteria, and (4) Alarms that are provided for manually controlled actions for which no automatic control is provided, and that are required for the safety systems to accomplish their safety functions, should meet the applicable specifications for Class 1E equipment and circuits.

DCD, Tier 2, Table 7.1-1, identifies that the SRM to SECY-93-087, Item II.T, applies to applicable information systems important to safety, the Q-DCIS and the N-DCIS. DCD, Tier 2,

Section 7.1.6.3, states that the AMS follows guidance in the SRM to SECY-93-087, Item II.T, for redundancy, independence, and separation, because the "alarm system" is considered redundant (i.e., includes redundant features). Alarm points are sent through dual networks to redundant message processors on dual power supplies. The processors are dedicated only to performing alarm processing. The alarms are displayed on multiple independent VDUs that each have dual power supplies. The alarm tiles, or their equivalent, are driven by redundant datalinks (with dual power). There are redundant alarm processors. There are no alarms that require manually controlled actions for safety systems to accomplish their function. Thus, the requirements for safety equipment and circuits are not applicable.

SRP Appendix 7.1-A states that alarms that are provided for manually controlled action for which no automatic control is provided, and that are required for the safety systems to accomplish their safety function, should meet the applicable specifications for Class 1E equipment and circuits. Because the design is a passive plant, all the safety systems are initiated automatically. There is no preplanned manual controlled action required for the safety systems. The NRC staff finds that the exception documented in DCD, Tier 2, Section 7.1.6.3 and Table 1.9-7 (alarm is not classified as Class 1E equipment or circuits) is acceptable. Section 7.5 of this report provides a further evaluation of alarm (annunciator) systems, In addition, in DCD, Tier 1, Sections 2.2.15, 3.2, 3.3, 3.7, and 3.8 include the DAC/ITAAC for the applicant to verify that the I&C systems design conforms to the applicable regulations. Based on the above, the NRC staff finds that the guidelines of SRM to SECY-93-87, Item II.T, have been adequately addressed for the DCIS.

7.1.1.3.8 Regulatory Guides

In DCD, Tier 2, Table 7.1-1, the applicant identified the applicable regulatory requirements, including the applicable RGs, for each of the DCIS systems. DCD, Tier 2, Table 7.1-1, identifies that the RGs applies to the applicable systems identified in SRP Table 7.1 with the exception for 4 RGs: 1.174, 1.177, 1.189, and 1.200. A general discussion of differences in applicability between DCD, Tier 2, Table 7.1-1 and SRP Table 7.1 is provided in Section 7.1.1.3.2 of this report.

SRP Table 7.1 does not identify any applicability for RGs 1.174, 1.177, and 1.200 but refers to BTP HCIB-12 instead. HCIB-12 identifies that RGs 1.174, 1.177, and 1.200 provide guidance for using a risk informed approach to evaluate changes to instrument calibration and surveillance test intervals for reasons other than a 24-month fuel cycle. DCD, Tier 2, Table 1.9-21 identifies that these RGs are not applicable to the design certification but indicate that they may be used by COL holders. Accordingly, the applicant does not apply these approaches to the design for calibration intervals, which the NRC staff finds acceptable.

SRP Table 7.1 identifies that RG 1.189 is applicable to SAR Chapter 7.4. SRP Section 7.4 identifies RG 1.189 as a reference and discusses RG 1.189 in a footnote concerning remote shutdown capability and the assumptions to be used in the case smoke from a fire requires the evacuation of the MCR. The footnote also states that conformance to RG 1.189 is evaluated with SRP Section 9.5.1. DCD, Tier 2, Section 9.5.1, describes conformance of the fire protection program to RG 1.189, which is evaluated in Section 9.5.1 of this report. Accordingly, the NRC staff finds the above approach acceptable.

In DCD, Tier 2, Table 1.9-21b, no exceptions have been identified to I&C-related RGs. DCD, Tier 2, Table 1.9-7, identifies differences with the SRPs with regard to RGs 1.22, 1.118, and 1.151.

DCD, Tier 2, Table 1.9-7, identifies that some actuators and digital sensors, because of their locations, cannot be fully tested during actual reactor operation in conformance with RG 1.22. DCD, Tier 2, Section 7.1.6.4, states that such equipment is identified and provisions for meeting the guidance of Paragraph D.4 (per BTP HCIB-8) are discussed in the Safety Evaluation of DCD, Tier 2, Sections 7.2 through 7.8. In DCD, Tier 2, Sections 7.2.1.3.4, 7.3.1.1.3.4, 7.3.1.2.3.4, and 7.3.6.3.4, identify alternatives to full system testing during reactor operations for the RPS, ADS, GDCS, and VBIF system, respectively.

In RAI 7.3-17, the NRC staff requested the applicant to describe how the VBIF conforms to RG 1.22 and HICB-8. This question was raised since the DCD Section 7.3.6.4 states that VB isolation function equipment inside containment is tested during refueling outages but does not state why it is not practicable to test during reactor operation. RG 1.22 provides guidelines for justifying not testing actuated equipment during reactor operations. RAI 7.3-17 was being tracked as an open item in the SER with open items. In its response, the applicant modified the DCD to specify VBIF testing during reactor operation consistent with RG 1.22, which addresses HICB-8. The staff determined the response was acceptable since the applicant clarified conformance to RG 1.22. Based on the applicant's response, RAI 7.3-17 is resolved.

Consistent with RG 1.22, Regulatory Position D.4, the applicant has shown for the RPS, ADS, and GDCS, that there is no practicable system design that would permit operation of the actuated equipment without adversely affecting the safety or operability of the plant. For example, testing during operation would result in reactor scram or releases from the RCPB. The alternative testing includes: (1) testing the RPS in overlapping stages (2) testing the ADS and GDCS components during outages, and (3) testing of the ADS and GDCS (described in DCD, Tier 2, Section 6.3.2.7.4) squib initiators in a laboratory after removal from the squib valves. The NRC staff finds these alternative testing approaches consistent with RG 1.22 Regulatory Position D.4 and therefore acceptable.

DCD, Tier 2, Table 1.9-7, identifies clarifications and testing exceptions to RG 1.118. DCD, Tier 2, Section 7.3.1.1.3.4, identifies that a full functional test of the ADS is not practical, because a LOCA results if the non re-closable DPVs are opened. Acceptable reliability of equipment operation is demonstrated by alternate test methods. System logic is periodically self-tested, and initiating circuits are continuously monitored. DPV valve initiators periodically are removed and test-fired in a laboratory. RPV level transmitters are located outside containment, so calibration verification can be performed during plant operation. The NRC staff finds this acceptable.

DCD, Tier 2, Table 1.9-7, identifies that RG 1.151 is not applicable to the SB&PC system and the N-DCIS. DCD, Tier 2, Section 7.1.5.3.4, identifies that the N-DCIS receives signals from sensors in various systems in the plant that are from instrument sensing lines from non-safety instrumentation but the N-DCIS itself does not contain instrument sensing lines. DCD, Tier 2, Section 7.7.5.3.3 identifies that the SB&PC system receives pressure signals from sensors in the NBS and the Main Condenser and Auxiliaries System but does not itself contain instrument sensing lines. The NRC staff finds this acceptable.

7.1.1.3.9 Branch Technical Positions

In DCD, Tier 2, Table 7.1-1, the applicant identifies the applicable regulatory requirements and guidance, including the applicable SRP BTPs, for each of the DCIS systems. The NRC staff compares DCD, Tier 2, Table 7.1-1, with SRP Table 7.1, in the SRP and finds that the applicant

has either documented the applicability of the guidance or addressed any exceptions, as discussed in Section 7.1.1.3.3 of this report.

In DCD, Tier 2, Table 1.9-7, the applicant states that the approach to software management and quality assurance complies with the intent of the SRP and BTP HCIB-14, but is implemented in a set of acceptable equivalent alternative and mutually consistent plans, which applied in total, comprise the general requirements. The NRC staff's review of software development activities is addressed in Section 7.1.2 of this report. DCD, Tier 1, Section 3.2, documents the DAC/ITAAC for the software development process. DCD, Tier 2, Section 7.1.6.5, generally discusses the conformance of the design to the BTPs listed in DCD, Tier 2, Table 7.1-1. This report discusses conformance to BTPs throughout Chapter 7. The NRC staff finds that the applicant has adequately addressed conformance with the listed SRP BTPs for the DCIS.

7.1.1.3.10 IEEE Standard 603 Requirements

The NRC staff evaluated whether the applicant has adequately addressed all the criteria listed in IEEE Std 603, as required by 10 CFR 50.55a(h)(3). As discussed in Section 7.1.1.3.1 of this report, the applicant is using the DAC approach to comply with IEEE Std 603 requirements. To implement this approach, the NRC staff evaluated whether the applicant specified conformance to IEEE Std 603, consistent with the acceptance criteria in SRP Appendix 7.1-C. The NRC staff also evaluated whether sufficient DAC were included in DCD Tier 1 to confirm that the completed design meets IEEE Std 603 requirements.

The NRC staff also evaluated, in parallel, whether additional applicable guidance in IEEE Std 7-4.3.2 for safety systems using digital programmable computers has been addressed. The NRC staff used the acceptance criteria in SRP Appendix 7.1-D for criteria related to IEEE Std 7-4.3.2. However, in RAI 7.1-99, Item D, the NRC staff requested that IEEE Std 7-4.3.2 criteria not already covered by the DAC/ITAAC in DCD, Tier 1, Sections 2.2.15 or 3.2, be included in that DAC/ITAAC. RAI 7.1-99 was being tracked as an open item in the SER with open items. In its response to RAI 14.3-265, Supplement 1, and RAI Numbers 7.1-99, 7.1-100, and 7.1-101, all of which were incorporated in DCD Revision 6, the applicant corrected the inconsistent documentation in DCD Tier 1 and Tier 2. DCD, Tier 1, Table 2.2.15-1, was updated to include applicable IEEE Std 603 criteria for all safety I&C systems. Table 2.2.15-2, identifies design commitment to each IEEE Std 603 criterion for the software projects. As explained in Section 7.1.1.3.10 of this report, DCD, Tier 1, Section 2.2.15, design description identifies that some IEEE Std 603 criteria do not appear in Table 2.2.15-1 (and therefore do not appear in Table 2.2.15-2) as some IEEE Std 603 criteria do not require ITAAC consistent with NRC guidance or because the criteria are covered by other non-system ITAAC. The ITAAC acceptance criteria contain two phases: (a) DAC phase that specifies the software projects design requirements, and (b) ITAAC implementation phase that specifies the methods to verify that the as-built design has satisfied the IEEE Std 603 requirements. Key changes to Tier 2 included significantly augmenting the discussion of compliance with IEEE STD 603 sections in DCD, Tier 2, Section 7.1.6.6.1, revising DCD Tier 2, Table 7.1.1 and 7.1.2 to more clearly show conformance to regulatory requirements and IEEE Std 603, and making revisions to use a consistent designation of systems and their conformance to requirements and guidelines throughout Chapter 7. Based on the review of DCD, Tier 1, Sections 2.2.15, 3.2 and the information referenced by DCD, Tier 2, Table 7.1-2, the NRC staff finds that the DCD has properly addressed the IEEE Std 7-4.3.2 compliance. Based on the above and the applicant's response, RAIs 14.3-265, 7.1-99, 7.1-100, and 7.1-101 are resolved.

DCD, Tier 2, Table 7.1-2, identifies specific sections of DCD Chapters 7 where compliance with IEEE Std 603 is discussed.

7.1.1.3.10.1 IEEE Standard 603, Section 4, "Safety System Designation"

The NRC staff evaluated whether IEEE Std 603, Section 4, was adequately addressed using SRP Appendix 7.1-C, Section 4. IEEE Std 603 states that, "The [safety system] design basis shall also be available as needed to facilitate the determination of the adequacy of the safety system design." SRP Appendix 7.1-C, Section 4, identifies characteristics that the safety system design basis should exhibit: completeness, consistency, correctness, traceability, unambiguity, and verifiability. For the completeness characteristic, SRP Appendix 7.1-C states, "As a minimum each of the design basis aspects identified in IEEE Std 603, Clauses [i.e., Sections] 4.1 through 4.12 should be addressed." DCD, Tier 2, Section 7.1.6.6.1.1, provides a general discussion of conformance to IEEE Std 603, Section 4, and identifies several sections where high level safety system functional information is provided. DCD, Tier 2, Table 1.3-1, defines the reactor system design characteristics. Tables 15.0-3, 15.0-4, 15.0-5, and 15.0-6 define the safety analysis acceptance criteria for the AOOs, infrequent events, special events, and accidents. Table 15.1-2 defines the operating modes for the entire operating envelope. Table 15.1-3 defines the abnormal events with applicable operating modes. Table 15.2-1 defines the input parameters, initial conditions and bounding limits for ATWS events and infrequent events. Table 15.5-2 defines the initial conditions and bounding limits for ATWS events. Credited systems, interlocks, and functions for each DBE are described in DCD, Tier 2, Sections 15.2, 15.3, 15.4 and 15.5. Safety system design basis descriptions are documented in various sections of DCD, Tier 2, Chapter 7, Sections 7.2 through 7.5.

The NRC staff evaluated whether IEEE Std 603, Section 4.1, has been adequately addressed for the safety systems. This criterion requires the identification of the DBEs applicable to each mode of operation, along with the initial conditions and allowable limits of plant conditions for each such event. The information to be provided should be consistent with the analysis in DCD, Tier 2, Chapter 15. The analysis should include how the Q-DCIS automatically initiates appropriate protective action when a condition monitored by the system reaches a preset level. DCD, Tier 2, Section 7.1.6.6.1.1, provides a general discussion of conformance to Section 4 and identifies several sections where high level safety system functional information is provided. DCD, Tier 1, Table 2.2.15-2 provides DAC/ITAAC for IEEE Std 603, Section 4.1 to verify that DBE information is incorporated into software projects during the software lifecycle process. Based on the review of DCD, Tier 2, Chapter 15 tables listed above and the review of DCD, Tier 1, Section 2.2.15, DAC/ITAAC verification, the NRC staff finds that Section 4.1 of IEEE Std 603 has been adequately addressed.

The NRC staff evaluated whether IEEE Std 603, Section 4.2, has been adequately addressed for the safety systems. This criterion requires the identification of the safety functions and corresponding protective actions of the execute features for each DBE as part of the design basis. DCD, Tier 2, Section 7.1.6.6.1.1, provides a general discussion of conformance to IEEE Std 603, Section 4, and identifies several sections where high level safety system functional information is provided. DCD, Tier 2, Table 15.1-6, defines the automatic safety instrument trips in response to each event. Safety design bases for each system are discussed in DCD, Tier 2, Chapter 7. Consistent with RG 1.206, DAC/ITAAC are not provided for IEEE Std 603, Section 4.2 as the information is provided in the DCD and the IEEE STD 603, Section 4 criteria with DAC/ITAAC adequately verify the design basis information. Based on the review of the DCD, Tier 2, Chapter 7 documentation and the review of DCD, Tier 1, Section 2.2.15, DAC/ITAAC verification, and the staff's safety evaluation for each applicable system provided in

this report as part of conformance to 10 CFR 50.55a(h), the NRC staff finds that Section 4.2 of IEEE Std 603 has been adequately addressed.

The NRC staff evaluated whether IEEE Std 603, Section 4.3, has been adequately addressed for the safety systems. This criterion requires the identification of the permissive conditions for each operating bypass capability that is to be provided. The permissive conditions for each operating bypass for each system are discussed in DCD, Tier 2, Chapter 7. Consistent with RG 1.206, DAC/ITAAC are not provided for IEEE Std 603, Section 4.3 as the information is provided in the DCD and the IEEE STD 603, Section 4 criteria with DAC/ITAAC adequately verify the design basis information. Based on the review of the DCD, Tier 2, Chapter 7 documentation and the review of DCD, Tier 1, Section 2.2.15, DAC/ITAAC verification, and the staff's safety evaluation for each applicable system provided in this report as part of conformance to 10 CFR 50.55a(h), the NRC staff finds that Section 4.3 of IEEE Std 603 has been adequately addressed.

The NRC staff evaluated whether IEEE Std 603, Section 4.4, has been adequately addressed for the safety systems. This criterion requires the identification of variables or combinations of variables, or both, that are to be monitored to manually or automatically, or both, control each protective action; the analytical limit associated with each variable, the ranges (normal, abnormal, and accident conditions); and the rates of change of these variables to be accommodated until proper completion of the protective action is ensured. The list of such variables to be monitored is determined as part of the HFE design process described in DCD Chapter 18. The variables that are associated with each event are discussed in the relevant subsection describing the event as defined in DCD, Tier 2, Table 15.1-7. DCD, Tier 1, Table 2.2.15-2 provides DAC/ITAAC for IEEE Std 603, Section 4.4 to verify that monitored variables are incorporated into software projects during the software lifecycle process. Based on the review of the DCD, Tier 2, Chapters 7 and 15 documentation and the review of DCD, Tier 1, Section 2.2.15, DAC/ITAAC verification, the NRC staff finds that Section 4.4 of IEEE Std 603 has been adequately addressed.

The NRC staff evaluated whether IEEE Std 603, Section 4.5, has been adequately addressed for the safety systems. This criterion describes the minimum criteria under which manual initiation and control of protective actions may be allowed. 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. In DCD, Tier 2, Section 7.1.6.6.1.1, the applicant committed that the software projects design bases includes (1) the points in time and the plant conditions during which manual control is allowed, (2) the justification for permitting initiation or control subsequent to initiation solely by manual means, (3) the range of environmental conditions imposed upon the operator during normal, abnormal, and accident conditions throughout which the manual operations will be performed, and (4) the variables that will be display for the operator to use in taking manual action. DCD Tier 1, Table 2.2.15-2 provides DAC/ITAAC for IEEE Std 603, Section 4.5 to verify that manual initiation and control information is incorporated into software projects during the software lifecycle process. Based on the review of the DCD, Tier 2, Chapter 7, documentation and the review of DCD, Tier 1, Section 2.2.15, DAC/ITAAC verification, the NRC staff finds that Section 4.5 of IEEE Std 603 has been adequately addressed.

The NRC staff evaluated whether IEEE Std 603, Section 4.6, has been adequately addressed for the safety systems. This criterion requires the identification of the minimum number and location of spatial dependence sensors. These sensors are for those variables in Section 4.4 of

IEEE Std 603 that have a spatial dependence. The applicant/licensee's analysis should demonstrate that the number and location of sensors are adequate. The applicant committed in DCD, Tier 1, Section 2.2.15, that the software projects design bases list the minimum number and locations of sensors for those variables that are required to perform a safety function and have a spatial dependence (e.g., where the variable varies as a function of position in a particular region). DCD, Tier 1, Table 2.2.15-2 provides DAC/ITAAC for IEEE Std 603, Section 4.6 to verify that information related to the minimum number and location of sensors is incorporated into software projects during the software lifecycle process. Based on the review of the DCD, Tier 2, Chapter 7, documentation and the review of DCD, Tier 1, Section 2.2.15, DAC/ITAAC verification, the NRC staff finds that Section 4.6 of IEEE Std 603 has been adequately addressed.

The NRC staff evaluated whether IEEE Std 603, Section 4.7, has been adequately addressed for the safety systems. This criterion requires the identification of the range of transient and steady-state conditions of both motive and control power and the environment (for example, voltage, frequency, radiation, temperature, humidity, pressure, and vibration) during normal, abnormal, and accident circumstances throughout which the safety system shall perform. DCD, Tier 2, Section 7.1.6.6.1.5, states that all Q-DCIS equipment will be environmentally qualified to meet the accident conditions through which it operates to mitigate the consequences of the accident and will be seismically qualified to meet safe-shutdown earthquake levels. DCD, Tier 1, Table 3.8.1, specifies the ITAAC for the EQ process for safety mechanical and electrical equipment. The Q-DCIS is powered by four pairs of separate Class 1E alternating current power supplies. Each Q-DCIS division uses the two independent, UPS from the same division. The applicant committed in DCD, Tier 1, Section 2.2.15, that the software projects design bases list the range of transient and steady state conditions of motive and control power and environment (e.g., voltage, frequency, radiation, temperature, humidity, pressure, and vibration) during normal, abnormal, and accident circumstance throughout which the safety system is to perform. DCD, Tier 1, Table 2.2.15-2 provides DAC/ITAAC for IEEE Std 603, Section 4.7 to verify that information related to the range of transient and steady-state conditions is incorporated into software projects during the software lifecycle process. Based on the review of the DCD, Tier 2, Chapter 7, documentation and the review of DCD, Tier 1, Sections 2.2.15 and 3.2, DAC/ITAAC verification, the NRC staff finds that Section 4.7 of IEEE Std 603 has been adequately addressed.

The NRC staff evaluated whether IEEE Std 603, Section 4.8, has been adequately addressed for the safety systems. This criterion requires the identification of the conditions having the potential for functional degradation of safety system performance and for which provisions shall be incorporated to retain the capability for performing the safety function. Safety mechanical equipment and electrical equipment (which comprises electrical power and instrumentation and controls equipment) is qualified in accordance with the EQ program described in DCD, Tier 2, Section 3.9 through 3.11. Environmental conditions for the zones where qualified equipment is located are calculated for normal, AOO, test, accident and post accident conditions and are documented in DCD, Tier 2, Appendix 3H. DCD, Tier 1, Table 2.2.15-2 provides DAC/ITAAC for IEEE Std 603, Section 4.8 to verify that information related to conditions having the potential for causing functional degradation of safety system performance is incorporated into software projects during the software lifecycle process. Based on the review of the DCD, Tier 2, Chapter 3, documentation and the review of DCD, Tier 1, Section 2.2.15, DAC/ITAAC verification, the NRC staff finds that Section 4.7 of IEEE Std 603 has been adequately addressed.

The NRC staff evaluated whether IEEE Std 603, Section 4.9, has been adequately addressed for the safety systems. This criterion requires the identification of the methods used to determine that the reliability of the safety system design is appropriate for each such design. In addition, it requires the identification of the methods used to verify that any qualitative or quantitative reliability goals imposed on the system design have been met. In DCD, Tier 2, Section 7.1.6.6.1.1, states that the Design Reliability Assurance Program (D-RAP) is a program utilized during detailed design and specific equipment selection phases to assure that important ESBWR reliability assumptions of the probabilistic Risk Assessment (PRA) are addressed throughout the plant life. The D-RAP is described in DCD, Tier 2, Section 17.4. DCD, Tier 1, Table 2.2.15-2 provides DAC/ITAAC for IEEE Std 603, Section 4.9 to verify that information related to the methods used to determine that the reliability of the safety system design is incorporated into software projects during the software lifecycle process. Based on the review of the DCD, Tier 2, Chapter 7, and Chapter 17 documentation and the review of DCD, Tier 1, Section 2.2.15, DAC/ITAAC verification, the NRC staff finds that Section 4.9 of IEEE Std 603 has been adequately addressed.

The NRC staff evaluated whether IEEE Std 603, Section 4.10, has been adequately addressed for the safety systems. This criterion requires the documentation of the critical points in time or the plant conditions, after the onset of a DBE, including: (1) the point in time or plant conditions, after the protective actions of the safety system are initiated, (2) the point in time or plant conditions that define the proper completion of the safety function, (3) the point in time or the plant conditions that require automatic control of protective actions, and (4) the point in time or the plant conditions that allow returning a safety system to normal. The relevant point in time or plant conditions are discussed in DCD, Tier 2, Table 15.1-7. The allowable conditions for returning a plant to normal are described in DCD, Tier 2, Chapter 16. Consistent with RG 1.206, DAC/ITAAC are not provided for IEEE Std 603, Section 4.10 as the information is provided in the DCD and the IEEE STD 603, Section 4 criteria with DAC/ITAAC adequately verify the design basis information. Based on the review of the DCD, Tier 2, Chapters 7, 15 and 16 documentation, the NRC staff finds that Section 4.10 of IEEE Std 603 has been adequately addressed.

The NRC staff evaluated whether IEEE Std 603, Section 4.11, has been adequately addressed for the safety systems. This criterion requires the analysis and documentation of any equipment protective provisions that may prevent the safety systems from accomplishing their safety function. The safety systems are designed to accomplish their safety function in accordance with the single failure criteria, IEEE Std 603, Section 5.1. Failure modes and effects analyses (FMEA) are performed on the safety system final design. Consistent with RG 1.206, DAC/ITAAC are not provided for IEEE Std 603, Section 4.11 as the information is provided in the DCD and the IEEE STD 603, Section 4 criteria with DAC/ITAAC adequately verify the design basis information. In addition, DCD, Tier 1, Table 2.2.15-2 provides DAC/ITAAC for IEEE Std 603, Section 5.1 to verify that the software projects design bases comply with the single failure criterion, and that the as-built software projects test results confirm the results of the FMEA. Based on the review of the DCD, Tier 2, Chapter 7, documentation and the review of DCD, Tier 1, Section 2.2.15, DAC/ITAAC verification, the NRC staff finds that Section 4.11 of IEEE Std 603 has been adequately addressed.

The NRC staff evaluated whether IEEE Std 603, Section 4.12, has been adequately addressed for the safety systems. This criterion requires identification of any other special design basis that may be imposed on the system design. DCD, Tier 2, Chapter 7, has documented the design bases for each subsystem, including bases for diversity, interlocks, and regulatory agency criteria. Consistent with RG 1.206, DAC/ITAAC are not provided for IEEE Std 603,

Section 4.12 as the information is provided in the DCD and the IEEE STD 603, Section 4 criteria with DAC/ITAAC adequately verify the design basis information. The NRC staff finds that Section 4.12 of IEEE Std 603 has been adequately addressed.

7.1.1.3.10.2 IEEE Standard 603, Section 5, "Safety - System Criteria"

The NRC staff evaluated whether IEEE Std 603, Section 5, has been adequately addressed using SRP Appendix 7.1-C, Section 5. Section 5 requires that the safety systems, with precision and reliability, maintain plant parameters within acceptable limits established by DBEs.

The NRC staff evaluated whether IEEE Std 603, Section 5.1, has been adequately addressed for the safety systems. According to this criterion, no single failure within the safety system shall prevent proper protective action at the system level when required. DCD, Tier 2, Sections 7.1.2.3 and 7.1.6.6.1.2, provides a general description of design features that contribute to meeting IEEE Std 603, Section 5.1. These features include (1) the Q-DCIS is arranged into four divisions, (2) the intra-divisional and safety to non-safety fiber optic cable communication paths are redundant, (3) safety cabinets and chassis are powered by redundant safety UPS, and (4) an N-2 design basis. DCD, Tier 1, Table 2.2.15-1, documented that in the design, each safety platform complies with the requirements of IEEE Std 603, Section 5.1. DCD, Tier 1, Table 2.2.15-2, provides DAC/ITAAC for IEEE Std 603, Section 5.1, for the applicant to perform an analysis, or FMEA, that confirms that the requirements of the single failure criterion are satisfied for the safety systems. Based on the review of the DCD, Tier 2, Chapter 7, documentation and the review of DCD, Tier 1, Section 2.2.15, DAC/ITAAC verification, the NRC staff finds that Section 5.1 of IEEE Std 603 has been adequately addressed.

The NRC staff evaluated whether IEEE Std 603, Section 5.2, has been adequately addressed for the safety systems. This criterion requires the safety system design to provide features to ensure that system-level actions go to completion. DCD, Tier 2, Section 7.1.6.6.1.3, provides a general description of design features that contribute to meeting IEEE Std 603, Section 5.2. In accordance with SRP Appendix 7.1-C, the NRC staff review of this item should include a review of functional and logic diagrams to ensure that "seal-in" features are provided to enable system-level protective actions to go to completion. DCD, Tier 1, Table 2.2.15-2, provides DAC/ITAAC for IEEE Std 603, Section 5.2, for the applicant to perform an inspection of the design phase summary Baseline Review Report (BRR) of the software project to verify that the "seal-in" features are provided (DAC requirement). DAC/ITAAC are also provided for the applicant to perform an inspection of the as-built soft project installation phase summary BRR to verify that the safety functions of the "execute features" continue until completion. As documented in DCD, Tier 2, Section 7.1.6.6.1.3 and Tier 1, Table 2.2.15-2, item (9), the applicant committed in DCD, Tier 1, Section 2.2.15, that the I&C platform software projects are designed to include these seal-in feature for all safety systems. Based on the review of the DCD, Tier 2, Chapter 7, documentation and the review of DCD, Tier 1, Section 2.2.15, DAC/ITAAC verification, the NRC staff finds that Section 5.2 of IEEE Std 603 has been adequately addressed.

The NRC staff evaluated whether IEEE Std 603, Section 5.3, has been adequately addressed for the safety systems. SRP Appendix 7.1-C states that the applicant should confirm that the quality assurance provisions of Appendix B to 10 CFR Part 50 are applicable to the safety system. DCD, Tier 2, Section 7.1.6.6.1.4, states that the NRC-accepted applicant quality assurance program with its implementing procedures, constitutes the applicant's quality assurance system that is applied to the Q-DCIS design. The evaluation of the adequacy of the quality assurance program is addressed in the review of Chapter 17 of this report. Also, IEEE

Std 7-4.3.2, Section 5.3, provides quality requirements for digital computer systems split into six criteria, (1) software development, (2) software tools, (3) verification and validation (V&V), (4) independent V&V requirements, (5) software configuration management, and (6) software risk management. NEDE-33226P and NEDE-33245P describe implementation of these requirements, including the software life cycle process for the safety systems hardware and software. Section 7.1.2.3 of this report provides the NRC staff's evaluation of the applicant's software development activities. DCD, Tier 1, Section 3.2, includes the DAC/ITAAC for the applicant to perform results analyses to confirm that the software development activities for the safety systems were conducted consistently with the DCD and produce results that satisfy the acceptance criteria in BTP HCIB-14. Accordingly, based on the applicant's use of an acceptable software development process, as evaluated in Section 7.1.2.3 of this report, and its verification in the DCD Tier 1, DAC/ITAAC, the NRC staff finds that Section 5.3 of IEEE Std 7-4.3.2 has been adequately addressed.

The NRC staff evaluated whether IEEE Std 603, Section 5.4, has been adequately addressed for the safety systems. This criterion requires that safety systems be qualified to meet performance requirements identified in the design basis. SRP Appendix 7.1-C provides acceptance criteria for EQ. In DCD, Tier 2, Sections 3.10 and 3.11 describe the EQ programs for safety electrical and digital I&C equipment and are evaluated in Chapter 3 of this report. In DCD, Tier 2, Sections 7.1.6.4 and 7.1.6.6.1.5 describe how the Q-DCIS components are designed to be qualified by type testing and analysis to perform all safety functions when operated within the specified EMI limits. The Q-DCIS components are qualified in conformance to RG 1.180, when mounted in accordance with the specified methods. The Q-DCIS equipment is designed so that it is not susceptible to electromagnetic disturbances from neighboring modules and will not cause electromagnetic disturbances to neighboring modules. As endorsed by RG 1.180, the EMI qualification design follows the requirements specified in Military (Mil) Std 461E, "Department of Defense Interface Standard - Requirement for the Control of Electromagnetic Interference Characteristics of Subsystems and Equipment" and International Electrotechnical Commission (IEC) 61000-4, "International Standard - Electromagnetic Compatibility Testing and Measurement Techniques", depending on the specific requirement conditions. DCD, Tier 1, Table 3.8-1, provides ITAAC for the applicant to confirm the EQ of safety electrical and digital I&C equipment, which addresses the EQ aspects of IEEE Std 603, Section 5.4. Accordingly, based on the applicant's appropriate identification of EQ programs and their confirmation of the ITAAC, the NRC staff finds that the EQ aspects of IEEE Std 603, Section 5.4, have been adequately addressed.

In addition, IEEE Std 7-4.3.2, Section 5.4, provides criteria for computer system testing and qualification of existing commercial computers. With regard to computer system testing, IEEE Std 7-4.3.2, Section 5.4.1, states, "Equipment qualification testing shall be performed with the computer functioning with software and diagnostics that are representative of those used in actual operation." In regulatory position C(2) of RG 1.209, the NRC staff directly enhanced this statement by adding, "The qualification testing should be performed with the I&C system functioning, with software and diagnostics that are representative of those used in actual operation, while the system is subjected to the specified environmental service conditions, including abnormal operational occurrences." In RAI 7.1-47, the NRC staff requested the applicant to demonstrate how this standard is met. In response the applicant added RG 1.209 as an applicable RG in DCD, Tier 2, Table 7.1-1, and added discussion of conformance to RG 1.209 in the applicable sections of DCD, Tier 2, Chapter 7. The staff determined the response was acceptable since the applicant revised the DCD to address conformance to RG 1.209. Based on the applicant's response, RAI 7.1-47 is resolved. DCD, Tier 1, Table 3.8-1, provides ITAAC for the applicant to confirm the EQ of safety electrical and digital I&C

equipment, DCD, Tier 1, Table 3.2-1, provides DAC/ITAAC for the applicant to develop and implement software test plans for safety systems, These two sets of DAC/ITAAC together address the computer system testing aspects of IEEE Std 603, Section 5.4. Accordingly, based on the inclusion of IEEE Std 603, Section 5.4, and RG 1.209 commitments in the safety systems design basis and verification of the EQ and computer system testing being in the DCD Tier 1, DAC/ITAAC, the NRC staff finds that the computer system testing aspects of IEEE Std 603, Section 5.4, have been adequately addressed.

With regard to the qualification of existing commercial computers, IEEE Std 7-4.3.2, Section 5.4.2, provides criteria for the qualification of existing commercial computers. The NRC has approved the use of two EPRI reports for conforming to this criterion; EPRI TR-106439, as approved by the NRC in its safety evaluation, dated July 17, 1997, and EPRI TR-107330, as approved by the NRC on July 30, 1998. In DCD, Tier 2, Section 7.2.1.3.5, the applicant states that the Q-DCIS hardware, embedded and operating system software, and peripheral components conform to the guidance in BTP HCIB-18. The Q-DCIS is built and qualified specifically for ESBWR applications as safety and not as commercial-grade PLCs. The Q-DCIS meets the acceptance criteria contained in BTP HCIB-14, for safety applications. NEDE-33226P Section 5.8.3.6, states that commercial off the shelf (COTS) software to be used in a safety application shall be dedicated in accordance with an NRC-acceptable method of commercial-grade dedication for software and digital components (e.g., EPRI TR-106439). NEDE-33226P, Section 5.8.3.6, provides an additional description of the qualification of existing commercial computers for software. In its description of the software development plan (SDP), NEDE-33226P states that the COTS Evaluation Report and Documentation Package will be a design-phase output document. DCD, Tier 1, Section 3.2, provides the DAC/ITAAC to confirm the implementation of the SDP. Accordingly, the NRC staff finds that the criterion for the qualification of existing commercial computers is adequately addressed for the DCIS. Based on the applicant's commitment to use NRC-acceptable qualification methods and their verification in the DCD Tier 1, DAC/ITAAC, the NRC staff finds that the qualification of existing commercial computers in IEEE Std 603, Section 5.4, has been adequately addressed.

The NRC staff evaluated whether IEEE Std 603, Section 5.5, has been adequately addressed for the safety systems. This criterion requires that the safety system accomplish its safety functions under the full range of applicable conditions enumerated in the design basis. For digital computer-based systems, system real-time performance should be adequate to ensure completion of protective actions within the critical points of time identified, as required by IEEE Std 603, Section 4.10. BTP HCIB-21, provides supplemental guidance on evaluating response times for digital computer-based systems and discusses design constraints that allow greater confidence in the results analyses or prototype testing to determine real-time performance. The complete design basis for real-time performance is not available in the DCD. In the supplemental response to RAI 7.9-10, the applicant stated, "NEDE-33226P and NEDE-33245P, define a process by which plant performance requirements under various operational conditions will be specified, implemented, and tested." DCD Tier 1, Section 3.2, provides the DAC/ITAAC to verify activities associated with NEDE-33226P and NEDE-33245P. DCD, Tier 1, Table 3.8-1, provides ITAAC for the applicant to confirm the EQ of safety electrical and digital I&C equipment, which confirms that the safety systems function in the full range of applicable conditions enumerated in the design basis consistent with IEEE Std 603, Section 5.5,

IEEE Std 7-4.3.2 indicates that designs for computer system integrity and for test and calibration should be addressed as part of safety system integrity. SRP Appendix 7.1-D states that computer system software integrity (including the effects of hardware-software interaction) should be demonstrated by the applicant's software safety analysis activities. BTP HCIB-14,

Section B.3.1.9, describes the acceptable characteristics of software safety plans. HCIB-14, Section B.3.2.1, describes the characteristics of acceptable software safety analyses. As mentioned above for the plant performance requirements, DCD, Tier 1, Section 3.2, provides the DAC/ITAAC to verify the software safety plans and analyses for RPS. The NRC staff finds that IEEE Std 7-4.3.2 has been adequately addressed.

SRP Appendix 7.1-D states that the design should provide for safety 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, loss of energy, or adverse environments are experienced. This aspect is typically addressed by the applicant's FMEA. DCD, Tier 1, Table 2.2.15-2, provides DAC/ITAAC for IEEE Std 603, Section 5.1, for the applicant to perform an analysis, or FMEA, that confirms that the requirements of the single failure criterion are satisfied for the safety systems. The NRC staff finds that these FMEAs are an acceptable method to address this aspect of IEEE Std 603, Section 5.5 .

Accordingly, based on the inclusion of IEEE Std 603, Section 5.5, in the safety systems design basis and its confirmation in the DCD Tier 1, DAC/ITAAC, the NRC staff finds that Section 5.5 has been adequately addressed.

The NRC staff evaluated whether IEEE Std 603, Section 5.6, has been adequately addressed for the safety systems. This criterion requires, in part, independence among (1) redundant portions of a safety system, (2) safety systems and the effects of DBEs, and (3) safety systems and other systems. The following three aspects of independence should be addressed in each case:

(1) physical independence
(2) electrical independence
(3) communications independence

DCD, Tier 2, Section 7.1.2.4, specifies conformance to RG 1.75 and IEEE Std 384. RG 1.75 and IEEE Std 384 provide criteria for the independence of electrical safety systems, including physical separation and electrical isolation. Communications independence is evaluated in Section 7.1.5 of this report. DCD, Tier 2, Section 7.1.6.6.1.7, provides a general description of the design features that contribute to meeting IEEE Std 603, Section 5.6. These features include: (1) the Q-DCIS is arranged into four redundant and independent divisions, (2) each division of has an independent electrical power source, and (3) the sensors for each division are independent and physically separated. DCD, Tier 2, Table 7.1-2, identifies DCD sections where IEEE Std 603, Section 5.6, is addressed for specific systems, which are evaluated throughout this report.

DCD, Tier 1, Table 2.2.15-2, provides DAC/ITAAC for IEEE Std 603, Section 5.6, to verify that software projects have four independent redundant division, have communications independence, and have independence between safety systems and non-safety equipment. Accordingly, based on the inclusion of IEEE Std 603, Section 5.6, in the safety systems design basis and its confirmation in the DCD Tier 1, DAC/ITAAC, the NRC staff finds that Section 5.6 has been adequately addressed.

The NRC staff evaluated whether IEEE Std 603, Section 5.7, has been adequately addressed for safety systems. This criterion requires that the capability for testing and calibration of safety system equipment be provided while retaining the capability of the safety systems to accomplish their safety functions. DCD Tier 2, Section 7.1.6.6.1.8, provides a general description of design

features that contribute to meeting IEEE Std 603, Section 5.7. DCD, Tier 2, Table 7.1-2, identifies DCD sections where IEEE Std 603, Section 5.7, is addressed for specific systems. These discussions are evaluated in the corresponding sections of this report. In DCD, Tier 1, Table 2.2.15-2, provides DAC/ITAAC for IEEE Std 603, Section 5.7, to verify that maintenance bypasses allow test and calibration of one out of four divisions, that the divisions not in bypass status will accomplish their safety functions, that bypassed divisions alarm in the MCR, and that the division logic automatically becomes a two-out-of-three voting scheme. SRP Appendix 7.1-C also states that any failure that is not detectable must be considered concurrently with any random postulated, detectable, single failure. DCD, Tier 1, Table 2.2.15-2, provides DAC/ITAAC for IEEE Std 603, Section 5.1, for the applicant to perform an analysis, or FMEA, which confirms that the requirements of the single failure criterion are satisfied for the safety systems. Accordingly, based on the inclusion of IEEE Std 603, Section 5.7, in the safety systems design basis and its verification in the DCD Tier 1, DAC/ITAAC, the NRC staff finds that Section 5.7 has been adequately addressed.

The NRC staff evaluated whether IEEE Std 603, Section 5.8, has been adequately addressed for the safety systems. This criterion is associated with information displays and inoperable surveillance. DCD, Tier 2, Section 7.1.6.6.1.9, provides a general description of design features that contribute to meeting IEEE Std 603, Section 5.8. DCD, Tier 2, Table 7.1-2, identifies DCD sections where IEEE Std 603, Section 5.8, is addressed for specific systems, which are evaluated throughout this report. SRP Appendix 7.1-C states that safety system bypass and inoperable status indications should conform to RG 1.47. DCD, Tier 2, Section 7.1.6.4, specifies that bypass indications are designed to satisfy RG 1.47. DCD, Tier 2, Chapter 18, describes the HFE design process to design information displays and is evaluated in Chapter 18 of this report. DCD, Tier 1, Section 3.3, includes the DAC/ITAAC for implementing the HFE design process, which includes the design and verification of controls and information displays for monitoring variables and systems in the control room. This verification is applicable to all safety systems and includes verifying the inventory of displays for manually controlled actions, system status indications, and indications of bypasses. Accordingly, based on the inclusion of IEEE Std 603, Section 5.8, in the safety systems design basis and its confirmation in the DCD Tier 1, DAC/ITAAC, the NRC staff finds that Section 5.8 has been adequately addressed.

The NRC staff evaluated whether IEEE Std 603, Section 5.9, has been adequately addressed for the safety systems. This criterion requires that the design permit the administrative control of access to safety system equipment. This criterion also requires that the administrative controls be supported by provisions within the safety systems, by provisions in the generating station design, or by a combination thereof. DCD, Tier 2, Section 7.1.6.6.1.11, generally describes access controls to safety I&C systems. Keys, passwords, and other security devices are used to control access to specific rooms; open specific equipment cabinets; obtain permission to access specific electronic instruments for calibration, testing, and setpoint changes; and gain access to safety system software and data. DCD, Tier 2, Section 13.6.1.1.5, also describes access controls for certain I&C cabinets. DCD, Tier 1, Section 2.2.15, provides DAC/ITAAC for IEEE Std 603, DCD, Tier 2, Section 7.1.6.6.1.10, states that computer-related access controls and authorization are part of the cyber-security program plan, which is described in NEDO-33295 and NEDE-33295P. DCD, Tier 1, Section 3.2, provides the DAC/ITAAC to confirm the implementation of the cyber security program. Based on the review of the DCD, Tier 2, Chapter 7, documentation and the review of DCD Tier 1, DAC/ITAAC verification, the NRC staff finds that Section 5.9 of IEEE Std 603 has been adequately addressed.

The NRC staff evaluated whether IEEE Std 603, Section 5.10, has been adequately addressed for the safety systems. This criterion requires that the safety systems be designed to facilitate timely recognition, location, replacement, repair, and adjustment of malfunctioning equipment. SRP Appendix 7.1-C states that digital safety systems may include self-diagnostic capabilities to aid in troubleshooting, but the use of self-diagnostics does not replace the need for the capability for test and calibration systems as required by IEEE Std 603, Sections 5.7 and 6.5. DCD, Tier 2, Section 7.1.6.6.1.11, specifies that the Q-DCIS provide periodic self-diagnostic functions to locate failures to the component level. DCD, Tier 2, Section 7.1.6.6.1.11, also specifies that the Q-DCIS provide through individual division bypassing the capability to repair or replace a failed component on-line without affecting the safety system protection function. DCD, Tier 1, Table 2.2.15-2, provides DAC/ITAAC for IEEE Std 603, Section 5.10, to verify that the software projects have self-diagnostic features that facilitate the timely recognition, location, replacement, repair, and adjustment of malfunctioning equipment. Accordingly, based on the inclusion of IEEE Std 603, Section 5.10, in the safety systems design basis and its verification in the DCD Tier 1, DAC/ITAAC, the NRC staff finds that Section 5.10 of IEEE Std 603 has been adequately addressed.

The NRC staff evaluated whether IEEE Std 603, Section 5.11, has been adequately addressed for the safety systems. The requirements of this criterion are the following.

- Safety system equipment should be distinctly identified for each redundant portion of a safety system in accordance with the requirements of IEEE Std 384.

- Components or modules mounted in equipment or assemblies that are clearly identified as being in a single redundant portion of a safety system should not themselves require identification.

- The identification of safety system equipment should be distinguishable from other purposes.

- The identification of safety system equipment should not require frequent use of reference material.

- The associated documentation should be distinctly identified.

SRP Appendix 7.1-A states that guidance on identification is provided in RG 1.75, which endorses IEEE Std 384. The preferred identification method is color coding of components, cables, and cabinets. DCD, Tier 2 , Section 7.1.2.4, states that the Q-DCIS conforms to RG 1.75 and IEEE Std 384.

DCD, Tier 2, Section 7.1.6.6.1.12, provides a general description of conformance to IEEE 603, Section 5.11, including stating that color coding is used as a method of identification and safety equipment is distinctly marked in each redundant division of safety system addresses. DCD, Tier 2, Section 8.3.1.3 specifies additional methods of identification, including: (1) the identification method is color coding, (2) all markers within a division have the same color, (3) the ESBWR standard plant design eliminates safety associated circuits as defined by IEEE Std 384 and in accordance with RG 1.75, (4) divisional separation requirements of individual pieces of hardware are shown in the system elementary diagrams, and (5) identification of raceways, cables, etc., is compatible with the identification of the safety equipment with which it interfaces. DCD, Tier 2, Section 8.3.1.3, specifies how identification will

be implemented for equipment, cables, and raceways. The NRC staff finds that the applicant adequately commits to implementing the requirements of IEEE 603, Section 5.11. DCD, Tier 1, Section 2.2.15, provides DAC/ITAAC for IEEE Std 603, Section 5.11, to verify the distinct identification of each redundant portion of safety systems.

In addition, IEEE Std 7-4.3.2, Section 5.11, provides additional criteria for computer system testing and qualification of existing commercial computers, including that (1) firmware and software identification shall be used to assure the correct software is installed in the correct hardware component, and (2) means shall be included in the software such that the identification may be retrieved from the firmware using software maintenance tools. NEDE-33245P, Section 6.4.1, specifies guidelines for configuration identification consistent with IEEE Std 7-4.3.2, Section 5.11, as part of the software configuration management. DCD Tier 1, Section 3.2 includes the DAC/ITAAC to verify activities associated with NEDE-33226P and NEDE-33245P. Accordingly, based on the inclusion of IEEE Std 603, Section 5.11, and IEEE Std 7-4.3.2, Section 5.11, in the safety systems design basis and their confirmation in the DCD Tier 1, DAC/ITAAC, the NRC staff finds that Section 5.11 has been adequately addressed.

The NRC staff evaluated whether IEEE Std 603, Section 5.12, has been adequately addressed for the safety systems. This criterion states the following:

- Auxiliary supporting features shall meet all requirements of this standard.

- Other auxiliary features that perform a function that is not required for the safety systems to accomplish their safety functions, or are part of the safety system by association, shall be designed to meet those criteria necessary to ensure that such components, equipment, and systems do not degrade the safety systems below an acceptable level.

DCD, Tier 2, Section 7.1.6.6.1.13, identifies two auxiliary systems applicable to the power systems and HVAC. DCD, Tier 2, Section 8.3, identifies that separate AC and DC power systems are provided for safety and non-safety systems. These systems are evaluated in Section 8.3 of this report, which finds that there is acceptable physical separation and independence between the safety and non-safety systems, including the auxiliary systems.

DCD, Tier 2, Section 7.1.6.6.1.13, states that if the non-safety redundant HVAC is not available, safety temperature sensors with 2/4 logic trip the control room power that feeds pre-defined components of the non-safety I&C and other pre-defined non-safety heat loads. DCD, Tier 2, Sections 6.4.4, 9.4.1, 9.4.1.1, and 9.4.1.2, clarifies that the purpose of this trip is to remove the heat load due to the N-DCIS. DCD, Tier 2, Section 7.1.6.6.1.13, states that the Q-DCIS and support equipment is qualified for the expected temperature rise and therefore the Q-DCIS is dependent on the trip of the N-DCIS to minimize the temperatures in the safety I&C rooms. In RAI 7.1-132, the staff requested that the applicant include a discussion of this trip in the applicable instrumentation sections of the system descriptions in the DCD. In response to RAI 7.1-132, which was incorporated in DCD Revision 6, the applicant updated DCD, Tier 2, Subsections 6.4.8, 7.3.4.2, and 9.4.1.5 to clarify the function of the safety CRHAVS emergency trip circuit for the N-DCIS equipment installed in the control room habitability area. DCD, Tier 1, Tables 2.2.13-2 and 2.2.13-3 were updated for ITAAC verification. The staff determined the response was acceptable since the applicant clarified the trip of the N-DCIS throughout the DCD. Based on the applicant's response, this aspect of RAI 7.1-132 is resolved. DCD, Tier 1, Table 2.2.15-2, provides DAC/ITAAC for IEEE Std 603, Section 5.12, to verify that auxiliary features do not degrade the performance of software projects. Accordingly, based on the inclusion of IEEE Std 603, Section 5.12, in the safety systems design basis and its verification in

the DCD Tier 1, DAC/ITAAC, the NRC staff finds that Section 5.12 of IEEE Std 603 has been adequately addressed.

The NRC staff evaluated whether IEEE Std 603, Section 5.13, has been adequately addressed for the safety systems. This criterion states that the sharing of SSCs between units at multi-unit generating stations is permissible, provided that the ability to simultaneously perform required safety functions in all units is not impaired. In RAI 7.1-134, the staff requested that the applicant clarify whether there are shared components, and if so, clarify why the failure of shared components does not impact the Q-DCIS. DCD, Tier 2, Revision 5, Section 7.1.6.6.1.14, states that for multiple unit designs only the N-DCIS would have common network components as necessary to control and monitor common hardware and systems. DCD, Tier 2, Revision 5, Section 7.1.6.6.1.14 also states that the operation or failure of shared N-DCIS components does not affect the performance of the Q-DCIS. RAI 7.1-134 was being tracked as an open item in the SER with open items. In its response to RAI 7.1-134, the applicant revised DCD, Tier 2, Section 7.1.6.6.1.14 to state that the multi-unit station criteria do not apply to the standard single unit plant design submitted for NRC certification and statements concerning multiple units in DCD Tier 1 and Tier 2 were removed. The staff determined the response was acceptable since the applicant removed references to a multi-unit station from the DCD. Based on the applicant's response, RAI 7.1-134 is resolved. The NRC staff finds that IEEE Std 603, Section 5.13, is not applicable to design certification.

The NRC staff evaluated whether IEEE Std 603, Section 5.14, has been adequately addressed for the safety systems. This criterion states that human factors shall be considered at the initial stages, and throughout the design process, to ensure that the functions allocated in whole or in part to the human operator(s) and maintenance personnel can be successfully accomplished to meet the safety system design goals. The I&C design is integrated with the HFE design process, as described in DCD, Tier 2, Chapter 18, and evaluated in Chapter 18 of this report. DCD, Tier 1, Section 3.3, includes the DAC/ITAAC for implementing the HFE design process, which includes the design and verification of controls and information displays for monitoring variables and systems in the control room. Accordingly, based on the inclusion of IEEE Std 603, Section 5.14, in the safety systems design basis and its verification in the HFE DAC/ITAAC, the NRC staff finds that Section 5.14 of IEEE Std 603 has been adequately addressed.

The NRC staff evaluated whether IEEE Std 603, Section 5.15, has been adequately addressed. This criterion requires performing an analysis of the design to confirm that established reliability goals have been achieved. SRP Appendix 7.1-C states that the applicant should justify the degree of redundancy, diversity, testability, and quality provided in the safety system design is adequate to achieve functional reliability commensurate with the safety functions to be performed. SRP Appendix 7.1-C further states that software that complies with the quality criteria of IEEE Std 603, Section 5.3, and that is used in safety systems that provide measures for defense against CCFs, as described in the SRP Appendix 7.1-C discussion of IEEE Std 603, Section 5.1, is considered by the NRC staff to comply with the fundamental reliability requirements of IEEE Std 603. DCD, Tier 1, Section 3.2, provides DAC/ITAAC for the applicant to perform results analyses to confirm that the software development activities for the safety systems were conducted consistently with the DCD and produce results that satisfy the acceptance criteria in BTP HCIB-14 consistent with IEEE Std 603, Section 5.3. DCD, Tier 1, Section 2.2.15, includes the DAC/ITAAC for IEEE Std 603, Sections 5.1 to verify the implementation of the single failure criteria. DCD, Tier 2, Section 7.1.6.6.1.16, identifies that the Design Reliability Assurance Program (D-RAP), evaluated in Section 17.4 of this report, confirms that any quantitative or qualitative reliability goals established for the protection

systems have been met. DCD, Tier 1, Section 3.6 provides ITAAC to confirm the reliability of the SSCs in D-RAP, including the software projects. Accordingly, based on the inclusion of IEEE Std 603, Section 5.15, in the safety systems design basis and its verification in the DCD Tier 1, DAC/ITAAC, the NRC staff finds that Section 5.15 has been adequately addressed.

7.1.1.3.10.3 IEEE Standard 603, Section 6, "Sense and Command Features - Functional and Design Requirements"

The NRC staff evaluated whether IEEE Std 603, Section 6.1, has been adequately addressed. This criterion states that means shall be provided to automatically initiate and control all protective actions except as justified in Section 4.5. SRP Appendix 7.1-C states that: (1) the applicant's analysis should confirm that the safety system has been qualified to demonstrate that the performance requirements are met, (2) the evaluation of the precision of the safety system should be addressed to the extent that setpoints, margins, errors, and response times are factored into the analysis, (3) for digital computer-based systems, the evaluation should confirm that the functional requirements have been appropriately allocated into hardware and software requirements, and (4) the evaluation should also confirm that the system's real-time performance is deterministic and known. DCD, Tier 2, Section 7.1.6.6.1.17, provides a broad description of the design basis applicable to this criterion. NEDE-33226P and NEDE-33245P address the first three SRP topics as they define a software development process by which plant performance requirements for I&C systems under various operational conditions will be specified, implemented, and tested. DCD Tier 1, Section 3.2 includes the DAC/ITAAC to verify activities associated with NEDE-33226P and NEDE-33245P. DCD Tier 2, Section 7.1.3.2.7, addresses the fourth topic by specifying that the Q-DCIS internal and external communication protocols are deterministic. DCD, Tier 1, Table 2.2.15-2, provides the DAC/ITAAC for IEEE Std 603, Section 6.1, to confirm the automatic initiation and control of the required safety functions. Accordingly, based on the inclusion of IEEE Std 603, Section 6.1, in the safety systems design basis and its verification in the DCD Tier 1, DAC/ITAAC, the NRC staff finds that Section 6.1 of IEEE Std 603 has been adequately addressed.

The NRC staff evaluated whether IEEE Std 603, Section 6.2, has been adequately addressed. This criterion requires, in part, that (1) means shall be provided in the control room to implement manual initiation at the division level of the automatically initiated protective actions, (2) means shall be provided in the control room to implement manual initiation and control of the protective actions identified in IEEE Std 603, Section 4.5, that have not been selected for automatic control under IEEE Std 603, Section 6.1, and (3) means shall be provided to implement the manual actions necessary to maintain safe conditions after the protective actions are completed as specified in IEEE Std 603, Section 4.10. SRP Appendix 7.1-C states that features for manual initiation of protective action should conform with RG 1.62. DCD, Tier 2, Section 7.1.6.6.1.18, states that "Each protective action can be manually initiated at the system level, in conformance to RG 1.62, and at the division level in conformance to IEEE Std 603, Sections 6.2 and 7.2." DCD, Tier 1, Table 2.2.15-1, requires that all safety I&C platforms comply with IEEE Std 603, Section 6.2. DCD, Tier 1, Table 2.2.15-2, provides DAC/ITAAC for IEEE Std 603, Section 6.2, to confirm that applicable systems have MCR features that are capable of manually initiating and controlling automatically initiated safety functions at the division level. DCD, Tier 2, Section 7.1.6.6.1.18, also identifies that the design of manual control is integrated into the overall HFE design as described in DCD, Tier 2, Chapter 18, and evaluated in Chapter 18 of this report. DCD, Tier 1, Section 3.3, includes the DAC/ITAAC for verifying the implementation of the HFE design process, which includes the design and verification of controls and information displays for monitoring variables and systems in the control room. Accordingly, based on the inclusion of IEEE Std 603, Section 6.2, in the safety systems design basis and its

verification in the DCD Tier 1, DAC/ITAAC, the NRC staff finds that Section 6.2 of IEEE Std 603 has been adequately addressed.

The NRC staff evaluated whether IEEE Std 603, Section 6.3, has been adequately addressed. This criterion requires that any failure of non-safety systems should not affect safety protection systems or prevent them from performing their safety functions. For example, DI&C-ISG-04, states 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 Appendix A to 10 CFR Part 50 (see GDC 24). Appendix 7.1-C states that where the event of concern is the single failure of a sensing channel shared between control and protection functions, previously accepted approaches have included the following:

- isolating the safety system from channel failure by providing additional redundancy
- isolating the control system from channel failure by using data validation techniques to select a valid control input

DCD, Tier 2, Section 7.1.6.6.1.19, provides a general description of conformance by stating, "The Q-DCIS protection systems are separate and independent from the non-safety control systems." DCD, Tier 1, Table 2.2.15-2, provides DAC/ITAAC for IEEE Std 603, Section 6.3, to verify that software projects have four independent redundant division, have communications independence, and have independence between safety systems and non-safety equipment. Accordingly, based on the inclusion of IEEE Std 603, Section 6.3, in the safety systems design basis and its verification in the DCD Tier 1, DAC/ITAAC, the NRC staff finds that Section 6.3 has been adequately addressed.

The NRC staff evaluated whether Section 6.4 of IEEE Std 603 has been adequately addressed. This criterion 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. SRP Appendix 7.1-C states that the applicant should verify that any indirect parameter is a valid representation of the desired direct parameter for all events. DCD, Tier 2, Section 7.1.6.6.1.20, states that "To the extent feasible, the protection system inputs are derived from signals that directly measure the designated process variables," which is consistent with the high level conceptual nature of the DCIS design. DCD, Tier 1, Table 2.2.15-2, provides DAC/ITAAC for IEEE Std 603, Section 6.4, to confirm that sense and command feature inputs for software projects are derived from signals that are direct measures of the desired variables specified in the design bases.

SRP Appendix 7.1-C states that for both direct and indirect parameters, the applicant should verify that the characteristics (e.g., range, accuracy, resolution, response time, sample rate) of the instruments that produce the safety system inputs are consistent with the analysis provided in DCD, Tier 2, Chapter 15. NEDE-33226P and NEDE-33245P define a software development process by which plant performance requirements for I&C systems under various operational conditions will be specified, implemented, and tested. DCD, Tier 1, Section 3.2, includes the DAC/ITAAC to verify activities associated with NEDE-33226P and NEDE-33245P. Accordingly, based on the inclusion of IEEE Std 603, Section 6.4, in the safety systems design basis and its verification in the DCD Tier 1, DAC/ITAAC, the NRC staff finds that Section 6.4 has been adequately addressed.

The NRC staff evaluated whether Section 6.5 of IEEE Std 603 has been adequately addressed. This criterion states, in part, that means shall be provided for checking the operational availability of each sensor required for a safety function. SRP Appendix 7.1-C provides guidance on the checking of sensors. DCD, Tier 2, Section 7.1.6.6.1.21, states protection system sensors have the capability to be checked by perturbing the monitored variable, by varying the input to the sensor within the constraints, or by cross-checking between redundant channels. This capability is consistent with SRP Appendix 7.1-C. DCD, Tier 2, Section 7.1.6.6.1.21, also describes features to provide at least two valid divisions for cross-checking of monitored variables. DCD, Tier 1, Table 2.2.15-2, provides DAC/ITAAC for IEEE Std 603, Section 6.5, to verify that maintenance bypasses allow test and calibration of one out of four divisions, that the divisions not in bypass status will accomplish their safety functions, that bypassed divisions alarm in the MCR, and that the division logic automatically becomes a two-out-of-three voting scheme. Accordingly, based on the inclusion of IEEE Std 603, Section 6.5, in the safety systems design basis and its verification in the DCD Tier 1, DAC/ITAAC, the NRC staff finds that Section 6.5 has been adequately addressed.

The NRC staff evaluated whether IEEE Std 603, Section 6.6, has been adequately addressed. This requirement states, in part, that whenever the applicable permissive conditions are not met, a safety system shall automatically prevent the activation of an operating bypass or initiate the appropriate safety function(s). SRP Appendix 7.1-C states that the operator may take action to prevent the unnecessary initiation of a protective action. DCD, Tier 2, Section 7.1.6.6.1.22, describes the applicability of IEEE Std 603, Section 6.6, to the protection systems and states that the design provides for the automatic removal of operational bypasses. DCD, Tier 2, Sections 7.2.1.5 and 7.3.5.2 provide descriptions of the Q-DCIS operating bypasses and provisions for their automatic removal. DCD, Tier 1, Table 2.2.15-1, requires that all safety I&C platforms comply with IEEE Std 603, Section 6.6 criterion. DCD, Tier 1, Table 2.2.15-2, provides DAC/ITAAC for IEEE Std 603, Section 6.6, to verify that software projects are capable of automatically (1) preventing the activation of an operating bypass, whenever the applicable permissive conditions for an operating bypass are not met, and (2) removing activated operating bypasses, if the plant conditions change so that an activated operating bypass is no longer permissible. Accordingly, based on the inclusion of IEEE Std 603, Section 6.6, in the safety systems design basis and its verification in the DCD Tier 1, DAC/ITAAC, the NRC staff finds that Section 6.6 has been adequately addressed.

The NRC staff evaluated whether IEEE Std 603, Section 6.7, has been adequately addressed. This criterion states, in part, that the capability of a safety system to accomplish its safety function shall be retained while sense and command features equipment is in maintenance bypass. The criterion further states that during such operation, the sense and command features shall continue to meet the requirements of Sections 5.1 and 6.3. DCD, Tier 2, Section 7.1.6.6.1.23, describes the general capability of safety systems to accomplish their safety functions while a safety division is in maintenance bypass. DCD, Tier 2, Section 7.1.6.6.1.23 states that this capability is provided since only one safety division, out of four, may be bypassed at any given time. In DCD, Tier 2, Sections 7.2.1.5.2.2 and 7.3.5.2.4 provide descriptions of the Q-DCIS systems capability to accomplish their safety functions while a safety division is in maintenance bypass. DCD, Tier 1, Table 2.2.15-1, requires that all safety I&C platforms comply with IEEE Std 603, Section 6.7 criterion. DCD, Tier 1, Table 2.2.15-2, provides DAC/ITAAC for IEEE Std 603, Section 6.7, to verify that software projects are capable of performing their safety functions, when one division is in maintenance bypass. Accordingly, based on the inclusion of IEEE Std 603, Section 6.7, in the safety systems design basis and its verification in the DCD Tier 1, DAC/ITAAC, the NRC staff finds that Section 6.7 of IEEE Std 603 has been adequately addressed.

The NRC staff evaluated whether IEEE Std 603, Section 6.8, has been adequately addressed. This criterion states that the allowance for uncertainties between the process analytical limit documented in IEEE Std 603, Section 4.4, and the device setpoint shall be determined using a documented methodology. The criterion also 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 a positive means of ensuring that the more restrictive setpoint is used when required. DCD, Tier 2, Section 7.1.6.6.1.24, states that instrument setpoints are determined by the methodology described in NEDO-33304, which is evaluated in Section 7.1.4 of this report. DCD, Tier 1, Table 2.2.15-2, provides DAC/ITAAC for IEEE Std 603, Section 6.8, to confirm that the safety systems' setpoints for safety functions are defined, determined and implemented based on a defined setpoint methodology. Accordingly, based on the inclusion of IEEE Std 603, Section 6.8, in the safety systems design basis and its verification in the DCD Tier 1, DAC/ITAAC, the NRC staff finds that Section 6.8 has been adequately addressed.

7.1.1.3.10.4 IEEE Standard 603, Section 7, "Execute Features - Functional and Design Requirements"

The NRC staff evaluated whether IEEE Std 603, Section 7.1, has been adequately addressed. Section 7.1 states, in part, that the safety system should, with precision and reliability, automatically initiate and execute protective action for the range of conditions and performance requirements. SRP Appendix 7.1-C states that: (1) the applicant's analysis should confirm that the safety system has been qualified to demonstrate that the performance requirements are met, (2) the evaluation of the precision of the safety system should be addressed to the extent that setpoints, margins, errors, and response times are factored into the analysis, (3) for digital computer-based systems, the evaluation should confirm that the functional requirements have been appropriately allocated into hardware and software requirements, and (4) the evaluation should also confirm that the system's real-time performance is deterministic and known. DCD, Tier 2, Section 7.1.6.6.1.17, provides a broad description of the design basis applicable to this criterion. NEDE-33226P and NEDE-33245P address the first three SRP topics as they define a software development process by which plant performance requirements for I&C systems under various operational conditions will be specified, implemented, and tested. DCD Tier 1, Section 3.2, includes the DAC/ITAAC to verify activities associated with NEDE-33226P and NEDE-33245P. DCD Tier 2, Section 7.1.3.2.7, addresses the fourth topic by specifying that stating that the Q-DCIS internal and external communication protocols are deterministic. DCD, Tier 1, Table 2.2.15-1, requires that all safety I&C platforms comply with IEEE Std 603, Section 7.1 criterion. DCD, Tier 1, Table 2.2.15-2, provides DAC/ITAAC for IEEE Std 603, Section 7.1, to confirm the automatic initiation and control of the required safety functions. Accordingly, based on the inclusion of IEEE Std 603, Section 7.1, in the safety systems design basis and its verification in the DCD Tier 1, DAC/ITAAC, the NRC staff finds that Section 7.1 of IEEE Std 603 has been adequately addressed.

The NRC staff reviewed whether Section 7.2 of IEEE Std 603 has been adequately addressed. Section 7.2 states, in part, that the review of manual controls should confirm that the controls will be functional (e.g., power will be available and command equipment is appropriately qualified) and accessible within the time required of the operator during plant conditions under which manual actions may be necessary. DCD, Tier 1, Table 2.2.15-1, requires that all safety I&C platforms comply with IEEE Std 603, Section 7.2. DCD, Tier 1, Table 2.2.15-2 provides the DAC/ITAAC for IEEE Std 603, Section 7.2, to confirm that applicable systems have MCR features that are capable of manually initiating and controlling automatically initiated safety

functions at the division level. DCD, Tier 2, Section 7.1.6.6.1.18, identifies that the design of manual control is integrated into the overall HFE design as described in DCD, Tier 2, Chapter 18, and evaluated in Chapter 18 of this report. DCD, Tier 1, Section 3.3, includes the DAC/ITAAC for verifying the implementation of the HFE design process, which includes the design and verification of controls and information displays for monitoring variables and systems in the control room. Accordingly, based on the inclusion of IEEE Std 603, Section 7.2, in the safety systems design basis and its verification in the DCD Tier 1, DAC/ITAAC, the NRC staff finds that Section 7.2 of IEEE Std 603 has been adequately addressed.

The NRC staff evaluated whether IEEE Std 603, Section 7.3, has been adequately addressed. This criterion requires that the design of the execute features shall be such that once initiated, the protective actions of the execute features shall go to completion. In DCD, Tier 2, Section 7.1.6.6.1.3, provides a general description of design features that contribute to meeting IEEE Std 603, Section 7.3. In accordance with SRP Appendix 7.1-C, the NRC staff review of this item should include a review of functional and logic diagrams, which are not available at this time, to ensure that "seal-in" features are provided to enable system-level protective actions to go to completion. DCD, Tier 1, Table 2.2.15-1, requires that all safety I&C platforms comply with IEEE Std 603, Section 7.3. DCD, Tier 1, Table 2.2.15-2 provides the DAC/ITAAC for IEEE Std 603, Section 7.3, for the applicant to perform an inspection of the design phase summary Baseline Review Report (BRR) of the software project to verify that the "seal-in" features are provided (DAC requirement). DAC/ITAAC are also provided for the applicant to perform an inspection of the as-built soft project installation phase summary BRR to verify that the safety functions of the "execute features" continue until completion. As documented in DCD, Tier 1, Table 2.2-15 and DCD, Tier 2, Section 7.1.6.6.1.3, the applicant committed that the I&C platform software projects are designed to include these seal-in feature for all safety systems. Accordingly, based on the inclusion of IEEE Std 603, Section 7.3, in the safety systems design basis and its verification in the DCD Tier 1, DAC/ITAAC, the NRC staff finds that Section 7.3 of IEEE Std 603 has been adequately addressed.

The NRC staff reviewed whether Section 7.4 of IEEE Std 603 has been adequately addressed. This requirement states, in part, that whenever the applicable permissive conditions are not met, a safety system shall automatically prevent the activation of an operating bypass or initiate the appropriate safety function(s). SRP Appendix 7.1-C states that the operator may take action to prevent the unnecessary initiation of a protective action. DCD, Tier 2, Section 7.1.6.6.1.22, describes the applicability of IEEE Std 603, Section 7.4, to the protection systems and states that the design provides for the automatic removal of operational bypasses. In DCD, Tier 2, Sections 7.2.1.5 and 7.3.5.2 provide descriptions of the Q-DCIS operating bypasses and provisions for their automatic removal and are evaluated in Sections 7.2 and 7.3 of this report, respectively. DCD, Tier 1, Table 2.2.15-1, requires that all safety I&C platforms comply with IEEE Std 603, Section 7.4 criterion. DCD, Tier 1, Table 2.2.15-2, provides the DAC/ITAAC for IEEE Std 603, Section 7.4, to verify that software projects are capable of automatically (1) preventing the activation of an operating bypass, whenever the applicable permissive conditions for an operating bypass are not met, and (2) removing activated operating bypasses, if the plant conditions change so that an activated operating bypass is no longer permissible. Accordingly, based on the inclusion of IEEE Std 603, Section 7.4, in the safety systems design basis and its verification in the DCD Tier 1, DAC/ITAAC, the NRC staff finds that Section 7.4 of IEEE Std 603 has been adequately addressed.

The NRC staff evaluated whether IEEE Std 603, Section 7.5, has been adequately addressed. This criterion states that the capability of a safety system to accomplish its safety function shall be retained while execute features equipment is in maintenance bypass. DCD, Tier 2,

Section 7.1.6.6.1.23, describes the general capability of safety systems to accomplish their safety functions while a safety division is in maintenance bypass. DCD, Tier 2, Section 7.1.6.6.1.23, states that this capability is provided since only one safety division, out of four, may be bypassed at any given time. In DCD, Tier 2, Sections 7.2.1.5 and 7.3.5.2 provide descriptions of the Q-DCIS systems capability to accomplish their safety functions while a safety division is in maintenance bypass and are evaluated in Sections 7.2 and 7.3 of this report, respectively. DCD, Tier 1, Table 2.2.15-1, requires that all safety I&C platforms comply with IEEE Std 603, Section 7.5 criterion. DCD ,Tier 1, Table 2.2.15-2 provides the DAC/ITAAC for IEEE Std 603, Section 7.5, to verify that software projects are capable of performing their safety functions, when one division is in maintenance bypass. Accordingly, based on the inclusion of IEEE Std 603, Section 7.5, in the safety systems design basis and its verification in the DCD Tier 1, DAC/ITAAC, the NRC staff finds that Section 7.5 of IEEE Std 603 has been adequately addressed.

7.1.1.3.10.5 IEEE Standard 603, Section 8, "Power Source Requirements"

The NRC staff evaluated whether IEEE Std 603, Section 8.1, has been adequately addressed. This criterion states that those portions of the Class 1E power system that are required to provide the power to the many facets of the safety system are governed by the criteria of IEEE Std 603 and are a part of the safety systems. The criterion further states that specific criteria unique to the Class 1E power systems are given in IEEE Std 308, "IEEE Standard Criteria for Class 1E Power Systems for Nuclear Power Generating Stations". DCD, Tier 2, Section 7.1.6.6.1.25, states that the Q-DCIS protection system cabinets and components are supported by two independent power sources. Each division of safety I&C is powered by two UPS that can supply 120 VAC from offsite power, diesel generator power, or safety batteries (for 72 hours). Either of the two power sources allows the Q-DCIS operation. DCD, Tier 1, Table 2.2.15-2 provides the DAC/ITAAC for IEEE Std 603, Section 8.1 to verify that the software project's electrical components receive power from their respective, divisional, safety-related power supplies. Accordingly, based on the inclusion of IEEE Std 603, Section 8.1, in the safety systems design basis and its verification in the DCD Tier 1, DAC/ITAAC, the NRC staff finds that Section 8.1 has been adequately addressed.

The NRC staff evaluated whether IEEE Std 603, Section 8.2, has been adequately addressed. This criterion states that power sources, such as control air systems, bottled gas systems, and hydraulic systems, required to provide the power to the safety systems are a part of the safety systems and shall provide power consistent with the requirements of IEEE Std 603. DCD, Tier 2, Section 7.1.6.6.1.26, states that if a non-electrical power source is required for a safety function, then the source of the power is classified as safety-related and complies with IEEE 603. DCD, Tier 1, Table 2.2.15-1, requires that all safety I&C platforms comply with IEEE Std 603, Section 8.2 criterion. DCD, Tier 1, Table 2.2.15-2 provides the DAC/ITAAC for IEEE Std 603, Section 8.2 to verify that the software project's safety systems and components that require non-electric power receive it from safety-related sources. Accordingly, based on the inclusion of IEEE Std 603, Section 8.2, in the safety systems design basis and its verification in the DCD Tier 1, DAC/ITAAC, the NRC staff finds that Section 8.2 of IEEE Std 603 has been adequately addressed.

The NRC staff evaluated whether IEEE Std 603, Section 8.3, has been adequately addressed. This criterion states that the capability of the safety systems to accomplish their safety functions shall be retained while power sources are in maintenance bypass. The criterion further states that portions of the power sources with a degree of redundancy of one shall be designed such that, when a portion is placed in maintenance bypass (that is, reducing temporarily its degree of

redundancy to zero), the remaining portions provide acceptable reliability. DCD, Tier 2, Section 7.1.6.6.1.27, states that the Q-DCIS components are powered by redundant, independent, and separated UPS appropriate to their division with battery backup (per division) for at least 72 hours. Operation of the Q-DCIS when one of its power supplies is in maintenance bypass technically makes one division inoperable since the maintenance bypass reduces a division's ability to operate to approximately 36 hours from 72 hours should offsite or diesel power be lost. However, since the Q-DCIS retains full functionality with 3 out of 4 divisions operable, the NRC staff finds the reduced operating lifetime of a single division on loss of power acceptable. DCD, Tier 1, Table 2.2.15-1, requires that all safety I&C platforms comply with IEEE Std 603, Section 8.3 criterion. DCD, Tier 1, Table 2.2.15-2 provides the ITAAC for IEEE Std 603, Section 8.3 to verify that software projects are capable of performing their safety functions, when one power supply division is in maintenance bypass. Accordingly, based on the inclusion of IEEE Std 603, Section 8.3, in the safety systems design basis and its verification in the DCD Tier 1, DAC/ITAAC, the NRC staff finds that Section 8.3 of IEEE Std 603 has been adequately addressed.

7.1.1.4 Conclusion

Based on the above, and additional details provided in Sections 7.1.1.3.1 through 7.1.1.3.10 of this report, the staff concludes that the applicant has identified the I&C systems that are important to safety. The applicant has identified the NRC regulations that are applicable to these systems. The applicant has also identified appropriate guidelines consisting of the regulatory guides and the industry codes and standards that are applicable to the systems. The staff concludes that the applicant has included sufficient DAC/ITAAC in Tier 1 to verify that the design of ESBWR I&C systems is completed in compliance with the applicable requirements. Therefore, the staff concludes that the NRC regulations identified in Section 7.1.1 of this report are met.

7.1.2 Software Development Activities

7.1.2.1 Regulatory Criteria

The NRC staff's acceptance of the software for safety system functions is based on (1) confirmation that acceptable plans were prepared to control software development activities, (2) evidence that the plans were followed in an acceptable software life cycle, and (3) evidence that the process produced acceptable design outputs. BTP HCIB-14, provides acceptance criteria for evaluating software life cycle processes for digital computer-based I&C systems.

The acceptance criteria are based on meeting the relevant requirements of 10 CFR 50.55a(a)(1); 10 CFR 50.55a(h); GDC 1 and 21; Appendix B to 10 CFR Part 50, Criterion III. The acceptance criteria are also based on conforming to the guidelines of RG 1.152, RG 1.168, RG 1.169, RG 1.170, RG 1.171, RG 1.172, and RG 1.173.

7.1.2.2 Summary of Technical Information

DCD, Tier 2, Appendix 7B, Software Development, states that the Q-DCIS comprise the following platforms:

- RTIF-NMS
- SSLC/ESF
- ICP (VBIF, ATWS/SLC, and HP CRD IBF)

and the N-DCIS comprise the following Network Segments:

- GENE (DPS)
- PIP A
- PIP B
- BOP
- PCF

These platforms and network segments comprise systems of integrated software and hardware elements. Software projects are developed for the various platforms and network segments. Project software plans control the development of each platform and network segment using a software life cycle process. NEDE-33226P and NEDE-33245P are incorporated by reference into the DCD.

NEDE-33226P and NEDE-33245P are two high level documents establishing the guidelines, restrictions, requirements, program measures, and framework for creating software life cycle plans intended for the development of the digital I&C application software. These two LTRs describe the applicant's managerial, design, development, and software quality assurance processes. They also address conformance with the NRC review acceptance criteria provided in the SRP. NEDE-33226P describes the design and development activities, while NEDE-33245P describes the software quality assurance activities during all the software life cycle phases of the digital I&C systems.

NEDO-33217 (NEDE-33217P), "Man-Machine Interface System and Human Factors Engineering Implementation Plan", is not covered in this section but is reviewed in Chapter 18 of this SER. NEDE-33217P, Section 3.3.1, states that NEDE-33226P and NEDE-33245P are governing documents for the software development activities described in this LTR.

The applicant has not included any specific project plans, documentation of completed life cycle phases, or design outputs within the scope of the design certification. Instead, NEDE-33226P and NEDE-33245P provide templates for completing specific project plans, describe the documents and the review processes to be completed for each life cycle phase, and describe the design outputs that will be produced. The applicant also provides the DAC/ITAAC in DCD, Tier 1, Section 3.2, to confirm that the completion of these activities and products conforms to the processes described in NEDE-33226P and NEDE-33245P and the guidelines of BTP HCIB-14.

7.1.2.3 NRC Staff Evaluation

7.1.2.3.1 Review Method for Software Development Activities

The NRC staff reviews project-specific software for safety systems by (1) confirming that acceptable plans have been developed to control software development activities, (2) verifying that the plans have been followed in an acceptable software life cycle process, and (3) confirming that the process produced acceptable design outputs. As discussed in Section 7.1.1.3.1 of this report, the NRC implements the policy (SECY-92-053) of accepting the use of DAC in lieu of detailed design information in the digital I&C area during design certification. The NRC staff examines the software life cycle planning, implementation, and design outputs. This information can be organized as described in BTP HCIB-14.

BTP HCIB-14 groups the software life cycle activities into the following eight phases:

(1) planning
(2) requirements
(3) design
(4) implementation
(5) integration
(6) validation
(7) installation
(8) operations and maintenance

Eleven different documents detail the planning effort in BTP HCIB-14:

(1) software management plan (SMP)
(2) software development plan (SDP)
(3) software quality assurance plan (SQAP)
(4) software integration plan (SIntP)
(5) software installation plan (SInstP)
(6) software maintenance plan (SMaintP)
(7) software training plan (STrngP)
(8) software operations plan (SOP)
(9) software safety plan (SSP)
(10) software verification and validation plan (SVVP)
(11) software configuration management plan (SCMP)

The implementation effort produces four types of documents in multiple life cycle phases in BTP HCIB-14:

(1) safety analyses
(2) verification and validation analyses and test reports
(3) configuration management reports
(4) testing activities

Nine types of documents detail the design outputs in BTP HCIB-14:

(1) software requirements specifications (SRS)
(2) hardware and software architecture descriptions (SAD)
(3) software design specifications (SDS)
(4) code listings
(5) build documents
(6) installation configuration tables
(7) operations manuals
(8) maintenance manuals
(9) training manuals

The process that BTP HCIB-14 discusses is generally sequential in flow. Figure 7-1 is a graphic presentation of this information.

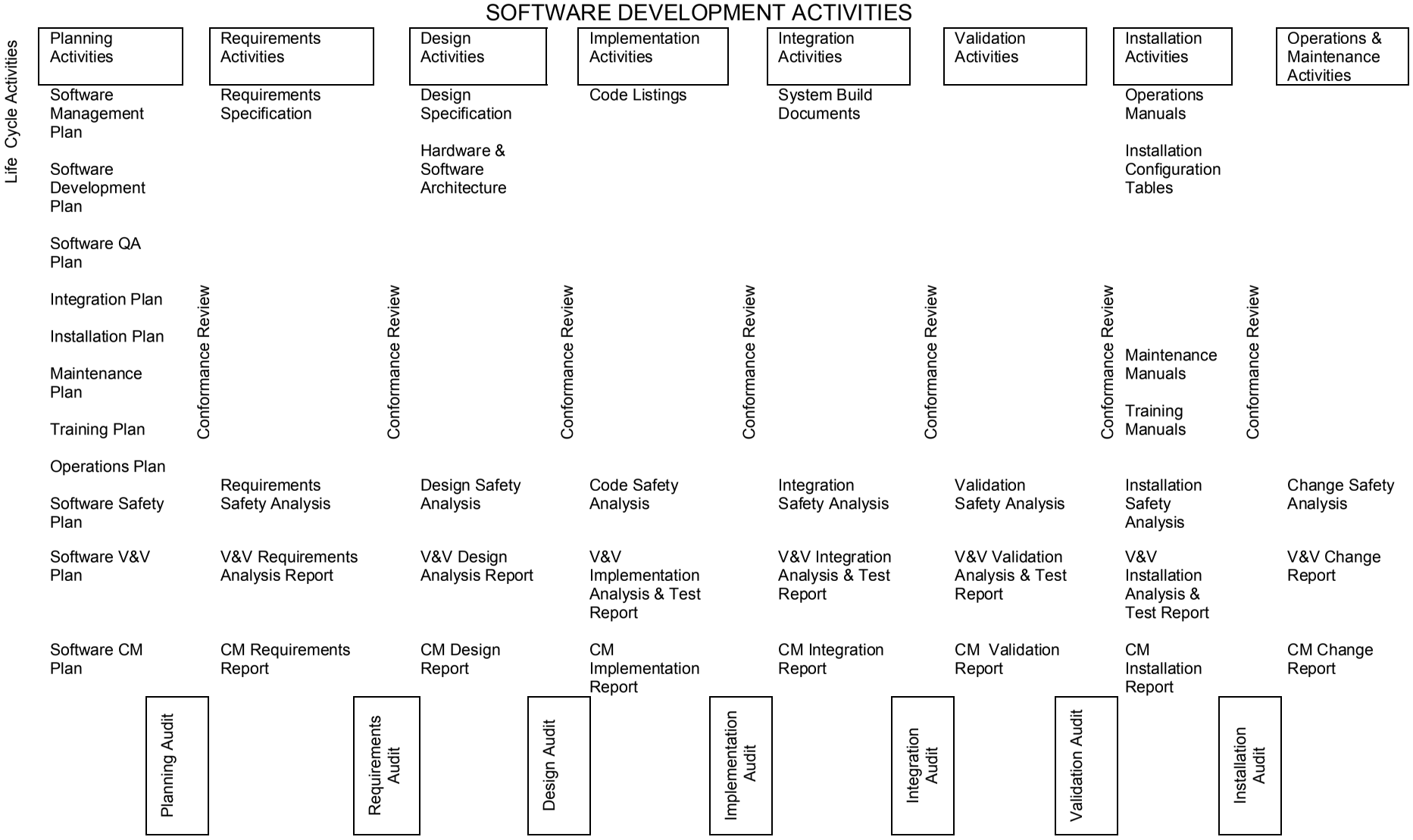

Figure 7-1 Example of Software Development Activities Using Generic Waterfall Life Cycle

BTP HCIB-14 provides the criteria for the various life cycle documents acceptable to the NRC staff. The specific acceptance criteria for software reviews also include other applicable RGs and standards as listed in Section 7.1.2.1 of this report.

7.1.2.3.2 General Evaluation of Software Development Activities

In NEDE-33226P and NEDE-33245P, the applicant states that it conforms to BTP HCIB-14 for the software development activities. The stated purpose of the LTRs is to provide a general template for the development of project-specific plans. The template should generically present the same information as will be found in project-specific plans. The NRC staff's review of the LTRs is to determine that they do provide this information and give adequate direction for the development of the project-specific plans.

The NRC staff verified that all planning documents from BTP HICB-14 are contained in NEDE-33226P and NEDE-33245P. The applicant combines BTP HICB-14, SMaintP and SOP documents into the software operations and maintenance plan (SOMP). The applicant refers to the BTP HICB-14 SInstP document as the software installation plan (SIP). NEDE-33226P details the information included in the SMP, SDP, SIntP, SIP, SOMP, and STrngP. NEDE-33245P details the information included in the SVVP, SSP, and SCMP.

The applicant identifies a specific life cycle (modified waterfall model). The applicant's life cycle phases map to the life cycle activities identified in BTP HICB-14 with minor deviations. The applicant combines the integration and validation activities into a single test phase. In addition, the applicant adds a retirement phase for activities related to replacement or removal of existing software products from operation.

The applicant integrates safety analyses, verification and validation analysis and test reports, configuration management reports, and testing activities into the life cycle phases consistent with BTP HICB-14.

The applicant details design outputs developed in project-specific plans. The design outputs are consistent with BTP HICB-14.

The applicant utilizes engineering operating procedures and other internal, non docketed materials as parts of NEDE-33226P and NEDE-33245P. In RAI 7.1-76, the NRC staff requested that information in the engineering operating procedures and other internal, non-docketed materials be abstracted to eliminate uncertainty over unknown or unexpected internal document changes. In its response, the applicant provided abstracts for these internal procedures and policies in the topical report in NEDE-33226P and NEDE-33245P. The staff determined the response was acceptable since the applicant removed specific references to non-docketed material from the topical reports. Based on the applicant's response, RAI 7.1-76 is resolved. RAI 7.1-76 was being tracked as a confirmatory item in the SER with open items. The NRC staff confirmed that these changes were included in NEDE-33226P, Revision 4 and NEDE-33245P Revision 4 and the confirmatory item is closed.

7.1.2.3.3 Evaluation of Compliance with Regulations

The NRC staff reviewed the submitted LTRs for compliance with the requirements of GDC 21. BTP HICB-14 states that the relevant part of GDC 21 requires that protection systems be designed for high functional reliability commensurate with the safety function to be performed.

The guidance in BTP HICB-14 provides an acceptable method by which the applicant can show compliance with this high functional reliability part of the requirement. Based on the applicant's commitment to follow the guidance in BTP HICB-14 as detailed in NEDE-33226P and NEDE-33245P and as confirmed by NRC staff in the review of these LTRs, the NRC staff finds that the applicant has adequately addressed the requirements of GDC 21.

The NRC staff evaluated whether 10 CFR 50.55a(1); 10 CFR 50.55a(h); GDC 1; and Appendix B to 10 CFR Part 50, Criterion III, have been adequately addressed for the software development activities per BTP HICB-14. 10 CFR 50.55a(a)(1) requires that structures, systems, and components must be designed, fabricated, erected, constructed, tested, and inspected to quality standards commensurate with the importance of the safety function to be performed. 10 CFR 50.55a(h) requires compliance with IEEE Std 603-1991 and the correction sheet dated January 30, 1995. As applied to software development activities for 10 CFR 50.55a(a)(1) and GDC 1, BTP HICB-14 and SRP Appendix 7.1-A identify that the applicant should commit to conformance with the regulatory guides, codes and standards referenced in BTP HICB-14. BTP HICB-14 guidance for 10 CFR 50.55a(h) identifies the need to specify quality requirements but does not identify specific quality requirements beyond those required by 10 CFR 50.55a(a)(1) and GDC 1. As described in Section 7.1.2.3.4 of this report, the NRC staff finds that the applicant used the applicable guidance and material provided in BTP HICB-14 to develop the material in NEDE-33245P and show compliance. GDC 1 also includes requirements for a quality assurance program and the maintenance of appropriate records. NEDE-33245P, Section 1.2, states that for software development activities, NEDE-33245P supplements the applicant's quality assurance program. As described in 7.1.2.3.5 of this report, the NRC staff finds the templates for project-specific plans acceptable, and therefore the NRC staff finds Appendix B to 10 CFR Part 50, Criterion III, adequately addressed for software development activities. The evaluation of the remaining portion of the quality assurance program and appropriate records is addressed in Chapter 17 of this report. Based on the above, the NRC staff finds that the requirements 10 CFR 50.55a(1); 10 CFR 50.55a(h); GDC 1; and Appendix B to 10 CFR Part 50, Criterion III, have been adequately addressed for the software development activities.

7.1.2.3.4 Evaluation of Deviations from Guidelines and Standards

In Appendix A, "Conformance Review," of both LTRs, the applicant documented the conformance with RGs and standards as listed in BTP HICB-14 and also addressed some deviations. With the exceptions of the stated deviations, NEDE-33226P and NEDE-33245P specify conformance to the criteria and guidance contained in BTP HICB-14. , The applicant's stated deviations from applicable RGs and standards are summarized and evaluated below.

(1) BTP HICB-14

The applicant deviates from this guidance in the measurement implementation characteristic. The applicant states "the use of metrics to monitor development process is not fully implemented, since a proven system has not been identified."

NEDE-33226P, Section 3.6.4, "Project Controls," states, "Project Control activities include measurement and monitoring of project execution." This section also states that "project performance is monitored using computer-based tools and project reviews." Each plan template discussed in the LTRs also includes a statement that the plan will contain the definition of measurements and metrics. The NRC staff finds that the applicant's commitment to use metrics to monitor the development process is acceptable. The particular choice of a "computer-based

tool" is not an issue for the NRC staff evaluation.

The applicant also states that the processes and activities in NEDE-33226P and NEDE-33245P are generally consistent with IEEE Std 1228, "Standard for Software Safety Plans", IEEE Std 12207, "Standard for Information Technology - Software Life Cycle Processes", IEEE Std 1219, "Standard for Software Maintenance", and IEEE Std 1058, "Standard for Software Project Management Plans", but explicit conformance is not claimed. The NRC staff finds that the level of conformance described is acceptable.

The NRC staff reviewed the deviations for BTP HICB-14 and finds they are acceptable.

(2) RG 1.152

The applicant excludes IEEE Std 12207.0 and IEEE Std 603-1998, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Station", from stated conformance. The applicant describes this nonconformance as follows:

> [IEEE Std] 12207.0-1996, is not directly referenced. However, IEEE 1074-1995 is directly referenced by RG 1.173, and is therefore used instead of IEEE 12207. IEEE 1074-1995 covers similar topics and is the committed reference. IEEE 603-1998 addresses criteria for safety systems but is not within the scope of the SMPM and SQAPM because it does not provide guidance on software design and software quality assurance.

Since IEEE Std 12207-1996 has not been endorsed by the NRC, and the applicant followed IEEE Std 1074, "IEEE Standard for Developing Software Life Cycle Processes", which has been endorsed by RG 1.173. The NRC staff finds this deviation is acceptable.

Conformance with IEEE Std 603-1991 is required by 10 CFR 50.55a(h). IEEE Std 603 is applicable to safety systems. Safety software is a part of the overall safety system and is applicable to the development process discussed in NEDE-33226P and NEDE-33245P. In RAI 7.1-78, the NRC staff requested that the applicant directly reference IEEE 603-1991, and the correction sheet dated January 30, 1995 in NEDE-33226P and NEDE-33245P. In its response, the applicant stated that linkage to this standard will be acknowledged in NEDE-33226P and NEDE-33245P. The staff determined the response was acceptable since the applicant referenced the version required by 10 CFR 50.55a(h) in NEDE-33226P and NEDE-33245P. Based on the applicant's response, RAI 7.1-78 is resolved. RAI 7.1-78 was being tracked as a confirmatory item in the SER with open items. The NRC staff confirmed that these changes were included in NEDE-33226P, Revision 4 and NEDE-33245P Revision 4 and the confirmatory item is closed.

(3) RG 1.168

The applicant deviates from this RG in the area of software reviews. The applicant uses a different process than that outlined in IEEE Std 1028, "IEEE Standard for Software Reviews and Audits". The NRC staff compared the applicant's review process against that of the standard. Terminology differences were found to be the major deviation. The necessary information for software reviews as discussed in the standard is found in the applicant's processes. The NRC staff finds this deviation is acceptable.

The applicant also states that "within the scope of the software plans, there is no equivalent for software integrity level 4. Detailed mapping of V&V tasks to each software classification (Q, N3, and N2) is specified in Table 2 of NEDE-33245P." The applicant's Q, N3, and N2 safety classifications are discussed in NEDE-33245P.

The NRC staff's review and comparison of the tasks listed by the applicant for software classifications Q, N3, and N2 show that they are equivalent in scope to those detailed for the appropriate integrity levels of IEEE Std 1028. The NRC staff finds this deviation is acceptable.

(4) RG 1.169

The applicant deviates from the specified SCMP outline in IEEE Std 828, "IEEE Standard for Configuration Management Plans".

NEDE-33245P, Section 6.0, "SCMP," was reviewed against IEEE Std 828, particularly Section 5.0, "Conformance to the Standard." The general information discussed in IEEE Std 828 was found to be present in the SCMP template discussion. However, conformance cannot be claimed per IEEE Std 828, Section 5.4, "Conformance Declaration."

The main deviation is that the applicant's "sequence of information" is different from the sequence in the standard, and no explicit cross-reference is provided (IEEE Std 828, Section 5.1). Additionally, all plan information will not be included in a single document, because internal applicant procedures are referenced and augmented by the SCMP.

However, the applicant's proposed outline does meet the IEEE Std 828, Section 5.3, "Consistency Criteria," and provides the basic information discussed in the standard. The deviation from Section 5.4 is considered minor. The NRC staff finds this deviation is acceptable.

(5) RG 1.172

RG 1.172 endorses IEEE Std 830-1993, "IEEE Recommended Practice for Software Requirements Specifications". Section 4.3.5 of IEEE Std 830 discusses ranking software requirements specifications for importance and stability. This ranking is used for allocation of development/design effort. The applicant does not utilize this metric to determine allocation of effort. NEDE-33245P, Section 1.5, identifies alternative criteria for the classification of software, resulting in three classes of software. In NEDE-33226P, Section 5.7.5, the applicant commits to applying an appropriate level of design/development effort to each identified requirement to "achieve a high degree of functional reliability and design quality" as per IEEE Std 830. The classes of software and the level of effort applied to each is evaluated in Section 7.1.2.3.7 of this report and found to be acceptable

The NRC staff reviewed the deviation for RG 1.172 and finds it acceptable.

(6) RG 1.173

The applicant uses names for some life cycle phases that are different from the terms in IEEE Std 1074. These differences are based on an attempt to maintain consistency with the applicant's internal procedures for software development activities, as well as address naming inconsistencies between RGs and standards. The NRC staff's review finds that the primary differences just affect the names, and the information represented is equivalent.

The NRC staff reviewed the deviation for RG 1.173 and finds it acceptable.

7.1.2.3.5 Evaluation of Templates for Project-Specific Plans

As stated, the primary purpose of these LTRs is to provide guidance and direction to produce project-specific plans that meet the acceptance criteria of BTP HICB-14. Therefore, each document description detailed in NEDE-33226P and NEDE-33245P has been reviewed for expected content against BTP HICB-14 and associated RGs. In particular, the templates for component plans were examined to confirm that they adequately address the management, implementation, and resource characteristics as addressed in BTP HICB-14 and that the elements of BTP HICB-14 are incorporated into NEDE-33226P and NEDE-33245P. Applicant deviations for RGs were also considered in the review of the templates for component plans.

NEDE-33226P templates for component plans have been evaluated by the NRC staff as follows:

(1) SMP

The SMP is discussed in Section 3.0 of NEDE-33226P. The purpose of the SMP is to establish the managerial process and provide overall technical direction for software development activities. The NRC staff reviewed the material discussed and finds that the elements of BTP HICB-14 for an SMP are incorporated into NEDE-33226P guidance. The NRC staff also finds that any SMP developed under NEDE-33226P procedures will meet the requirement for a sufficient SMP as outlined in BTP HICB-14. Accordingly, the NRC staff finds that the SMP component of NEDE-33226P is acceptable.

(2) SDP

The SDP is discussed in Section 5.0 of NEDE-33226P. The NRC staff reviewed this section of NEDE-33226P and finds that the SDP material conforms to the guidance in IEEE Std 1074-1995, as endorsed by RG 1.173. The SDP material was also reviewed against RGs 1.152 and 1.172. The NRC staff finds that any SDP developed under NEDE-33226P procedures will meet the requirement for a sufficient SDP as outlined in BTP HICB-14. Accordingly, the NRC staff finds that the SDP component of NEDE-33226P is acceptable.

(3) SIntP

The SIntP is discussed in Section 6.0 of NEDE-33226P. The purpose of the SIntP is to provide a description of the software integration process, the hardware/software integration process, and the goals of these processes. The NRC staff reviewed the SIntP material provided in NEDE-33226P and finds that the necessary information is discussed and identified. The NRC staff finds that project-specific SIntPs developed under NEDE-33226P will meet the requirements for SIntPs as outlined in BTP HICB-14. Accordingly, the NRC staff finds that the SIntP component of NEDE-33226P is acceptable.

(4) SIP

This SIP is referred to as the SInstP in BTP HICB-14 and is discussed in Section 7.0 of NEDE-33226P. The NRC staff reviewed this section of NEDE-33226P and finds that the SIP material contains the necessary information and guidance for developing project-specific SIPs

as identified in BTP HICB-14. Accordingly, the NRC staff finds that the SIP component of NEDE-33226P is acceptable.

(5) SOMP

The SOMP is a combination of the SOP and SMaintP as described in BTP HICB-14 and is discussed in Section 8.0 of NEDE-33226P. The activities used to operate and maintain software products during plant operation are covered by this material. The NRC staff reviewed this section of NEDE-33226P and finds that the material contains the necessary information and guidance for developing project-specific SOMPs as identified in BTP HICB-14. Accordingly, the NRC staff finds that the SOMP component of NEDE-33226P is acceptable.

(6) STrngP

The STrngP is discussed in Section 9.0 of NEDE-33226P. The purpose of the STrngP is to ensure that adequate NRC staff training, including training for plant operators, I&C engineers, and technicians, is achieved. The NRC staff reviewed the STrngP material provided in NEDE-33226P and finds that the necessary information is discussed and identified. The NRC staff finds that project-specific STrngPs developed under NEDE-33226P will meet the requirements as outlined in BTP HICB-14. Accordingly, the NRC staff finds that the STrngP component of NEDE-33226P is acceptable.

NEDE-33245P templates for component plans have been evaluated by the NRC staff as follows:

(7) SQAP

The SQAP is discussed in Section 3.0 of NEDE-33245P. The NRC staff reviewed this section of NEDE-33245P and finds that the software quality assurance activities conform with the requirements of Appendix B to 10 CFR Part 50 and the applicant's overall quality assurance program. Accordingly, the NRC staff finds that the SQAP component of NEDE-33245P is acceptable.

(8) SVVP

The SVVP is discussed in Section 5.0 of NEDE-33245P. The NRC staff reviewed this section of NEDE-33245P and finds that the activities are consistent with RG 1.168 and the guidance provided by IEEE Std 1012, "IEEE Standard for Software Verification and Validation". Accordingly, the NRC staff finds that the SVVP component of NEDE-33245P is acceptable.

(9) SSP

The SSP is discussed in Section 4.0 of NEDE-33245P. The NRC staff reviewed this section of NEDE-33245P and finds that the software safety activities are consistent with RG 1.173 and are consistent with the guidance provided by IEEE Std 1228. Accordingly, the NRC staff finds that the SSP component of NEDE-33245P is acceptable.

(10) SCMP

The SCMP is discussed in Section 6.0 of NEDE-33245P. The NRC staff reviewed this section of NEDE-33245P and finds that the configuration management activities are consistent with

RG 1.169 and the guidance provided by IEEE Std 828 and IEEE Std 1042, “IEEE Guide to Software Configuration Management”. Accordingly, the NRC staff finds that the SCMP component of NEDE-33245P is acceptable.

(11) STP

A separate STP is not specifically listed in BTP HICB-14. The applicant has provided details on its STP in Section 7.0 of NEDE-33245P. The NRC staff reviewed this section of NEDE-33245P and finds that the software test activities are consistent with RG 1.170, which endorses IEEE Std 829-1983, “IEEE Standard for Software Test Documentation” and RG 1.171, which endorses IEEE Std 1008-1987, “IEEE Standard for Software Unit Testing”. Accordingly, the NRC staff finds that the STP component of NEDE-33245P is acceptable.

Based on the acceptability of the guidance for the project-specific plans, NEDE-33226P and NEDE-33245P are acceptable. The NRC staff review of the LTRs finds that these documents provide high level template guidance. This determination is based on the identification of the activities specified in BTP HICB-14 as required for project-specific plans.

7.1.2.3.6 Evaluation of Software Development Activities DAC/ITAAC

The applicant has chosen to use the DCD Tier 1, DAC/ITAAC process to allow completion of both system and project-specific design activities, as well as the completion of verifiable activities through the project-specific and system operational phases after the finalization of this evaluation.

The necessary DAC/ITAAC items are derived from the BTP HICB-14 process and resulting documents. Sufficient DAC/ITAAC are required to allow the NRC staff to confirm (1) that acceptable plans were prepared to control software development activities, (2) that the plans were followed in an acceptable software life cycle, and (3) that the process produced acceptable design outputs. These three areas are covered in DCD, Tier 1, Section 3.2, with the exception of the open item noted below.

NEDE-33226P and NEDE-33245P provide templates for completing specific project plans. DCD, Tier 1, Section 3.2, provides the DAC/ITAAC to confirm the completion of acceptable specific project plans with the necessary management, implementation, and resource characteristics.

NEDE-33226P and NEDE-33245P describe the documents and the review processes to be completed for each life cycle phase. DCD, Tier 1, Section 3.2, provides the DAC/ITAAC to allow future confirmation that the plans were properly followed and the accomplishments documented.

NEDE-33226P and NEDE-33245P describe the design outputs that will be produced. DCD, Tier 1, Section 3.2, provides the DAC/ITAAC to confirm that design outputs have the necessary functional and process characteristics. The DAC/ITAAC in DCD, Tier 1, Section 3.2, also provide confirmation that the software development activities as a whole were implemented consistently with NEDE-33226P and NEDE-33245P and the guidelines of BTP HCIB-14.

However, in DCD Revision 5, there were no DAC/ITAAC items explicitly established for creating the specific project plans from the templates. Also, it was not clear if closure activities would take place on a project basis, a life cycle phase basis, or system wide. Additionally, the

provided DAC/ITAAC are not clear as to the delineation between design and inspection tasks. Therefore, in RAI 14.3-402 and RAI 14.3-418, the NRC staff requested the applicant to provide the DAC/ITAAC coverage for the templates and clearly relate the template to the project-specific implementation process, including the closure process. Additionally, the NRC staff requested that the DAC/ITAAC tasks be more clearly described and criteria adequately allocated to the specific DAC and/or ITAAC tasks. RAI 14.3-418 was being tracked as a open item in the SER with open items. In its responses to RAI 14.3-402 and RAI 14.3-418, the applicant updated the DCD Tier 1 and Tier 2 documentation to align them with the software project life cycles and to ensure that each corresponding DAC will be closed prior to completion of a software life cycle phase. The staff determined the response were acceptable since the applicant aligned the DAC with the software project life cycle process described in NEDE-33226P and NEDE-33245P. Based on the applicant's response, RAIs 14.3-402 and 14.3-418 are resolved. The NRC staff confirmed that these changes were included in DCD Revision 6. With the resolution of the above RAIs, the NRC staff finds the DCD Tier 1, DAC/ITAAC for software development activities acceptable.

7.1.2.3.7 Evaluation of Software for Non-safety System

SRP Section 7.7, states that control system software should be developed using a structured process similar to that applied to safety system software. Elements of the review process may be tailored to account for the lower safety significance of control system software. NEDE-33245P, Table 1.5-1, identifies three classes of software: (1) Class Q which is safety-related software; (2) Class N3 which is non-safety systems software whose failure could challenge safety systems; and (3) Class N2 which is other non-safety systems software. NEDE-33245P, Section 1.5, identifies additional criteria for the classification of software. The NRC staff finds the software classes acceptable.

The NRC staff verified that non-safety systems software is developed using a structured process. NEDE-33226P and NEDE-33245P describe the software development process for all three software classes and how it varies by software class. In NEDE-33245P, Tables 1-1 to 1-7, show that all software life cycle phases and design outputs identified in BTP HICB-14 are produced for the three classes.

The NRC staff also evaluated the differences between the software classes. The primary differences between the treatment of safety and non-safety software is in the responsibilities for performing V&V tasks and the types of V&V tasks performed. For safety software, NEDE-33245P, Section 3.2.3, states that the V&V tasks are conducted by a team that is organizationally independent of those who perform the design of the software product. For non-safety software, NEDE-33245P, Section 3.2.3, states that the V&V tasks are conducted by individual(s) or group(s) other than those who perform the design of the software product. NEDE-33245P, Tables 1-1 to 1-7, shows how the responsibilities for performing software tasks vary by software class. NEDE-33245P, Table 2, shows how the types of V&V tasks vary by software class during the software life cycle phase. The NRC staff finds the differences in the performance of V&V tasks based on software class acceptable.

A secondary area of the differences between software class is in the level of qualification for development tools. NEDE-33245P, Section 4.2.9, identifies that the software tools used in the development and evaluation of software class Q and N3 software are evaluated for suitability. NEDE-33226P, Section 5.7.9, describes different levels of qualification documentation for software tools based on software class. The NRC staff finds the differences in the qualification of software tools based on software class acceptable.

Based on the defined software classes, the implementation of the life cycle process for all software classes, and the defined differences between software classes, the NRC staff finds that NEDE-33226P and NEDE-33245P provide a structured process for developing non-safety system software, including control system software, that is appropriately tailored for safety significance and therefore are acceptable.

7.1.2.4 Conclusion

The applicant has identified deviations from some of the BTP HCIB-14 guidance. These deviations have been reviewed and found acceptable. Based on this determination, the NRC staff finds that the applicant's DCD software development activities are consistent with BTP HCIB-14 and associated regulatory guidance. Consistency with this BTP and associated guidance ensures compliance with the applicable requirements of IEEE Std 603, as required by 10 CFR 50.55a(h). As discussed in Section 7.1.2.3 above, the NRC staff concludes that the applicant has adequately addressed the relevant requirements of 10 CFR 50.55a(a)(1); 10 CFR 50.55a(h); GDC 1 and 21; and 10 CFR Appendix B, Criterion III for software development activities. The applicant also adequately addressed the guidelines in RG 1.152, RG 1.168, RG 1.169, RG 1.170, RG 1.171, RG 1.172, and RG 1.173.

The information provided in the NEDE-33226P and NEDE-33245P and the DCD Tier 1, DAC/ITAAC for software development activities are sufficient to confirm (1) that acceptable plans are prepared to control software development activities, (2) that the plans are followed in an acceptable software life cycle, and (3) that the process produces acceptable design outputs. The NRC staff finds that there is reasonable assurance that the applicant's software development activities will result in high quality safety system software. Accordingly, the NRC staff concludes that the software development activities and the associated DCD Tier 1, DAC/ITAAC are acceptable.

7.1.3 Diversity and Defense-in-Depth Assessment

7.1.3.1 Regulatory Criteria

In SRP Chapter 7, the NRC staff position on D3 was established in the guidelines of BTP HCIB-19. This position was based on the agency's policy prescribed in the SRM on Item II.Q of SECY-93-087. As a result of the reviews of ALWR design certification applications for designs that use a digital protection system, the NRC has established the following four-point position on D3 for digital computer-based I&C systems:

Point 1: The applicant/licensee should assess the D3 of the proposed I&C system to demonstrate that vulnerabilities to CCF have been adequately addressed.

Point 2: In performing the assessment, the vendor or applicant/licensee should analyze each postulated CCF for each event that is evaluated in the accident analysis section of the SAR using best-estimate or DCD, Tier 2, Chapter 15 analysis methods. The vendor or applicant/licensee should demonstrate adequate diversity within the design for each of these events.

Point 3: If a postulated CCF could disable a safety function, a diverse means, with a documented basis that the diverse means is unlikely to be subject to the same CCF, should be required to perform either the same function as the safety system function

that is vulnerable to CCF or a different function that provides adequate protection. 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.

Point 4: A set of displays and controls located in the MCR should be provided for manual system-level actuation of critical safety functions and for monitoring of parameters that support safety functions. The displays and controls should be independent and diverse from the computer-based safety systems identified in Points 1 and 3.

The purpose of BTP HCIB-19 is to provide guidance for evaluating an applicant/licensee's D3 assessment and the design of manual controls and displays to ensure conformance with the NRC position on D3 for I&C systems incorporating digital computer-based RPS or ESFAS. BTP HCIB-19 has the objective of confirming that vulnerabilities to CCFs have been addressed in accordance with the guidance of the SRM on SECY-93-087 and specifically the following:

- Verify that adequate diversity has been provided in a design to meet the criteria established by the NRC's requirements.

- Verify that adequate defense-in-depth has been provided in a design to meet the criteria established by the NRC's requirements.

- Verify that the displays and manual controls for critical safety functions initiated by operator action are diverse from the primary protection systems.

7.1.3.2 Summary of Technical Information

The applicant originally submitted NEDO-33251 in July 2006. By letter MFN-09-359, dated June 9, 2009, the applicant submitted Revision 2 of NEDO-33251.

The applicant's D3 assessment is based on the following:

- PRA methods were used to consider the role of both safety and non-safety equipment in the prevention and mitigation of transients and faults. For the design, this consideration has been reflected in the overall design of the plant DCIS and mechanical systems.

- The non-safety DPS provides a reactor trip and ESF actuations diverse from the Q-DCIS. The DPS is included to support the design risk goals by reducing the probability of a severe accident that potentially results from the unlikely coincidence of postulated transients and postulated CCFs.

NEDO-33251 provides I&C system architecture that includes the Q-DCIS and the N-DCIS. The proposed DPS is triple-redundant, non-safety, and diverse from and independent of the Q-DCIS. The DPS provides an alternate means of initiating reactor trip and actuating selected ESF systems and providing plant information to the operator. The NRC staff's evaluation of the DPS is addressed in Section 7.8 of this report.

In NEDO-33251, Section 2, “Architecture/System Description,” and Section 3, “Defense-in-Depth Features,” which contain guidelines, requirements, and recommendations, address compliance with NUREG-0493, “A Defense-in-Depth & Diversity Assessment of the RESAR-414 Integrated Protection System” and compliance with NUREG/CR-6303, “Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems”, Section 4, addresses the specific compliance with NUREG/CR-6303. Section 5, addresses specific design features to satisfy the defense-in-depth requirements. Appendix A documents the assessment of each postulated CCF for events that are evaluated in the DCD, Tier 2, Chapter 15, analyses assuming CCF of a digital protection system.

7.1.3.3 NRC Staff Evaluation

BTP HCIB-19 includes NRC’s four-point position on D3 and the NRC staff acceptance criteria. The NRC staff evaluated each of the four points using BTP HCIB-19.

Point 1: The applicant/licensee should assess the D3 of the proposed I&C system to demonstrate that vulnerabilities to CCFs have been adequately addressed.

The NRC staff evaluated the applicant’s D3 analysis using the criteria in BTP HCIB-19 and NUREG/CR-6303. BTP HCIB-19 emphasizes the review of the following topics:

(1) System Representation as Blocks

The NRC staff evaluated the system representation as described in NEDO-33251, Sections 2.6 and 4.1, and Table 4.2. The NEDO-33251 block structure is consistent with NUREG/CR-6303, Sections 2.2 and 2.5. The NRC staff finds this acceptable.

In NEDO-33251, Section 2.6, the applicant documents conformance to the NUREG/CR-6303 echelon of defense structure and to the NUREG/CR-6303 block structure. The four echelons are divided into three levels containing the non-safety systems, safety systems, and non-safety diverse systems that provide automatically and manually actuated functions to support them. The functions assigned to the I&C systems are implemented by processor-based subsystems, which are placed within a structure of separate cabinets and the DCIS rooms. The applicant maps the echelons of defense to the I&C architecture and illustrates the relationship between these subsystems and cabinets and the block structure and shows the assignment of equipment to the blocks for each level within the echelons of defense. The NRC staff finds that the applicant has properly mapped the echelons of defense in accordance with the NUREG/CR-6303 guidance.

(2) Documentation of Assumptions

The NRC staff evaluated the acceptability of assumptions documented in the D3 analysis. For example, in Appendix A to NEDO-33251, the applicant provided preliminary evaluation of the DCD, Tier 2, Chapter 15, AOOs and DBAs assuming CCF of the Q-DCIS. The preliminary evaluation is acceptable because the assumptions are bounded by Chapter 15 analyses. DCD, Tier 1 Table 2.2.14-4, Item (8) documents the ITAAC for confirmatory analyses support and will validate the DPS design scope. The evaluation will be finalized when design details are final and confirmatory analyses are completed. In Section 4.7 (NUREG/CR-6303 approach), the applicant assumes no protective action initiated as the result of CCF in the Q-DCIS. DCD, Tier 1, Revision 5, Table 2.2.14-4, provided DAC/ITAAC for the applicant to perform FMEAs of the Q-DCIS to confirm the identified DPS functions and DAC/ITAAC for the applicant to perform

confirmatory analyses to confirm that the DPS design ensures releases during a common mode protection system failure coincident with the DBEs discussed in DCD Chapter 15 are within the 10 CFR Part 100 limits (or percentage thereof) as specified in BTP HCIB-19. However it was not clear that the events and confirmatory analyses are related to specific I&C such that the DAC process would be applicable. In RAI 7.1-135, the NRC staff requested that the applicant justify the use of the DAC process for the analyses in NEDO-33251, Table A1, including clarifying how each event is related to specific I&C. RAI 7.1-135 was being tracked as an open item in the SER with open items. In its response, the applicant clarified that the DCD Chapter 15 events are sufficiently analyzed to determine what DPS actions are required to meet the radiological criteria and that the confirmatory evaluation does not fall under the DAC process. DCD, Tier 1, Table 2.2.14-4, was revised to no longer designate any items as DAC. The separate ITAAC for confirmatory analyses and FMEAs were consolidated into an ITAAC for the applicant to complete a FMEA per NUREG/CR-6303 of the Q-DCIS to validate the DPS protection functions. The staff determined the response was acceptable because the revised ITAAC in DCD, Tier 1 Table 2.2.14-4, Item (8) covers the complete DPS design scope. Based on the applicant's response, RAI 7.1-135 is resolved. The staff confirmed that Revision 2 of NEDO-33251 clearly identifies that the DCD Chapter 15 events are evaluated based on the credible failures identified from the final protection system design. NEDO-33251, Table A1 is deleted to eliminate the ambiguity. Based on the changes made in Revision 2 of NEDO-33251, the NRC staff finds that the applicant's documentation of assumptions acceptable.

(3) Postulated CCFs

The NRC staff evaluated the selection of CCFs used in the analysis. (Note that with regard to D3 analyses, the terms CCFs and common mode failures (CMFs) are used interchangeably. NEDO-33251, Section 4, describes the CCF scenarios considered in the NUREG/CR-6303 analysis:

- Postulated CCF of processor-based subsystems (failure occurs in all similar subsystems) - Entire system fails to perform protective functions.

- Postulated CCF in I&C architecture, in conjunction with random failures - Results are pending final hardware/software selection; however, PRA results are favorable with regard to CCFs.

- Postulated CCF within the Q-DCIS - No protective actions are initiated; the DPS provides protective actions.

- Postulated accident in conjunction with CCF of the Q-DCIS and the DPS failure - I&C strategy still enables safe shutdown (with operator input).

- Postulated event (requiring reactor trip) with CCF in the RPS function of the Q-DCIS - DPS trips reactor.

- Postulated event (requiring ESF) with CCF in the SSLC/ESF function of the Q-DCIS - DPS initiates ESF.

The NRC staff finds the selection of CCF scenarios to be acceptable.

(4) Effect of Other Blocks

The NRC staff evaluated the blocks assumed to function correctly. NEDO-33251, Section 4.7, states that within the ESBWR I&C architecture, with no sharing of signals between the safety systems and the DPS, CCF within the Q-DCIS would prevent the Q-DCIS from initiating any protective action (a conservative assumption). The NRC staff finds the treatment of other blocks acceptable.

(5) Identification of Alternate Trip or Initiation Sequences

The NRC staff evaluated the selection of sequences in NEDO-33251, Appendix A. The event sequences evaluated are consistent with DCD, Tier 2, Revision 4, Chapter 15. DCD, Tier 2, Revision 5, Chapter 15, reordered its list of sequences. For example, DCD, Tier 2, Revision 4, Chapter 15 and NEDO-33251, Appendices A and B identify that there are no reactor and power distribution anomalies. However, DCD, Tier 2, Revision 5, Chapter 15 identifies two reactor and power distribution anomalies, "Control Rod Withdrawal Error During Startup," and "Control Rod Withdrawal Error During Power Operation." In RAI 7.1-131, the NRC staff requested that NEDO-33251 be revised to ensure that the events and accidents evaluated in the D3 analysis is consistent with DCD, Tier 2, Chapter 15. The NRC staff has not identified the need for additional sequences. RAI 7.1-131 was being tracked as an open item in the SER with open items. in its response, the applicant indicated that it would update the evaluation of Chapter 15 events in NEDO-33251 to be consistent with DCD, Tier 2, Chapter 15. The staff determined the response was acceptable since the applicant revised NEDO-33251 to be consistent with DCD, Tier 2, Chapter 15. Based on the applicant's response, RAI 7.1-131 is resolved. Based on the changes made in Revision 2 of NEDO-33251, the NRC staff finds that the applicant's identification of alternate trip or initiation sequences acceptable.

(6) Identification of Alternative Mitigation Capability

The NRC staff evaluated the selection of alternative mitigation actuation functions. NEDO-33251, Appendix A, describes the potential CCF for each DBE in DCD, Tier 2, Chapter 15. Appendix A also describes the associated alternative mitigation function provided by the DPS to prevent or mitigate core damage and unacceptable release of radioactivity. DCD Tier 2, Section 7.8.1.2, describes comparable alternative mitigation functions in the description of the DPS. NEDO-33251, Appendix A, identifies that the D3 analysis needs to be updated when design details are finalized (e.g., hardware platforms and details of the hardware components are determined, and failure modes and effects are better known or evaluated). DCD, Tier 1, Table 2.2.14-4 includes the ITAAC for the applicant to perform FMEAs of the Q-DCIS to confirm the identified the DPS functions. The NRC staff find the identification of alternative mitigation capability acceptable.

In conclusion, for BTP HCIB-19,

Point 1, the NRC staff finds that the applicant appropriately addressed the guidelines in NUREG/CR-6303,

Point 2, in performing the assessment, the vendor or applicant/licensee should analyze each postulated CCFs for each event that is evaluated in the accident analysis section of the SAR using best-estimate or SAR Chapter 15 analysis methods. The vendor or applicant/licensee should demonstrate adequate diversity within the design for each of these events.

The NRC staff evaluated the methods used to analyze postulated failures. NEDO-33251 uses best-estimate methods. The NRC staff finds the use of these methods acceptable since it is

consistent with the NRC position. The NRC staff evaluated the applicant's demonstration of diversity. The applicant uses a three-layered diversity approach as outlined in NEDO-33251, Section 5.2.1, the N-DCIS for monitoring and control of non-safety functions; the Q-DCIS for reactor trip, ESF, and safety monitoring; and the DPS for non-safety reactor trip functions, actuation of ESF, and operator displays. The DPS is specifically implemented in hardware and software that is diverse from and independent of that used in the Q-DCIS. The NRC staff finds the demonstration of diversity acceptable. Accordingly, the NRC staff finds that Point 2 has been adequately addressed,

Point 3, If a postulated CCF could disable a safety function, a diverse means, with a documented basis that the diverse means is unlikely to be subject to the same CCF, should be required to perform either the same function as the safety system function that is vulnerable to CCFs or a different function that provides adequate protection. The diverse or different function may be performed by a non-safety system if the system is of sufficient quality to perform the necessary function under the associated event conditions.

The NRC staff evaluated the means to ensure sufficient quality to perform the necessary function under the associated event conditions. As an example, NEDO-33251, Section 5.3, and DCD, Tier 2, Section 7.8.1, identify the use of the ATWS/SLC logic to accomplish the reactor shutdown function as a diverse method from the Q-DCIS platform (the RPS shutdown). The NRC staff finds this acceptable. Accordingly, the NRC staff finds that Point 3 has been adequately addressed.

Point 4, a set of displays and controls located in the MCR should be provided for manual system-level actuation of critical safety functions and for monitoring of parameters that support safety functions. The displays and controls should be independent and diverse from the computer-based safety systems identified in Points 1 and 3.

The NRC staff evaluated whether a set of displays and controls located in the MCR is provided for manual system-level actuation of critical safety functions and for monitoring of parameters that support safety functions. DCD, Tier 2, Section 7.8.1, identifies that the DPS provides diverse monitoring and indication of critical safety functions and process parameters required to support manual operations and assessment of plant status. Additionally, all safety systems have displays and controls located in the MCR that provide manual system-level actuation of their safety functions and monitoring of parameters that support those safety functions. The NRC staff finds this to be acceptable.

The NRC staff evaluated whether the displays and controls are diverse from and independent of the computer-based safety systems identified in Points 1 and 3.

In addition to the manual controls and displays for the safety reactor trip and ESF functions, DCD, Tier 2, Section 7.8.1, states that the DPS also has displays and manual control functions that are diverse from and independent of those of the safety protection and SSLC/ESF functions. They are not subject to the same CCF as the safety protection system components. The manual controls include the manual initiation of the SRV, DPV, GDCS and SLC system valves, and the ICS. The operator is provided with a set of diverse displays separate from those supplied through the safety platforms. The DPS displays provide independent confirmation of the status of major process parameters. The NRC staff finds this acceptable. Accordingly, the NRC staff finds that Point 4 has been adequately addressed.

7.1.3.4 Conclusion

Based on the review of the DCD and NEDO-33251, the NRC staff finds that the applicant has adequately addressed the relevant guidelines of SRM SECY-93-087, Item II.Q, and BTP HCIB-19 (including the NRC's D3 four-point position). The applicant addressed how the design conforms to the guidelines and recommendations discussed in NUREG/CR-6303. Therefore, the NRC staff finds the applicant's D3 assessment acceptable.

7.1.4 Setpoint Methodology

7.1.4.1 Regulatory Criteria

The objective of the review of NEDE-33304P, "GEH ABWR/ESBWR Setpoint Methodology," Revision 4 is to confirm that the applicant's setpoint methodology satisfies regulatory acceptance criteria, guidelines, and performance requirements to protect the integrity of physical barriers that guard against the uncontrolled release of radioactivity. The NRC staff evaluated the applicant's setpoint methodology based on the guidelines prescribed in Standard Review Plan (SRP) Branch Technical Position 7-12. The following regulatory requirements and guidance documents are applicable to the NRC staff's review of the applicant's ESBWR setpoint methodology:

GDC 13 requires, in part, that instrumentation be provided to monitor variables and systems, and that controls be provided to maintain these variables and systems within prescribed operating ranges.

GDC 20 requires, in part, that the protection system be designed 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.

Paragraph (c)(1)(ii)(A) of 10 CFR 50.36, "Technical Specifications," requires that the TS include limiting safety systems settings (LSSS). This paragraph specifies, in part, that "where a limiting safety 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." Accordingly, the setpoints for instrument channels that initiate protective functions must be properly established in the setpoint methodology.

Paragraph (c)(3) of 10 CFR 50.36 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.

10 CFR 50.55a(h) requires compliance with IEEE Std 603-1991 and the correction sheet dated January 30, 1995. Section 4.4 of IEEE Std 603 requires identification of the analytical limit associated with each variable. Section 6.8.1 requires that allowances for uncertainties between the analytical limit and device setpoint be determined using a documented methodology.

RG 1.105 describes a method acceptable to the NRC staff for complying with the NRC's regulations for ensuring that setpoints for safety instrumentation are initially within and remain within the TS. This RG endorses Part 1 of ISA-S67.04-1994, "Setpoints for Nuclear Safety-Related Instrumentation Used in Nuclear Power Plants". ISA-S67.04-1994, Part II, "Methodology for the Determination of Setpoints for Nuclear Safety-Related Instrumentation," provides additional guidance, but was not endorsed by the NRC staff.

7.1.4.2 Summary of Technical Information

The applicant's setpoint methodology computation method is based on a statistical, probabilistic approach. The setpoint methodology combines the uncertainty components to determine the allowance and trip settings including tolerances for the functions of the safety-related systems. All appropriate and applicable uncertainties have been considered for each safety-related function. The methodology used to combine the uncertainty components for a channel is an appropriate combination of those groups that are statistically and functionally independent. The basic algorithm to combine the independent and random uncertainty components is the square-root-sum-of-squares (SRSS) technique. The uncertainties that are not independent are conservatively treated by arithmetic summation and then systematically combined with the independent terms. The appropriate uncertainties, as defined by a review of the plant baseline design input documentation, have been included in each safety function uncertainty calculation. This setpoint methodology utilized ISA-RP67.04.02-2000, "Setpoint for Nuclear Safety-Related Instrumentation." as a guideline. The latest version of RG 1.105, Revision 3, endorses Part 1 of ISA-S67.04-1994.

The applicant's setpoint methodology describes the establishment of setpoints and the relationships between nominal trip setpoints (NTSPs), allowable value (AV), as-left tolerance (ALT), as-found tolerance (AFT), analytical limit (AL), 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 limit is developed from event analyses models that consider parameters including process delays, rod insertion times, reactivity changes, and instrument response times.

The purpose of the AV is satisfied by providing enough allowance for the AL to account for those uncertainties not measured during periodic testing (channel operational test, channel functional test, and calibration test) to protect the safety limit. The AV is derived from the AL by subtracting (or adding) the SRSS of instrument uncertainties that are not measured during periodic testing. The AV is the value at which the instrument channel should be evaluated for operability to protect the safety limit when the test is performed. These periodic surveillance tests provide assurance that the analytical limit will not be exceeded if the AV is satisfied.

The limiting trip setpoint (LTSP) is the equal to the first nominal trip setpoint ($NTSP_1$) and is the the final trip setpoint ($NTSP_F$) value with the minimum required allowance to AL. The second nominal trip setpoint ($NTSP_2$) is derived from the AV by subtracting the maximum allowance AFT (AFTmax) which is defined by the SRSS of channel instrument accuracy, measurement and test equipment accuracy including error and readability, and channel instrument drift. The allowance, designated as the AFT, between the AV and $NTSP_F$ is sufficient to assure that the AV is not exceeded during surveillance testing and is small enough not to mask channel degradation. The $NTSP_F$ is derived from the AV by subtracting (adding) the AFT. The $NTSP_F$ must be more conservative than the LTSP and is between $NTSP_1$ and $NTSP_2$. The AFT is derived from assumption or design inputs used in the trip setpoint calculations that are intended to assure that there is a high confidence in future acceptable channel performance. The ALT is established by the required accuracy band (calibration accuracy) that a device or instrument channel must be calibrated to the $NTSP_F$ within during surveillance. The maximum allowance for ALT is the SRSS of channel instrument accuracy and measurement & test equipment accuracy. The as-left condition is the condition in which the instrument channel is left after

calibration or trip setpoint verification. Additionally, if the as-found value is within the as-left tolerance, then recalibration is not required. The channel will be considered inoperable if the as-found value is outside the AFT.

10 CFR 50.36(c)(1)(ii)(A) states that the 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 final nominal trip setpoint 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.

7.1.4.3 NRC Staff Evaluation

The ESBWR setpoint methodology provides acceptable criteria as follows: (1) the $NTSP_F$ must be between $NTSP_1$ and $NTSP_2$; (2) the $NTSP_F$ is the AV minus AFT; and (3) the AFT is equal to or larger than ALT. The NRC staff evaluates if the applicant's setpoint methodology provides the $NTSP_F$ as the LSSS and the AV to comply with 10 CFR 50.36(c)(1)(ii)(A). The setpoint methodology provides the $NTSP_F$, AV, AFT, and ALT for the surveillance to comply with the requirement of 10 CFR 50.36(c)(3). The setpoint methodology provides the final nominal trip setpoints to comply with the requirements of GDC 13 and GDC 20. The setpoint methodology provides the trip setpoints to comply with the requirements stated in Section 4.4 and Section 6.8.1 of IEEE Std 603. All appropriate and applicable uncertainties have been considered for each safety function. The methodology used to combine the uncertainty components for a channel is an appropriate combination of those groups that are statistically and functionally independent.

NEDE-33304P, Revision 0, identified that a graded approach would be used to apply different levels of technical rigor, probability, and confidence to various setpoints. In RAI 7.1-86, the NRC staff requested that the applicant verify that the setpoint methodology can establish setpoints with the 95/95 tolerance limit consistent with RG 1.105 for uncertainties for each of the categories in the graded approach. In the RAI response, the applicant has revised their setpoint methodology to address only the scope of all safety automatic protective device settings as well as all automatic protective device settings that meet the requirements of 10 CFR 50.36(c)(1)(ii) for technical specification required limiting safety system settings.

The applicant takes a conservative approach to establishing their setpoint methodology by adding the calibration accuracy to an allowance between the analytical limit and AV. However, the setpoint methodology uses one-sided normally distributed probability at the 95 percent level, which will have 95 percent of the uncertainties falling between -1.645 and +1.645 standard deviations in the development of nominal trip setpoints and AVs. The allowances (margins) for the setpoint calculation, using one-sided normally distributed probability compared to two-sided, are significantly decreased to 0.82 (1.645/2). The applicant's setpoint methodology is based on General Electric Instrument Setpoint Methodology, NEDC-31336-1-P, September 1996, which utilizes single-sided distributions in the development of trip setpoints and AVs. The NRC staff SER states that NEDC-31336-1-P is acceptable provided that a channel approaches a trip in one direction. The setpoint methodology uses one-sided normally distributed probability at the 95 percent level, which will have 95 percent of the uncertainties falling between -1.645 and +1.645 standard deviations in the development of nominal trip setpoints and AVs. The allowances (margins) for the setpoint calculation, using one-sided normally distributed probability compared to two-sided, are significantly decreased to 0.82 (1.645/2). In RAI 7.1-102,

the NRC staff requested that the applicant provide a clear and detailed justification for the application of a one-sided distribution to their setpoint methodology.

The NRC staff found that the applicant had not demonstrated that their setpoint methodology conforms to the 95/95 tolerance limit as an acceptable criteria for uncertainties specified in RG 1.105, Revision 3. To provide an independent evaluation, the NRC staff contracted Oak Ridge National Laboratory (ORNL) to develop a technical evaluation report evaluating the applicant's methodology with RG 1.105, Revison 3. The ORNL report confirmed the NRC staff findings, therefore, the NRC staff requested in RAI 7.1-141, that the applicant revise the setpoint methodology to remove the reduction factor of 1.645/2, or provide an alternative to RG 1.105, Revision 3 acceptance criteria. RAI 7.1-141 included the ORNL report as an attachment and superseded and closed RAIs 7.1-86 and 7.1-102. In response to RAI 7.1-141, the applicant revised NEDE-33304P to remove the reduction factor of 1.645/2 and to make corresponding changes to the supporting information. The staff determined the responses were acceptable since the applicant revised its setpoint methodology to conform to the guidelines of RG 1.105, Revision 3. Based on the applicant's responses, RAI 7.1-86, 7.1-102 and 7.1-141 are resolved**.**

DCD, Tier 1, Table 2.2.15-2, Item 21, includes the DAC/ITAAC for verifying compliance with IEEE Std 603, Section 6.8.

7.1.4.4 Conclusion

Based on the review of information in Licensing Topical Report NEDE-33304P, "GEH ESBWR Setpoint Methodology," Revision 4, the NRC staff concludes that the ESBWR setpoint methodology is acceptable and meets the applicable regulatory requirements of 10 CFR 50.36, 10 CFR 50.55a(h), and GDC 13 and 20, The staff also finds that ESBWR setpoint methodology establishes the trip setpoint so that automatic protective action will correct the abnormal situation to protect the safety limit.

7.1.5 Data Communication Systems

The data communication functions are embedded within the Q-DCIS and the N-DCIS architecture. Many of the data communication functions are discussed in Sections 7.1, 7.2, and 7.3 of DCD Tier 2. The NRC staff used SRP Section 7.9, to review the acceptability of the data communication functions of the DCIS

7.1.5.1 Regulatory Criteria

The objectives of the review are to confirm that the DCIS meets the following criteria:

- conform to applicable acceptance criteria and guidelines
- perform the safety functions assigned to them
- meet the reliability and availability goals assumed for the system
- tolerate the effects of random transmission failures

SRP Table 7-1, identifies the regulatory requirements. It states that the data communication systems addressed by SRP Section 7.9 are support systems for one or more of the systems addressed by SRP Section 7.2 through 7.8. Acceptance criteria for a specific data communication system are derived from the acceptance criteria for the systems supported by that data communication system.

The acceptance criteria are based on meeting the relevant requirements of 10 CFR 50.55a(a)(1); 10 CFR 50.55a(h); 10 CFR 50.34(f)(2)(v); 10 CFR 50.62; GDC 1, 2, 4, 13, 15, 19, 21, 22, 23, 24, 28, and 29; and 10 CFR 52.47(b)(1). The acceptance criteria are also based on conforming to the guidelines of IEEE Std 7-4.3.2, as endorsed by RG 1.152, and the SRM on SECY-93-087, Item II.Q.

A potential concern is that the transmission of multiple signals over a single path may constitute a single point of failure that may have a larger impact on plant safety than would occur in analog systems.

7.1.5.2 Summary of Technical Information

The Q-DCIS provides the data processing and transmission network that encompasses the four independent and separate data multiplexing divisions, Divisions 1, 2, 3, and 4, corresponding to the four divisions of safety electrical and I&C equipment. Each Q-DCIS division consists of the RMUs, the fiber optic cable signal transmission path, the SSLC/ESF cabinets, the RTIF cabinets, Neutron Monitoring System (NMS) cabinets, the cabinet power supplies, the safety VDUs, and safety fiber optic CIMs.

The Q-DCIS contains multiple dual-redundant fiber optic cable networks for each of the four divisions. The networks connect the RMUs with the divisional safety VDUs, the digital trip modules (DTMs), the CIMs, the safety logic test cabinets, and the N-DCIS through isolated digital gateways/datalinks.

Each Q-DCIS system is housed in a set of uniquely identified cabinets. Separate cabinets are provided for each of the four divisions and the remotely mounted components within each division.

The field sensors and process transmitters are hard-wired to the divisional local RMUs in the reactor and control buildings. At the input module of the field RMUs, the analog data are delivered to the analog input modules, and discrete data are delivered to the digital input modules. The field sensors and wiring belong to the process system they are attached to and are not part of the Q-DCIS. Analog signal conditioning, analog-to-digital conversion, and digital signal conditioning such as filtering and voltage level conversion are performed at the input modules.

Each field RMU formats and transmits input signals as data messages to the dual network and then to the RTIF, NMS, SSLC/ESF, and ICP components within its own division. The field RMUs receive the SSLC/ESF equipment control signals from the network for distribution by hard-wired connection to the equipment actuators of the ESF functions.

The corresponding divisional Q-DCIS networks send data to the RTIF, NMS, and SSLC/ESF components in separate RTIF, NMS, and SSLC/ESF divisional cabinets. The data are also sent to other safety logic equipment such as the safety logic test cabinets for control of the functional tests, the CIMs, and the isolated divisional gateways/datalinks for communication with the N-DCIS.

The N-DCIS includes a non-safety network that is segmented into parts that can work independently of one another if failures occur. The segments are not visible to the operator during normal operation. The N-DCIS uses hardware and software platforms that are different

from the Q-DCIS. The N-DCIS network is dual redundant and redundantly powered. The following are the individual N-DCIS segments:

- GENE network
- PIP A network
- PIP B network
- BOP network
- plant computer network

The segments are redundant, managed network switches into which the data acquisition, control, and displays associated with that segment are connected. All connections to these switches are through the fiber optic cable network. The switches allow the various controllers, data acquisition, and displays associated with a segment to communicate with each other. The switches' "backbone" capacity determines how many simultaneous two-way connections can be made. Only when a switch determines that an information data packet is destined for a node on another switch is the information put on an uplink to that switch. The network switches learn and maintain their own forwarding tables containing a list of all the nodes and hosts on their respective network segment. When a network switch receives a data communication packet, it forwards only that particular data communication packet to the segment to which that receiving host is connected. This mechanism prevents data traffic between devices on the network from impacting devices on other segments of the network. Specifically, the switches use a "spanning tree protocol" to automatically enable and disable ports so there is normally only one path from the nodes of one switch to another. Should a path become disabled, the switches automatically reconfigure to establish another path through the remaining switches and fiber optic cable paths. Reconfiguration requires no operator input.

The N-DCIS is not a single network. It is redundant and segmented to support the DCIS. A single failure of one of the redundant switches in a segment or multiple failures that involve no more than one switch per segment have no effect on plant operation or data. The failure is alarmed and can be repaired online. If both switches of a segment simultaneously fail, that particular segment is lost. However, the remaining segments are unaffected, and individual nodes connected to the failed switches may continue to function. The remaining switches then automatically reconfigure their uplink ports such that the remaining segments automatically find data communication paths between themselves.

7.1.5.3 NRC Staff Evaluation

7.1.5.3.1 Evaluation of Data Communication System Conformance with Acceptance Criteria - Major Design Considerations

SRP Section 7.9 lists the following thirteen major design considerations that should be emphasized in the review:

(1) Quality of Components and Modules (IEEE Std 603, Section 5.3)

The NRC staff's evaluation of the quality of components and modules presented by the quality assurance program is discussed in Section 7.1.1.3.10 of this report regarding evaluation of conformance to IEEE Std 603, Section 5.3. Also, the applicant has stated that the quality assurance program conforms to GDC 1. The evaluation of the adequacy of the quality assurance program is addressed in Chapter 17 of this report. These evaluations are applicable

to the DCIS. Accordingly, the NRC staff finds that the quality of the components and modules design consideration has been adequately addressed.

(2) DCIS Software Quality (IEEE Std 7-4.3.2, Section 5.3)

The NRC staff's evaluation of software quality is discussed in Section 7.1.1.3.10 of this report regarding evaluation of conformance to IEEE Std 603, Section 5.3 and IEEE Std 7-4.3.2, Section 5.3. This evaluation is applicable to the DCIS. Accordingly, based on the applicant's use of an acceptable software development process, as evaluated in Section 7.1.2 of this report, and its verification in the DCD, Tier 1, Section 3.2, DAC/ITAAC, the NRC staff finds that the DCIS software quality design consideration has been adequately addressed.

(3) Performance (IEEE Std 603, Section 5.5)

The NRC staff evaluated whether issues related to real-time performance have been adequately addressed for the DCIS data communication systems. The NRC staff's evaluation of software quality is discussed in Section 7.1.1.3.10 of this report regarding evaluation of conformance to IEEE Std 603, Section 5.5. This evaluation is applicable to the DCIS data communication systems. The real-time performance should be reviewed with BTP HCIB-21. DCD, Tier 2, Section 7.1.6.5, states that the system conforms to BTP HCIB-21. BTP HCIB-21 notes that (1) time delays within the DCIS and measurement inaccuracies introduced by the DCIS should be considered when reviewing setpoints, (2) data rates and data bandwidths should be reviewed including impact from environmental extremes, and (3) sufficient excess capacity margins should be available to accommodate future increases. There are assurances that the safety networks will be completely deterministic (i.e., time based as opposed to event based), as indicated in DCD Tier 2, Section 7.1.3.2.7. This section states that the Q-DCIS internal and external communication protocols are deterministic (i.e., time based as opposed to event based), which is consistent with BTP HCIB-21 guidelines.

In RAI 7.9-10, the NRC staff asked the applicant to provide the design guidelines and the design approach concerning sufficient spare memory and speed (of the processors). In its response, the applicant stated that NEDE-33226P and NEDE-33245P define a process by which plant performance requirements under various operational conditions will be specified, implemented, and tested. DCD Tier 1, Table 3.2-1, provides for verification of activities associated with NEDE-33226P and NEDE-33245P. The response also states the following:

> For non deterministic links, which may exist as part of the N-DCIS, the networks and switches will be tested in an environment that includes large amounts of extraneous data to verify that no information needed for plant safety or control is lost. The use of managed network switches in the N-DCIS networks (as indicated in DCD, Tier 2, Subsection 7.1.5.2) prevents excessive or unexpected data on these networks.

The staff determined the response was acceptable since the applicant identified an approach to ensure sufficient spare memory and speed of the processors. Based on the applicant's response, RAI 7.9-10 is resolved.

Accordingly, based on the applicant's use of an acceptable software development process, as evaluated in Section 7.1.2.3 of this report, and its verification in the DCD Tier 1, DAC/ITAAC, the NRC staff finds that the performance design consideration has been adequately addressed.

(4) Reliability (IEEE Std 603, Section 5.15)

The NRC staff evaluated whether the reliability design consideration has been adequately addressed for the DCIS. Per SRP Section 7.9, the NRC staff reviewed the effects of unneeded functions; effects of error detection and recovery; and how corrupted, missing, or duplicate messages are detected and repaired. Also, the operating history of the DCIS in similar applications should be determined to be satisfactory, but this was not addressed in DCD Tier 2. Instead, the applicant states that its commitment to reliability is ensured by the functional reliability and equipment reliability provided under the applicant's 10 CFR Part 50, Appendix B, quality assurance program. The applicant also states that BTP HCIB-14 guidance followed for software development processes achieves reliable software design and implementation. The NRC staff's evaluation of the reliability design consideration is discussed in Section 7.1.1.3.10 of this report regarding evaluation of conformance to IEEE Std 603, Section 5.15. This evaluation is applicable to the data communication systems. Accordingly, the NRC staff finds that the reliability design consideration has been adequately addressed.

(5) Time Coherency of Data

As described in NEDE-33226P, communication protocols are developed as part of the software life cycle process, and DCD, Tier 1, Section 3.2, includes the DAC/ITAAC for verifying the implementation of the software life cycle process, including products such a communication protocols. Therefore, the applicant's methods to ensure the correct sequence of data packets at receiving data communication nodes can be verified by the ITAAC process. Accordingly, the NRC staff finds that the time coherency of data design consideration has been adequately addressed.

(6) Control of Access (IEEE Std 603, Section 5.9)

The NRC staff evaluated whether control of access is adequately addressed for the DCIS communication systems. Section 5.9 of IEEE Std 603 is evaluated in Section 7.1.1.3.10 of this report. This evaluation is applicable to the data communication systems. DCD, Tier 2, Section 7.1.6.6.1.10, "Control of Access (IEEE Std 603, Section 5.9)," does provide general assurances for physical access control of the DCIS. Administrative control is used to implement access control to vital areas of the plant, including the MCR. Physical security and electronic security devices are provided to ensure only authorized and qualified plant personnel are allowed to have access to the Q-DCIS cabinets and consoles. The Q-DCIS equipment has its own access control devices. The Q-DCIS cabinets have doors with key locks and position switches. The Q-DCIS components within the cabinets have key lock switches that are used to control access to special functions.

Keys, passwords, and other security devices (following the guidance of RG 1.152) are used to control access to specific rooms; open specific equipment cabinets; obtain permission for access to enter specific electronic instruments for calibration, testing, and setpoint changes; and gain access to safety system software and data. Safety software is not routinely changed at the plant site. Opening a Q-DCIS cabinet door produces an alarm in the MCR. There is no access to safety system equipment and control through the network from non-safety system equipment. Computer-related access controls and authorization are part of the cyber-security program plan, which is described in NEDO-33295 and NEDE-33295-P. In RAI 7.1-80, the staff asked the applicant to specifically verify that there will be no remote access to any safety systems. RAI 7.1-80 was being tracked as an open item in the SER with open items. In its response, the applicant added a statement to NEDE-33295P to clarify that that there will no remote access to

safety systems. The staff determined the response was acceptable since the applicant modified NEDE-33295P to clarify that that there will no remote access to safety systems. Based on the applicant's response, RAI 7.1-80 is resolved. The NRC staff confirmed that these changes were included in NEDE-3325P, Revision 1. Based on the above, the NRC staff finds that the control of access consideration has been adequately addressed.

(7) Single Failure Criterion (IEEE Std 603, Section 5.1)

The NRC staff evaluated whether the single failure criterion, IEEE Std 603, Section 5.1, has been adequately addressed for the DCIS communication systems. The Q-DCIS contains dual redundant data communication channels per division and four redundant divisions. With the commitment to this conformity, the NRC staff believes that the channel assignments to individual communication subsystems are appropriate to assure that redundancy of and diversity from requirements are met. The NRC staff's evaluation of the single failure criterion is discussed in Section 7.1.1.3.10 of this report regarding evaluation of conformance to IEEE Std 603, Section 5.1. This evaluation is applicable to the data communication systems. Accordingly, the NRC staff finds that the single failure criterion consideration has been adequately addressed.

(8) Independence (IEEE Std 603, Section 5.6)

The NRC staff evaluated whether the independence criterion, IEEE Std 603, Section 5.6, has been adequately addressed for the DCIS communication systems. This criterion is evaluated in Section 7.1.1.3.10 of this report, where the NRC staff finds that Section 5.6 is adequately addressed on the basis of its inclusion in the safety systems design basis and its verification in the DCD Tier 1, DAC/ITAAC. This evaluation is applicable to the data communication systems. In addition, the NRC staff evaluated whether non-safety data communications could interfere with safety data communications consistent with NUREG/CR-6082, "Data Communications", Section 2.1.9.1, which states, "Interference can occur even if supposedly independent data communications systems exchange only 'handshakes' or synchronizing signals." DCD, Tier 2, Section 7.1.3.3.4, identifies time tagging as one of the two types of signals sent from non-safety to safety components in the DCIS. (Non-safety calibration data are sent from the 3D Monicore function to the safety NMS; however, the information exchange is manual and rigorously controlled.) DCD, Tier 2, Section 7.1.3.3, states the following:

> Time signals are sent to the Q-DCIS safety fiber optic CIMs through the non-safety gateways for display on the Q-DCIS (SSLC/ESF) safety VDUs and for use by the Q-DCIS to allow time tagging of data sent to the N-DCIS. These time signals are only used by the Q-DCIS for VDU indication so that all displays show the same time of day. The time signals sent from the N-DCIS to the Q-DCIS are never used to synchronize logic nor is the safety logic dependent in any way on the absence, presence, or correctness of the time signal.

In RAI 7.9-8 and 7.9-8 S01, the NRC staff requested the applicant to clarify its approach to time tagging. In its responses, the applicant responded that "The design process described in NEDE-33226P and NEDE-33245P provides hardware/software development, construction, testing, and approval processes that ensure that any time tagging delays are within the design requirements specified for each system." The staff determined the response was acceptable since the applicant clarified its approach to time tagging. Based on the applicant's response, RAI 7.9-8 is resolved. In DCD, Tier 1, Table 3.2-1, provides for verification of activities

associated with NEDE-33226P and NEDE-33245P. Accordingly, the NRC staff finds that the independence design consideration has been adequately addressed.

(9) System Testing and Inoperable Surveillance (IEEE Std 603, Section 5.7, 5.8, and 6.5)

The NRC staff evaluated whether the system testing and inoperable surveillance design consideration has been adequately addressed for the DCIS communication systems. Per SRP Section 7.9, the system testing and inoperable surveillance design consideration is addressed by conformance to IEEE Std 603, Sections 5.7, 5.8 and 6.5. IEEE Std 603, Sections 5.7, 5.8 and 6.5. are evaluated in Section 7.1.1.3.10 of this report. These evaluation is applicable to the data communication systems. Accordingly, the NRC staff finds that the system testing and inoperable surveillance design consideration has been adequately addressed.

(10) Protocols

The NRC staff evaluated whether the protocols design consideration has been adequately addressed in the software development activities. DCD, Tier 2, Section 7.1.3.2.7, states that the Q-DCIS internal and external communication protocols are deterministic. In response to RAI 7.9-10, the applicant stated, “although the N-DCIS is not deterministic, the 100 mb ethernet ports and dedicated RMUs to control processor communications make the design almost so.” The response goes on to justify this statement. In NEDE-33226P, Section 5.7.7 and 5.8.3.2 specify the characteristics of data communication protocols and intrasystem communication protocols. NEDE-33226P specifies that the external data communication protocol specification is a requirements phase output document and the intrasystem communication protocols specification is design phase output document. DCD, Tier 1, Section 3.2, provides the DAC/ITAAC to confirm the implementation of software development activities. Accordingly, the NRC staff finds that the protocols design consideration has been adequately addressed.

(11) EMI/Radiofrequency Interference (RFI) Susceptibility (IEEE Std 603, Section 5.4)

The NRC staff evaluated whether the EMI/RFI susceptibility criterion has been adequately addressed for the DCIS communication systems. This criterion is part of EQ and Section 5.4 of IEEE Std 603. IEEE Std 603, Section 5.4 is evaluated in Section 7.1.1.3.10 of this report. In addition, the NRC staff evaluated whether the specification that fiber-optic-related materials do not become brittle under radiation is included in the hardware/software specification. NEDE-33226P, in its description of the SDP, identifies that the hardware/software specification, which includes cabling requirements, will be a requirements phase output document. DCD, Tier 1, Section 3.2, provides the DAC/ITAAC to confirm the implementation of the SDP. Accordingly, the NRC staff finds that the EMI/RFI susceptibility design consideration has been adequately addressed.

(12) D3 Analysis

SRP Section 7.8 states that the D3 assessment and conformance to the SRM on SECY-93-087, Item II.Q, should be reviewed for data communication systems that are part of protection and diverse systems. The NRC staff evaluation of the D3 assessment and conformance to the SRM on SECY-93-087, Item II.Q, in Sections 7.1.3 and 7.1.1.3.7 of this report is applicable to the data communication system. The NRC staff finds that the D3 analysis of the data communication design has been adequately addressed.

(13) DCIS Exposed to Seismic Hazard

DCD Tier 2 does not specify the location of the DCIS equipment. The NRC staff evaluated whether the DCIS components are in seismic Category I structures. DCD, Tier 2, Table 3.2-1, indicates that the Q-DCIS electrical modules and cables with safety functions are seismic Category I. DCD, Tier 2, Table 3.2-1, also indicates that the N-DCIS components whose failure can potentially adversely affect seismic Category I components (e.g., in the MCR) are required to be seismic Category II. Accordingly, the NRC staff finds the exposure to seismic hazard adequately addressed.

7.1.5.3.2 Evaluation of Data Communication Systems Conformance with Acceptance Criteria - Other Criteria

SRP Section 7.9 states that the data communication system design should be evaluated for conformance to IEEE Std 603. As Section 7.1.1.3.10 of this report provides a general evaluation of conformance to IEEE Std 603, this section focuses on the specific conformance of the data communication systems and may provide additional evaluations of IEEE Std 603 criteria previously considered in this report.

The NRC staff evaluated whether the DCIS data communication systems provide proper data isolation. In RAI 7.1-65, the staff asked the applicant to describe the CIM safety-related functions and how they will be confirmed. RAI 7.1-65 was being tracked as an open item in the SER with open items. In its response, the applicant clarified that CIMs are safety signal isolation devices. The applicant revised DCD, Tier 2, Section 7.1.3.3, to clarify that the safety fiber optic CIMs are the isolation devices, including data isolation, and convert signals between electricity and light on the safety side of the fiber optic cable. These safety fiber optic CIMs are powered by the division within which they are physically located. The safety fiber optic CIMs are qualified as safety components. The applicant also revised DCD, Tier 1, Table 2.2.15-2, Item 10, to provide DAC/ITAAC to verify that the software project's interdivisional communication systems have optically isolated fiber optical communication pathways. The NRC staff determined the responses were acceptable since the applicant clarified the CIM safety-related functions and how they will be confirmed. Based on the applicant's responses, RAI 7.1-65 is resolved. The NRC staff finds that the data communication design has proper data isolation provisions.

The NRC staff evaluated whether the data communication system design has deterministic character. The deterministic character is an instrumentation response that is predictable and repeatable from sensor input to output command to the control device to actuate. For digital systems and software, a deterministic character means that a specific function is always accomplished within the required time period specified. DCD, Tier 2, Section 7.1.3.2.7 states that the DCIS data communication functions are embedded within the Q-DCIS and the N-DCIS architectures. Safety internal and external communication protocols are deterministic. The RTIF-NMS and ATWS/SLC logic automatically initiates reactor trip and the SSLC/ESF, LD&IS and VBIF logic automatically actuates the ESF that mitigate the consequence of DBEs. These automatic protection actions are implemented through 2/4 voting logic whenever one or more process variables reach their actuation setpoint. Variables are monitored and measured by each of the RTIF-NMS, ATWS/SLC, SSLC/ESF, and VBIF divisions. As documented in DCD, Tier 2, Sections 7.2.1.3.5 and 7.3.5.3.5, the real-time performance of the Q-DCIS meets the requirements for the safety system trip and initiation response in conformance with BTP HCIB-21. As part of the DAC closure process in DCD, Tier 1, Section 3.2, the applicant will define the program cycle architecture to show how the deterministic character is achieved for

each of the Q-DCIS platforms. Accordingly, the NRC staff finds that data communication design has proper deterministic character provisions.

7.1.5.3.3 Evaluation of Data Communication Systems Compliance with GDC

The NRC staff reviewed the acceptance criteria for data communication systems in SRP Section 7.9 and SRP Appendix 7.1-A. An evaluation of the conformance of the Q-DCIS to the regulations and guidelines is provided in Section 7.1.1.3 of this report. The evaluation in this section will rely upon applicable portions of the Section 7.1.1.3 evaluation and upon evaluations specific to the data communication systems consistent with SRP Section 7.9.

GDC 1 requires quality standards and maintenance of appropriate records.
10 CFR 50.55a(a)(1) requires that structures, systems, and components must be designed, fabricated, erected, constructed, tested, and inspected to quality standards commensurate with the importance of the safety function to be performed. The NRC staff evaluated whether GDC 1 and 10 CFR 50.55a(a)(1) have been adequately addressed for the data communication systems per SRP Appendix 7.1-A. SRP Appendix 7.1-A states that the NRC staff review should confirm that the appropriate regulatory guides and endorsed standards are identified as applicable for each I&C system important to safety. The NRC staff evaluation of conformance to RGs and standards for 10 CFR 50.55a(a)(1) and GDC 1 in Section 7.1.1.3.3 and 7.1.1.3.6 of this report is applicable to the data communication systems. Therefore, the NRC staff finds that the requirements of GDC 1 and 10 CFR 50.55a(a)(1) have been adequately addressed.

GDC 2 requires design bases for protection against natural phenomena. GDC 4 requires environmental and dynamic effect design bases. The NRC staff evaluated whether GDC 2 and 4 have been adequately addressed for the data communication systems per SRP Appendix 7.1-A and SRP Section 7-9. The review included the identification of those subsystems of the data communication systems that are designed to survive the effects of earthquakes, other natural phenomena, abnormal environments, and missiles. In DCD, Tier 2, Sections 3.10 and 3.11 describe the EQ programs for safety electrical and digital I&C equipment, which are evaluated in Chapter 3 of this report. DCD, Tier 1, Table 3.8-1, Items 1 and 3, includes the ITAAC for the applicant to verify the EQ of safety electrical and digital I&C equipment. Accordingly, because the applicant has identified EQ programs consistent with the design bases for the data communication systems and the ITAAC for verification, the NRC staff finds that the requirements of GDC 2 and 4 have been adequately addressed.

The NRC staff evaluated whether GDC 13 and 19 have been adequately addressed for data communication systems. GDC 13 requires providing instrumentation to monitor variables and systems over their anticipated ranges for normal operation, AOOs, and accident conditions to assure adequate safety. GDC 13 also requires providing appropriate controls to maintain these variables and systems within prescribed operating ranges. GDC 19 requires control room functionality, control room habitability, and remote shutdown capability. The evaluation of GDC 19 is provided in Section 7.1.1.3.6 of this report with the exception of data communication systems support functions necessary for operating the reactor. The applicant has identified interrelated processes to design the monitoring capability and control room controls. NEDE-33226P and NEDE-33245P, as part of a software life cycle process, define a process by which plant performance requirements under various operational conditions will be specified, implemented, and tested. DCD, Tier 1, Section 3.2, includes the DAC/ITAAC for verifying that the software plans were developed and implemented consistent with this process and produce acceptable design outputs. DCD, Tier 1, Section 3.3, includes the DAC/ITAAC for implementing an HFE design process, which includes the design and verification of controls and information

displays for monitoring variables and systems in the control room and remote shutdown panels to maintain the nuclear power unit in a safe condition during shutdown, including shutdown following an accident. Accordingly, based on the defined processes for designing the monitoring capability and the control room functions and their verification in the DCD Tier 1, DAC/ITAAC, the NRC staff finds that the requirements of GDC 13 and 19 have been adequately addressed for data communication systems.

The NRC staff evaluated whether GDC 13 and 19 have been adequately addressed for the data communication systems that support protection system functions. As described above, Sections 3.2 and 3.3 of DCD Tier 1 include the DAC/ITAAC for verifying the software development and the HFE processes associated with the design and verification of controls and information displays for monitoring variables and systems in the control room. The DCD Tier 1, DAC/ITAAC are applicable to the data communication systems for protection systems. As described in Sections 7.2 and 7.3 of this report, the DAC/ITAAC include verifying the controls for manual initiation and control of functions in the control room necessary to support actions to operate the nuclear power unit safely under normal conditions and to maintain it in a safe condition under accident conditions. Accordingly, based on the defined processes for designing the monitoring capability and the control room functions and their verification in the DCD Tier 1, DAC/ITAAC, the NRC staff finds that the requirements of GDC 13 and 19 have been adequately addressed for the data communication systems that support protection system functions.

The NRC staff evaluated whether GDC 13 and 19 have been adequately addressed for the data communication systems that support safe shutdown systems, information systems, and interlock logic important to safety, reactor control systems, and the DPS functions. As described above, Sections 3.2 and 3.3 of DCD Tier 1 include the DAC/ITAAC for verifying the software development and the HFE processes associated with the design of information displays for monitoring variables and systems and control room controls. The DCD Tier 1, DAC/ITAAC are applicable to the data communication systems for safe shutdown systems, information systems, and interlock logic important to safety, reactor control systems, and the DPS functions. As described in Sections 7.4, 7.5, 7.6, 7.7, and 7.8 of this report, the DAC/ITAAC include verification of the design and transmission of the variables and commands necessary to maintain the fission process, the integrity of the reactor core, the RCPB, and the containment and its associated systems within prescribed operating ranges during plant shutdown. The DAC/ITAAC include verification of instruments and controls within the control room to allow actions to be taken to maintain the nuclear power unit in a safe condition during shutdown, including shutdown following an accident. Accordingly, based on the defined processes for designing the monitoring capability and the control room functions and their verification in the DCD Tier 1, DAC/ITAAC, the NRC staff finds that the requirements of GDC 13 and 19 have been adequately addressed for the data communication systems that support safe shutdown systems, information systems, and interlock logic important to safety, reactor control systems, and the DPS functions.

As described in the previous three paragraphs concerning general data communications and data communication systems for protection systems, safe shutdown systems, information systems, and interlock logic important to safety, reactor control systems, and the DPS functions, based on the defined processes for designing the monitoring capability and the control room functions and their verification in the DCD Tier 1, DAC/ITAAC, the NRC staff finds that the requirements of GDC 13 and 19 have been adequately addressed.

The NRC staff evaluated whether GDC 21 has been adequately addressed for the data communication systems. GDC 21 requires that protection systems be designed for high

functional reliability and in-service testability commensurate with the safety functions to be performed. SRP Appendix 7.1-A states that GDC 21 is addressed for protections systems by conformance to IEEE Std 603 criteria except for Sections 5.4, 6.1, and 7.1. In addition, SRP Section 7.9 identifies that GDC 21 is addressed by conformance to RGs 1.22, 1.47, 1.53, and 1.118, and IEEE Std 379. DCD, Tier 2, Section 7.1, describes the conformance of the DCIS to IEEE Std 603, which is evaluated in Section 7.1.1.3.10 of this report. DCD, Tier 1, Table 2.2.15-2, includes the DAC/ITAAC for verifying that the design of the Q-DCIS complies with IEEE Std 603. In particular, in DCD, Tier 1, Table 2.2.15-2, Item 11, confirms "Sections 5.7 and 6.5, Capability for Test and Calibration." DCD, Tier 2, Table 7.1-1, identifies that the guidelines for periodic testing in RG 1.22 and RG 1.118 applies to the DCIS. The bypassed and inoperable status indication conforms to the guidelines of RG 1.47. DCD, Tier 2, Section 7.1.2.4, states that the DCIS conforms to the guidelines on the application for the single failure criterion in IEEE Std 379, as supplemented by RG 1.53. The NRC staff evaluation of conformance to RGs and standards for 10 CFR 50.55a(a)(1) is addressed in Section 7.1.1.3.3 of this report. Based on the above, the the NRC staff finds that the requirements of GDC 21 have been adequately addressed for data communication systems.

Consistent with SRP Section 7.9, the NRC staff also addressed compliance with GDC 21 through its review of the SDPs and design outputs and of conformance to RG 1.152. As discussed in Section 7.1.2 of this report, NEDE-33226P, in its description of the SDP, identifies appropriate output documentation with regard to data communications. DCD, Tier 1, Section 3.2, provides the DAC/ITAAC to confirm the implementation of the SDP. SDPs are further discussed in Section 7.1.2 of this report. Based on the identified output documentation and its confirmation in the DCD Tier 1, DAC/ITAAC, the NRC staff finds that GDC 21 and IEEE Std 7-4.3.2, as endorsed by RG 1.152, have been adequately addressed with regard to SDPs.

The NRC staff evaluated whether GDC 22 and the SRM on SECY-93-087, Item II.Q, have been adequately addressed for the data communication systems. GDC 22 requires, in pertinent part, that protection systems 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. SRP Section 7.9 identifies that GDC 22 is addressed by the review of EMI/RFI susceptibility and that seismically exposed portions of the DCIS conform to GDC 2. SRP Section 7.9 also identifies that GDC 22 is addressed by conformance to IEEE Std 603, Section 5.6, and RG 1.75. As discussed in Section 7.1.1.3.10 of this report, Items (11) and (13) in Section 7.1.5.3.1 of this report, and in the evaluation of GDC 2 above, the criteria related to EMI/RFI susceptibility and seismically exposed portions have been adequately addressed for the DCIS. In DCD, Tier 2, Table 7.1-1, identifies that the guidelines in RG 1.75 applies to the Q-DCIS. DCD, Tier 2, Section 7.1.6.4, describes the conformance of the Q-DCIS to IEEE Std 603, Section 5.6, which is evaluated in Section 7.1.1.3.10 of this report. DCD, Tier 1, Table 2.2.15-2, provides DAC/ITAAC for verifying compliance with IEEE Std 603, Section 5.6.

Section 7.9 also identifies that the D3 assessment and conformance to the SRM on SECY-93-087, Item II.Q, should be reviewed for data communication systems that are part of protection and diverse systems in the review of GDC 22. The NRC staff evaluated whether the DCIS functions were included in the NRC staff review of D3 analysis for RPS and SSLC/ESF as described in Section 7.1.3 of this report. The NRC staff evaluation of the D3 assessment and conformance to the SRM on SECY-93-087, Item II.Q, in Sections 7.1.3 and 7.1.1.3.7 of this report is applicable to the data communication systems. Based on the above, the the NRC staff finds that the requirements of GDC 22 have been adequately addressed.

The NRC staff evaluated whether GDC 23 has been adequately addressed for the data communication systems. GDC 23 requires that protection systems be designed to fail into a safe state or into a state demonstrated to be acceptable on some other defined basis. The NRC staff evaluation of conformance to GDC 23 in Section 7.1.1.3.6 of this report is applicable to the data communication systems. Therefore, the NRC staff finds that the requirements of GDC 23 have been adequately addressed.

The NRC staff evaluated whether GDC 24 has been adequately addressed for the data communication systems. GDC 24 requires that the protection system 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. GDC 24 also requires that the interconnection of the protection and control systems be limited so as to assure that safety is not significantly impaired. The NRC staff evaluation of conformance to GDC 24 in Section 7.1.1.3.6 of this report is applicable to the data communication systems. Therefore, the NRC staff finds that the requirements of GDC 24 have been adequately addressed.

The NRC staff evaluated whether GDC 29 has been adequately addressed for the data communication systems. 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. SRP Appendix 7.1-A states that GDC 29 is addressed by conformance, as applicable, to GDC 20-25 and GDC 28, which include verification of the design by the DAC/ITACC. Sections 2.2.15, 3.2, 3.3, and 3.8 of DCD Tier 1 include the DAC/ITAAC for the applicant to verify that the data communication systems design implements these design criteria. The NRC staff evaluation of conformance to GDC 29 in Section 7.1.3.3.6 of this report is applicable to the data communication systems. Therefore, the NRC staff finds that the requirements of GDC 29 have been adequately addressed.

The NRC staff evaluated whether 10 CFR 50.62 has been adequately addressed for the data communication systems. As discussed in Section 7.8 of this report, the NRC staff finds that the applicant addresses 10 CFR 50.62 requirements for the ARI system to be diverse from the RPS, to be designed to perform its function in a reliable manner, and to be independent from the RPS and an SLC system to perform its function in a reliable manner. Accordingly, the NRC staff finds that the requirements of 10 CFR 50.62 have been adequately addressed.

The NRC staff evaluated whether 10 CFR 50.34(f)(2)(v) has been adequately addressed for the data communication systems. As described in Section 7.1.1.3.4 of this report, the NRC staff evaluated the DCIS compliance with 10 CFR 50.34(f)(2)(v) and found it acceptable. This evaluation is applicable to the data communication systems. Accordingly the NRC staff finds that the requirements of 10 CFR 50.34(f)(2)(v) have been adequately addressed.

The NRC staff evaluated whether 10 CFR 50.55a(h) has been adequately addressed for the data communication systems. 10 CFR 50.55a(h) requires compliance with IEEE Std 603-1991 and the correction sheet dated January 30, 1995, which is evaluated in Section 7.1.1.3.10 of this report. The NRC staff evaluation of conformance to IEEE Std 603 in Section 7.1.3.3.10 of this report is applicable to the data communication systems. Therefore, the NRC staff finds that the requirements of 10 CFR 50.55a(h) have been adequately addressed.

The NRC staff evaluated whether the requirements of 10 CFR 52.47(b)(1) have been met. This regulation requires that the application (for design certification) must contain proposed ITAAC that are necessary and sufficient to provide reasonable assurance that, if the ITA are performed and the acceptance criteria are met, a plant that references the design certification has been constructed and will operate in accordance with the design certification, the Atomic Energy Act, and the Commission's rules and regulations. The ITAAC specific to the data communication systems are addressed throughout section 7.1.5.3 of this report. The NRC staff evaluation of conformance to 10 CFR 52.47 in Section 7.1.1.3.4 of this report is applicable to the data communication systems. Therefore, the NRC staff finds that the requirements of 10 CFR 52.47(b)(1) have been adequately addressed.

7.1.5.4 Conclusion

Based on the review of information documented in DCD, Tier 2, Subsection 7.1.6.6.1, DCD, Tier 1, Table 2.2.15-1, and DCD Tier 1, Table 2.2.15-2, the NRC staff concludes that the applicant adequately addresses the major design considerations for data communication systems. As discussed in Sections 7.1.1.3.1 through 7.1.1.3.10 of this report and Section 7.1.5.3 above, the NRC staff concludes for data communication systems, the applicant adequately addresses the relevant requirements of 10 CFR 50.55a(a)(1); 10 CFR 50.55a(h); 10 CFR 50.34(f)(2)(v), 10 CFR 50.62, 10 CFR 52.47(b)(1), GDC 1, 2, 4, 13, 15, 19, 21, 22, 23, 24, 28, and 29; and the guidelines of the SRM on SECY-93-87. The staff also concludes that adequate high-level functional requirements are identified and sufficient DAC/ITAAC are included in Tier 1 to verify that the design is completed in compliance with the applicable requirements.

7.1.6 Secure Development and Operational Environment

7.1.6.1 Regulatory Criteria

RG 1.152, Revision 2 provides a method that the NRC finds acceptable for complying with the Commission's regulations (i.e., 10 CFR Part 50, Appendix A, GDC 21, 10 CFR Part 50, Appendix B, Criterion III, and IEEE Std 603-1991, Clauses 5.6.3 and 5.9) for promoting high functional reliability, design quality, and a secure development and operational environment (SDOE) for use of digital computers in safety systems of nuclear power plants. SDOE in this context refers to protective actions taken against a predictable set of non-malicious acts (e.g., inadvertent operator actions, undesirable behavior of connected systems) that could challenge the integrity, reliability, or functionality of a digital safety system. RG 1.152, Revision 2 utilizes the waterfall life cycle phases to provide a framework for establishing digital safety system the SDOE guidance, as well as criteria for acceptability, in the development of high quality safety systems. By committing to RG 1.152, Revision 2 in the DCD, the development of the Critical Digital Assets (CDAs) is evaluated to the criteria for securing the development process and providing reliable secure operational environment features within the design for the identified life cycle phases, which consists of the following phases:

- Concepts
- Requirements
- Design
- Implementation
- Test
- Installation, Checkout, and Acceptance Testing

- Operation
- Maintenance
- Retirement

The NRC staff's acceptance of system SDOE design features is based on (1) confirming that the appropriate CDA analysis and grouping have been made, (2) that appropriate secure operational environment design elements have been integrated into project specific plans, (3) verifying that the secure operational environment elements of the plans have been followed, (4) confirming that the process produced acceptable secure operational environment design outputs, and (5) validating that an effective and responsive secure operational environment has been utilized throughout all phases to protect process integrity.

Cyber security to address malicious events is under the purview of 10 CFR 73.54, "Protection of Digital Computer and Communication Systems and Networks." Section 1.7 of NEDE-33295P states that while GEH's Cyber Security Program Plan and Cyber Security Program may be used to demonstrate compliance to aspects of 10 CFR 73.54, conformance to 10 CFR 73.54 is the responsibility of the Combined Operating License applicant to demonstrate compliance, not GEH. Thus the staff did not evaluate the portion of NEDE-33295P that addresses aspects of 10 CFR 73.54 for compliance to this requirement. Compliance with 10 CFR 73.54 will be addressed by the COL applicant. Therefore, the ESBWR design certification does not include compliance with 10 CFR 73.54.

In the context of this safety evaluation report, for instances in which the DCD or its referenced documents uses the word "cyber security," the evaluation will be based on those SDOE features that address non-malicious acts.

7.1.6.2 Summary of Technical Information

DCD, Tier 2, Revision 6, Section 7.1.6.6.1.28, states that the cyber security measures included in RG 1.152 are evaluated and incorporated into the Q-DCIS design in accordance with NEDE-33295P. Coverage is extended to all systems and components determined to be CDAs. Cyber security design functionality is directly integrated into the project specific plans developed under NEDE-33226P and NEDE-33245P.

NEDE-33295P is a high level document defining the requirements for the development and management of an effective SDOE program for applicant and its ESBWR product. This document is a top-tier design basis and high level implementation guide for the ESBWR SDOE Program, per RG 1.152.

NEDE-33295P provides information on the system design cyber security as well as other cyber security material that is outside the scope of the design certification, as explained above. This review only bases its regulatory findings on Regulatory Positions C.2.1 through C.2.6 (i.e., Concepts through Installation, Checkout, and Acceptance Testing) of the development of the CDA SDOE design. Compliance with Regulatory Positions C.2.7 through C.2.9 of RG 1.152, Revision 2 (i.e., Operation; Maintenance; and Retirement phases) will be addressed by the COL applicant. Other guidance for system development, including the remainder of RG 1.152, is addressed in NEDE-33226P and NEDE-33245P.

The applicant has not included any specific SDOE project plans or design outputs within the scope of the design certification. Instead, NEDE-33295P provides template information for properly integrating SDOE elements into the design of all CDAs. This document also specifies

the processes required to be in place during all development activities to maintain secure development environment during the development and other pre-operational life cycle activities. These requirements are binding upon all components of the applicant's source of supply – including vendors and sub contractors.

The DAC/ITAAC in DCD, Tier 1, Section 3.2, is aligned to project activities, to confirm the proper integration of functions and features that support a SDOE into the system life cycle. In addition, the DAC/ITAAC confirms the completion of these activities and that the products conform to the processes described in NEDE-33295P and the guidelines of RG 1.152.

7.1.6.3 NRC Staff Evaluation

7.1.6.3.1 Review Method for SDOE Design

The NRC staff examines the software life cycle planning, implementation, and design outputs for elements of features and functions that support a SDOE. This information can be organized as described in RG 1.152, Section C.2, Regulatory Positions.

The SDOE integration model described in RG 1.152, C.2, Positions 2.1 through 2.9 is very similar to waterfall lifecycle described in BTP HCIB-14. The secure development environment program should be integrated into the overall physical access control, intellectual property protection, and quality assurance programs in place at the applicant's facility. The NRC staff will examine the applicant submissions for the integration into current and planned practices already identified for system development.

RG 1.152 is applicable to safety systems. An applicant can make a determination to apply this RG to all CDAs. If this determination is made, then RG 1.152 guidance should be applied to all CDAs in a graded approach. The lifecycle phase-specific SDOE requirements should be commensurate with the risk and magnitude of the harm resulting from unauthorized and inappropriate access, use, disclosure, disruption, or destruction of the applicable digital system.

7.1.6.3.2 General Evaluation of SDOE Activities

In NEDE-33295P, the applicant states that it conforms to RG 1.152 for SDOE activities. This document describes the plan for developing the program that implements the SDOE guidance provided by RG 1.152 and BTP HCIB-14. This LTR works in conjunction with the software development LTRs (NEDE-33226P and NEDE-33245P) to implement an overall SDOE system design. The two software LTRs provide the overall development guidance per BTP HCIB-14. NEDE-33295P provides guidance to enhance and modify the overall system development process with functionality that supports SDOE. The NRC staff's review of NEDE-33295P is to determine that it provides this information and gives adequate direction for implementing the SDOE processes in the project-specific plans.

The applicant identifies specific life cycle phases for this process. These life cycle phases are similar to those identified in RG 1.152 as well as those in BTP HCIB-14. The reviewed activities in each phase are consistent with the guidance provided in RG 1.152. The applicant refers to the concepts phase as the planning phase. In addition, the operations phase and the maintenance phase are combined into one operations and maintenance phase. The operations and maintenance phase, as well as the retirement phase, are outside the scope of this review. The review of life cycle phases is documented in Section 7.1.6.3.5 of this report.

The applicant states that a NUREG/CR 6847, “Cyber Security Self-Assessment Method for U.S. Nuclear Power Plants (not publicly available)”, process will be utilized to determine which systems or groupings of systems will be considered CDAs. The applicant has expanded the use of the basic process by applying it to a conceptual design rather than just an as built system. This process will be used iteratively and increase the quality and completeness of the system design. The NRC staff finds the expanded use of NUREG/CR 6847 acceptable.

7.1.6.3.3 Evaluation of Compliance with Regulations

The NRC staff has reviewed NEDE-33295P for compliance with the requirements of GDC 21 and IEEE Std. 603-1991, Clauses 5.6.3, and 5.9 as incorporated by reference in 10 CFR 50.55a(h)for promoting high functional reliability, design quality, and a secure development and operational environment for use of digital computers in safety systems of nuclear power plants. Designing in features to protect the protection system against a predictable set of non-malicious acts (e.g., inadvertent operator actions, undesirable behavior of connected systems) provides enhanced assurance of high functional reliability. Taking the same actions with systems which could adversely impact the ability of a safety system to perform its safety function also provides enhanced assurance of high functional reliability. The guidance in RG 1.152 provides general guidance by which the applicant can support high functional reliability. The use of a NUREG/CR 6847 method provides a means to identify all those systems which may be affected by non-malicious events including non-safety systems. Based on the applicant’s commitment to follow the applicable guidance in RG 1.152, as detailed in NEDE-33295P and confirmed in this review, the NRC staff finds that the applicant’s submission meets the requirements of GDC 21 and Clauses 5.6.3 and 5.9 of IEEE Std. 603-1991 and therefore 10 CFR 50.55a(h).

The NRC staff also reviewed NEDE-33295P for compliance to the quality assurance requirements of 10 CFR Part 50, Appendix B. Quality assurance comprises all those planned and systematic actions necessary to provide adequate assurance that a system will perform satisfactorily in service. In particular, quality assurance includes quality control. An adequate secure development environment program is important to control the quality of the systems being developed under this program and to protect them from the effects of cyber events. Based on the applicant’s commitment to follow the applicable guidance in RG 1.152 for quality assurance, as detailed in NEDE-33295P and as documented in DCD Tier 2 in NEDE-33245P (Software QA program manual),, the NRC staff finds that for cyber security, the applicant voluntarily meets the requirements for a sufficient quality assurance program per 10 CFR Part 50 Appendix B.

7.1.6.3.4 Evaluation of Deviations from Guidelines and Standards

In Appendix A, “Conformance Review,” of NEDE-33295P, the applicant documented the conformance with RG 1.152 and also addressed some deviations. With the exceptions of the stated deviations, NEDE-33295P specifies conformance to the criteria and guidance contained in RG 1.152. The applicant’s stated deviations from applicable RGs and industry standards are summarized and evaluated below.

(1) BTP HCIB-14

The applicant deviates in the use of metrics to monitor the development process. This issue is addressed in the review of the software development methodology in Section 7.1.2 of this report and has been found acceptable.

(2) RG 1.152

The applicant excludes IEEE Std 12207.0-1996 and IEEE Std 603-1998, from stated conformance. The applicant describes this nonconformance as follows:

> IEEE Std 12207.0-1996, is not directly referenced. However, IEEE Std 1074-1995 is directly referenced by RG 1.173, and is therefore used instead of IEEE Std 12207. IEEE Std 1074 covers similar topics and is the committed reference. IEEE Std 603-1998 addresses criteria for safety systems but is not within the scope of the SMPM and SQAPM because it does not provide guidance on software design and software quality assurance.

Since IEEE Std 12207 has not been endorsed by RG, and the applicant followed IEEE Std 1074, which has been endorsed by RG 1.173, this deviation is acceptable.

RG 1.152 is only applicable to safety-related systems. The applicant deviates by expanding the scope to all CDAs. This deviation is acceptable.

Parts of RG 1.152, Section C.2 are scoped to the licensee. These actions are not addressed in this document. This deviation is acceptable.

The NRC staff reviewed the deviations from RG 1.152 and finds them acceptable.

7.1.6.3.5 Evaluation of Life Cycle Phase Activities

The primary purpose of NEDE-33295P is to provide guidance and direction to enhance and modify the project-specific plans to include adequate SDOE functionality. Therefore, each life cycle phase activity listed in this plan has been reviewed for expected content against RG 1.152. Applicant deviations were also considered in the review of these activities.

NEDE-33295P life cycle phase activities have been evaluated by the NRC staff as follows:

(1) Concepts Phase

> The applicant refers to this phase at the Planning phase. In this phase, the CDAs are identified in a NUREG/CR-6847 process. Communication pathways and interfaces are defined. System design vulnerabilities are listed. Technologies to mitigate the vulnerabilities are identified. These activities are basically the same as those identified in RG 1.152. Some activities cross the boundary between Concepts and Requirements. However, this is acceptable as the information is appropriately developed and available when needed.
>
> The activities in this phase are acceptable.

(2) Requirements Phase

> System architecture requirements unique to each identified CDA are developed and defined. The requirements are directly driven by the outputs of the Planning phase. These requirements are integrated into the overall system development requirements. Network specific architecture issues are identified at this stage. Concepts for system

configuration, access control and similar protection level driven items are addressed. These items will be integrated into the overall Hardware and Software Specification (HSS). System interfaces will be addressed in further detail. COTS software and previously developed software requirements will be derived and evaluated. Identified V&V tasks will be evaluated. Any additional requirements in this area will be integrated into the overall project-specific V&V plans. The activities identified by the applicant meet the threshold identified in RG 1.152. The activities in this phase are acceptable.

(3) Design Phase

The design phase addresses the concepts of confidentiality, integrity and availability. The activities are directly integrated into the SMPM identified SDOE activities. The vulnerability assessment is taken from the NUREG/CR-6847 review and integrated into the SMPM and SQAPM activities and derived project-specific plans. Physical and logical access as well as interfaces between digital assets and other networks is addressed per RG 1.152. Additional SDOE requirements to address access to CDAs are addressed. This phase is in line with the activities detailed in RG 1.152. The activities in this phase are acceptable.

(4) Implementation Phase

The secure coding practices required by the SMPM are followed in this phase. Coordination between the SMPM and SQAPM commitments are specifically discussed in this phase. Unique issues of COTS software and its vulnerability evaluation are discussed. The general secure coding practices and procedures already present and identified by RG 1.152 are reemphasized in this phase. Particular attention is given to the difficult problems of securing COTS software. The NRC staff has reviewed this high level process description and determined that the activities in this phase are acceptable.

(5) Test Phase

The test activities are generally covered in the SMPM and SQAPM. Specific SDOE related issues are driven by RG 1.152 and the secure operational environment hazard analysis and related activities. Scanning and other actions will be performed to verify the functions and features that a support secure operational environment as designed into the system are adequate. An option to perform more in-depth scanning based on NUREG/CR-6847 procedures is also discussed. The majority of the testing activities were covered and approved in the SMPM and SQAPM documents. The implementation of these documents through their derivative project-specific plans provide assurance that sufficient testing will take place to validate the design functions and feature that support a secure operational environment for each CDA. Based on NRC staff's review and the conformance with the guidance on RG 1.152, the activities in this phase are acceptable.

(6) Installation, Checkout and Acceptance Testing Phase

The applicant refers to this phase as simply the Installation phase. The SMPM governs the general installation phase activities. Additional tests and procedures to validate the functions and feature that support a secure operational environment in the CDA will be integrated into the appropriate project-specific plan(s). The activities specifically listed in this section are equivalent or surpass the information provided in RG 1.152. The activities in this phase are acceptable.

The NRC staff review of the NEDE-33295P finds that this document provides adequate, high level guidance to support the design and implementation of functions and features that support a secure operational environment. This determination is based on the identification of the activities specified in RG 1.152 to establish and maintain a SDOE.

7.1.6.3.6 Evaluation of SDOE Activities DAC/ITAAC

The applicant has chosen to use the DCD Tier1 DAC/ITAAC process to allow completion of both system and project-specific SDOE design activities, as well as the completion of verifiable activities through the project-specific life cycle phases up to fuel load.

The necessary DAC/ITAAC items are derived from the RG 1.152 process and resulting documents. The DAC/ITAAC documented in DCD, Tier 1, Section 3.2 confirm and verify (1) that the appropriate CDA analysis and grouping has been made, (2) that appropriate secure operational environment design elements have been integrated into project specific plans, (3) that the secure operational environment design elements of the plans have been followed, (4) that the process produced acceptable secure operational environment design outputs, and (5) that an effective and responsive secure development environment plan has been utilized throughout all phases to protect process integrity.

7.1.6.4 Conclusion

The applicant has identified deviations from RG 1.152 guidance and applicable regulations. These deviations have been reviewed and found acceptable. The applicant's proposed design SDOE activities address the relevant requirements of 10 CFR 50.55a(h); GDC 21; and 10 CFR Part 50 Appendix B. The NRC staff finds that the applicant's SDOE design activities are consistent with RG 1.152 and associated regulatory guidance protection against a predictable set of non-malicious acts that could challenge the integrity, reliability, or functionality of a digital safety system..

The applicant has provided sufficient information on SDOE provisions in DCD, Tier 1, Section 3.2, DCD Tier 2, and NEDE-33295P to provide assurance that the defined process will sufficiently integrate functions and features that support a secure operational environment into the project specific software development plans. This integration will result in high quality safety system software with appropriate functions and features to address a predictable set of non-malicious acts.

Based on the review of DCD, Tier 1, Section 3.2, DCD Tier 2, and NEDE-33295P documentation, the NRC staff concludes that the SDOE activities are acceptable.

7.2 Reactor Trip System

7.2.1 Regulatory Criteria

The objective of the review of DCD, Tier 1, Section 2.2 and DCD, Tier 2, Section 7.2, is to confirm that the RTS satisfies regulatory acceptance criteria, guidelines, and performance requirements. The review of the I&C aspects of the RTS includes the RPS, the NMS, and the SPTM functions. The RTS detects a plant condition that initiates rapid insertion of control rods to shut down the reactor in situations that could result in unsafe reactor operations. This action prevents or limits fuel damage and system pressure excursions, minimizing the release of radioactive material.

Acceptance criteria of the RTS, hence the RPS as discussed below, are based on meeting the relevant requirements of 10 CFR 50.55a(a)(1); 10 CFR 50.55a(h); 10 CFR 50.34(f)(2)(v) and (f)(2)(xxiii); 10 CFR 52.47(b)(1); and GDC 1, 2, 4, 10, 13, 15, 19, 20-25, and 29. The acceptance criteria are also based on conforming to the guidelines of IEEE Std 7-4.3.2, as endorsed by RG 1.152, and the SRM on SECY-93-087.

7.2.2 Summary of Technical Information

7.2.2.1 Reactor Protection System Description and Architecture

7.2.2.1.1 Reactor Protection System Description

The RPS is designed to provide the capability to automatically or manually initiate a reactor scram while maintaining protection against unnecessary scrams resulting from single failures. The RPS logic will not result in a reactor trip when one entire division of channel sensors is bypassed and/or when one of the four automatic RPS trip logic systems is out of service (with any three of the four divisions of safety power available). This is accomplished through the combination of fail-safe equipment design, the redundant sensor channel trip decision logic, and the redundant 2/4 trip systems output scram logic. The RPS is classified as a safety system. The RPS electrical equipment is classified as seismic Category I and will be environmentally and seismically qualified.

The RPS logic design will be such that it initiates reactor trip signals within individual sensor channels when any one or more of the conditions listed below exists during reactor operation. A reactor scram results if system logic is satisfied. The following lists the condition and, in parentheses, the system monitoring the process condition:

- high drywell pressure (CMS)
- turbine stop valve closure (RPS)
- turbine control valve fast closure (RPS)
- NMS - monitored SRNM and APRM conditions exceed acceptable limits (NMS)
- reactor vessel pressure high (NBS)
- RPV water level low (Level 3) decreasing (NBS)
- RPV water level high (Level 8) increasing (NBS)
- main steam isolation valves closure (run mode only) (NBS)
- low-low CRD HCU accumulator charging header pressure (CRD)
- suppression pool temperature high (CMS)
- high condenser pressure (RPS)

- power generator bus loss (loss of feedwater flow) (run mode only) (RPS)
- high simulated thermal power (FW temperature biased) (NBS and NMS)
- FW temperature exceeding allowable simulated thermal power vs. FW temperature domain (NBS)
- operator - initiated manual scram (RPS)
- reactor mode switch in “shutdown” position (RPS)

7.2.2.1.2 Reactor Protection System Architecture

There are four instrument channels provided for each process variable being monitored, one for each RPS division. When more than four sensors are required to monitor a variable the output of the sensors are combined into only four instrument channels. The logic in each division is asynchronous with respect to the other divisions. The RPS is implemented with two communication methodologies: “point-to-point” optical fiber inter-divisional communication and a shared memory data communication ring network. Point-to-point communication is limited to trip and bypass information. Point-to-point fiber is also used for functional trip logic units (TLU) to output logic units (OLU), RPS to NMS and RPS to SSLC/ESF communication. The shared memory data communication ring network can read the entire shared memory on the CIMs card and write only to a designated portion of the CIMs card. The data on data communication ring are actively transported between one chassis transmitter and another’s receiver until all nodes have been updated. There are two “counter rotating” data communication rings within each division, therefore, no single failure will prevent data transmission.

Equipment within a sensor channel consists of sensors (transducers or switches), the DTM, and multiplexers. The sensors within each channel detect abnormal operating conditions and send analog (or discrete) output either directly to the RPS cabinets or to the RMUs within the associated division of the Q-DCIS. The RMUs within each division performs analog-to-digital conversion and signal processing, then sends the digital or digitized analog output values of the monitored variables to the DTM for trip determinations within the associated RPS sensor channel in the same division. The DTM in each sensor channel compares individual monitored variable values with trip setpoint values and for each variable sends a separate trip/no trip output signal to the TLUs in the four divisions of trip logic.

Equipment within an RPS division of trip logic consists of TLUs, manual switches, bypass units (BPUs), and OLU. The TLUs perform the automatic scram initiation logic, checking for 2/4 coincidence of trip conditions in any set of instrument channel signals coming from the four divisions of DTMs or when an NMS isolated digital trip signal (voted 2/4 in the NMS TLU) is received. The automatic scram initiation logic for any trip is based on the reactor operating mode switch status, channel trip conditions, NMS trip input, and bypass conditions. Each TLU, besides receiving the signals described above, also receives digital input signals from the BPUs and other control interfaces in the same division. The BPUs perform bypass and interlock logic for the division of channel sensors bypass and the division TLU bypass. Each BPU sends a separate bypass signal for the four channels to the TLU in the same division for channel sensors bypass. Each RPS BPU also sends the TLU bypass signal to the OLU in the same division.

The OLUs perform division trip, seal-in, reset, and trip test functions. Each OLU receives bypass inputs from the RPS BPUs, trip inputs from the TLU of the same division, and manual inputs from switches within the same division. Each OLU provides trip outputs to the trip actuators.

Equipment within a division of trip actuators includes load drivers for automatic primary scram and initiation of backup scram. The RPS includes two physically separate and electrically independent divisions of trip actuators receiving inputs from the four divisions of OLU. The operation of the load drivers is such that a trip signal on the input side creates a high impedance, current-interrupting condition on the output side. The output side of each load driver is electrically isolated from its input signal. The load driver outputs are arranged in the primary scram logic circuitry, which is between the scram solenoids and scram solenoid 120-VAC power source. When in a tripped state, the load drivers cause the scram solenoids (scram initiation) to de-energize. The load drivers within a division interconnect with the OLU of all other divisions to form a special arrangement (connected in series and in parallel in two separate groups) that result in 2/4 scram logic. Reactor scram occurs if load drivers associated with any two or more divisions receive trip signals from the OLUs.

Load drivers are also used for backup scram actuators, scram-follow initiation, and scram reset permissive actuators. When in a tripped state, the load drivers for backup scram cause the air header dump valve solenoids (air header dump initiation) to energize. The load drivers of the backup scram are arranged in a 2/4 configuration similar to that described above for the primary scram load drivers. Backup scram is diverse in power source and function from primary scram.

Equipment within a division of manual scram controls includes manual switches, contacts, and relays that provide an alternate, diverse, manual means to initiate a scram and air header dump. Each division's manual scram function controls the power sources to the same division of scram logic circuitry for scram initiation and division of scram logic circuitry for air header dump initiation. One of the two divisions of scram logic circuitry distributes Division 1 safety 120-VAC power to the A solenoids of the HCUs. The other division of scram logic circuitry distributes Division 2 safety 120-VAC power to the B solenoids of the HCUs. The HCUs (which include the scram pilot valves and the scram valves) and the air header dump (backup scram) valves are, themselves, components of the CRD system.

7.2.2.2 Neutron Monitoring System Description

DCD, Tier 2, Section 7.2.2, describes the NMS. The NMS monitors reactor core thermal neutron flux from the startup source range to beyond rated power and provides trip signals initiating reactor scrams under excessive neutron flux or excessive rates of change in neutron flux (short period) conditions. The NMS comprises the following subsystems:

- SRNM
- PRNM
- AFIP
- MRBM

The SRNM and PRNM subsystems are safety systems and are discussed below. The PRNM subsystem includes the LPRM, APRM, and OPRM functions. The AFIP subsystem and the MRBM are non-safety systems and are discussed in Section 7.7 of this report.

7.2.2.2.1 Startup Range Neutron Monitor Subsystem

Sections 7.2.1.2.4 and 7.2.2 of DCD Tier 2 describe the SRNM. The SRNM is designed as a safety subsystem generating trip signals to prevent fuel damage in the event of any abnormal reactivity insertion transients (while operating in the startup power range). The trip signal results

either from an excessively high neutron flux level or an excessive rate of neutron flux increase (a short reactor period). The setpoints of these trips are such that, under the worst reactivity insertion transients, fuel integrity is always protected. DCD, Tier 2, Table 7.2-2, provides the SRNM trip and rod block functions. DCD, Tier 2, Table 7.2-3, provides the SRNM trip signals. The trip setpoints are adjustable and are determined using the setpoint methodology in NEDE-33304P.

7.2.2.2.2 Power Range Neutron Monitor

7.2.2.2.2.1 Local Power Range Monitor

The LPRM is designed to monitor the local power level and to provide a sufficient number of LPRM signals to the APRM system to fulfill the safety design basis for the APRM. The LPRM is qualified to operate under DBAs and abnormal environmental conditions.

The LPRM design characteristics are the following:

- provides signals to the APRM that are proportional to the local neutron flux at various locations within the reactor core

- provides signals to alarm high or low local thermal neutron flux

- provides signals proportional to the local neutron flux to drive indicators and displays and for the PCF used for operator evaluation of power distribution.

- provides signals proportional to the local neutron flux for use by other interface systems such as the RC&IS for the rod block monitoring function

7.2.2.2.2.2 Average Power Range Monitor

DCD, Tier 2, Section 7.2.2.1.3.1, specifies the following safety design bases for the APRM:

- The functional requirements specify that, under the worst permitted input LPRM bypass conditions, the APRM is capable of generating a timely trip signal in response to excessive average neutron flux increases to prevent fuel damage.

- The system is designed to produce a safety simulated thermal power signal to the RPS to allow that system to support reactor power scram bypass requirements.

- The APRM provides information for monitoring the average power level of the reactor core in the power range. The APRM is capable of generating a trip signal to scram the reactor in response to excessive and unacceptable neutron flux increase to prevent fuel damage. Such a trip signal includes a trip from the simulated thermal power signal, representing the APRM flux signal through a time constant representing the actual fuel time constant. The resulting simulated thermal power signal accurately represents core thermal (as opposed to neutron flux) power and the heat flux through the fuel.

- Scram functions are assured when the minimum LPRM input requirement to the APRM is fulfilled. If this requirement cannot be met, an inoperative channel trip signal is generated. Independence and redundancy requirements are incorporated into the

design and are consistent with the safety design basis of the RPS.

Additional design characteristics of the APRM include the following:

- provides continuous indication of average reactor power (neutron flux) from 1 percent to 125 percent of rated reactor power, which overlaps with the SRNM range
- provides interlock logic signals for blocking further rod withdrawal to avoid an unnecessary scram actuation
- provides a simulated thermal power signal derived from each APRM channel, which approximates the heat dynamic effects of the fuel
- provides a continuously available LPRM/APRM display for detection of any neutron flux oscillation in the reactor core

7.2.2.2.2.3 Oscillation Power Range Monitor

DCD, Tier 2, Section 7.2.2.1.4.1, specifies the following safety design bases for the OPRM:

- Under the worst permitted input LPRM bypass conditions, the OPRM is capable of generating a timely trip signal in response to core neutron flux oscillation conditions and thermal-hydraulic instability to prevent violation of the thermal safety limit.
- The OPRM provides monitoring and protection function for core-regional and core-wide neutron flux oscillation monitoring using the LPRM signals sent to the associated APRM channel in which the OPRM channel resides. The OPRM is capable of generating a timely trip signal to scram the reactor in response to excessive and unacceptable neutron flux oscillation to prevent fuel damage. Scram functions are ensured when the minimum LPRM input requirement to the OPRM is fulfilled.
- The OPRM provides non-safety core flux oscillation information for the plant computer and MCR display and alarms when the OPRM is inoperative or has an insufficient number of LPRM inputs.

7.2.2.3 Suppression Pool Temperature Monitor

The SPTM provides suppression pool temperature data for automatic scram and automatic suppression pool cooling initiation when established high temperature limits are exceeded. In addition, the SPTM subsystem provides suppression pool temperature data for operator information and recording and for post accident conditions of the suppression pool. The SPTM hardware is redundantly powered by the appropriate dual divisional uninterruptible 120-VAC power sources, either of which can support the SPTM function.

The sensor electrical wiring, encapsulated in pliable, grounded sheathing, is terminated in wetwell-sealed, moisture-proof junction boxes for easy sensor replacement or maintenance during a plant outage. The temperature sensor wiring from the wetwell junction boxes is directed through the suppression pool divisional instrument penetrations to the four-divisional Q-DCIS RMUs and the DPS RMUs.

7.2.3 NRC Staff Evaluation

The NRC staff reviewed the RPS in accordance with SRP Section 7.2. The NRC staff also used acceptance criteria in SRP Section 7.1, SRP Table 7-1, SRP Appendix 7.1-A, and SRP Appendix 7.1-C, as directed by SRP Section 7.2. The acceptance criteria listing used as the basis for the NRC staff's review of the RPS is described in Section 7.1.1.1 of this report. SRP Section 7.2 highlights specific topics that should be emphasized in the RPS review and are addressed in Section 7.2.3.1 of this report. The NRC staff included the review of the DCD Tier 1, DAC/ITAAC during the review of this section because of the significant role of the DAC/ITAAC in determining the RPS conformance to all requirements.

As described in Section 7.1.1.3.1 of this report, the DCD does not provide the required RPS system design information to comply with IEEE Std 603. Instead, the applicant has included the DAC/ITAAC in DCD, Tier 1, Section 2.2.15, to confirm that the completed RPS design complies with IEEE Std 603. DCD, Tier 1, Section 2.2.15 also includes an DAC/ITAAC applicability table (Table 2.2.15-1), which identifies the applicability of the IEEE Std 603 criteria DAC/ITAAC to the RPS. The NRC staff has accepted the DAC approach to addressing compliance with IEEE Std 603. The NRC staff evaluation of conformance to IEEE Std 603 in Section 7.1.1.3.10 of this report is applicable to the RPS.

In RAI 7.1-99, the NRC staff asked the applicant to clarify the applicability of IEEE Std 603 criteria in a consistent manner throughout DCD, Tier 2, Chapter 7. By letter MFN 09-089, dated February 19, 2009, the applicant submitted a response to RAI 7.1-99, along with responses to 7.1-100, 7.1-101, and 14.3-265, Supplement 1, all of which are incorporated in DCD Revision 6. Section 7.1.1.3.1 of this report provides additional discussion of these RAI responses. With regard to the NRC staff evaluation of the RPS, the applicant significantly revised DCD, Tier 2 Tables 7.1-1 and 7.1-2 to clearly identify applicability of IEEE Std 603 criteria for each RPS subsystem. Concurrently, many references to IEEE Std 603 criteria were revised or removed from the discussions of RPS subsystems in DCD, Tier 2 Section 7.2 to address the consistency concerns. Accordingly, statements regarding applicability of IEEE Std 603 criteria provided in the NRC staff SER with open items have been updated or removed from the remainder of Section 7.2.3 of this report to be consistent with DCD Revision 6.

7.2.3.1 Evaluation of Reactor Protection System Conformance with Acceptance Criteria - Major Design Considerations

SRP Section 7.2 lists the following eight major design considerations that should be emphasized in the review:

(1) Design Basis (IEEE Std 603, Section 4)

The NRC staff evaluated the RPS design basis to determine whether IEEE Std 603, Section 4, was adequately addressed using SRP Appendix 7.1-C, Section 4, "Safety System Designation (IEEE Std 603)." For completeness, the SRP states, "As a minimum each of the safety system design basis aspects identified in IEEE Std 603, Sections 4.1 through 4.12 should be addressed." This criterion is evaluated in Section 7.1.1.3.10 of this report, where the NRC staff finds that Section 4 is adequately addressed based on its inclusion in the safety system design basis and the verification of applicable criteria in the DCD, Tier 1, Section 2.2.15, DAC/ITAAC. This evaluation is applicable to the RPS. Also, DCD, Tier 1, Table 2.2.15-1, identifies that the DAC/ITAAC for applicable criteria of Section 4 are applicable to the RPS and all subsystems.

DCD, Tier 2, Section 7.2.1.2.4.2, identifies individual parameters that determine when, in a particular condition or extreme, the RPS automatically initiates a reactor scram. As mentioned previously, NEDE-33226P and NEDE-33245P, as part of the software life cycle process, define a process by which plant performance requirements, including response times, under various operational conditions will be specified, implemented, and tested. DCD, Tier 1, Section 3.2, includes the DAC/ITAAC for verifying that the software plans were developed and implemented consistent with this process and produce acceptable design outputs. Accordingly, the NRC staff finds that Section 4 is adequately addressed for the RPS.

(2) Single Failure Criterion (IEEE Std 603, Section 5.1)

The NRC staff evaluated whether the single failure criterion in IEEE Std 603, Section 5.1, has been adequately addressed for the RPS. This criterion is evaluated in Section 7.1.1.3.10 of this report, where the NRC staff finds that Section 5.1 is adequately addressed based on its inclusion in the safety system design basis and its verification in the DCD, Tier 1, Section 2.2.15, DAC/ITAAC. This evaluation applicable to the RPS. Also, DCD, Tier 1, Table 2.2.15-1, identifies that the DAC/ITAAC for Section 5.1 are applicable to the RPS and all subsystems. Accordingly, the NRC staff finds that Section 5.1 is adequately addressed for the RPS.

(3) Quality of Components and Modules (IEEE Std 603, Section 5.3)

The NRC staff evaluated whether the quality criterion, IEEE Std 603, Section 5.3, has been adequately addressed for the RPS. This criterion is evaluated in Section 7.1.1.3.10 of this report, where the NRC staff finds that Section 5.3 has been adequately addressed based on the inclusion of IEEE Std 7-4.3.2, Section 5.3, in the safety system design basis and the verification of the software development activities in the DCD, Tier 1, Section 3.2, DAC/ITAAC. Also, the applicant has stated that the quality assurance program conforms to GDC 1. The evaluation of the adequacy of the quality assurance program is addressed in Chapter 17 of this report. These evaluations are applicable to the RPS. DCD, Tier 2, Section 7.1.6.6.1.4, also discusses the applicability of this criterion to the Q-DCIS design. Accordingly, based on the applicant's use of an acceptable software development process, as evaluated in Section 7.1.2.3 of this report, and its verification in the DCD Tier 1, DAC/ITAAC, the NRC staff finds that Section 5.3 of IEEE Std 7-4.3.2 and Section 5.3 of IEEE Std 603 are adequately addressed for the RPS.

(4) Independence (IEEE Std 603, Sections 5.6 and 6.3)

The NRC staff evaluated whether the independence-related criteria, IEEE Std 603, Sections 5.6 and 6.3, were adequately addressed for the RPS. IEEE Std 603, Section 5.6, is evaluated in Section 7.1.1.3.10 of this report, where the NRC staff finds that Section 5.6 is adequately addressed based on its inclusion in the safety system design basis and its verification in the DCD, Tier 1, Section 2.2.15, DAC/ITAAC. This evaluation is applicable to the RPS. Also, DCD, Tier 1, Table 2.2.15-1, identifies that the DAC/ITAAC for Section 5.6 are applicable to the RPS and all subsystems. Accordingly, the NRC staff finds that Section 5.6 is adequately addressed for the RPS.

The NRC staff evaluated conformance with IEEE Std 603, Section 6.3. This criterion is evaluated in Section 7.1.1.3.10 of this report, where the NRC staff finds that Section 6.3 is adequately addressed based on its inclusion in the safety system design basis and its verification in the DCD, Tier 1, Section 2.2.15, DAC/ITAAC. This evaluation is applicable to the RPS. Also, DCD, Tier 1, Table 2.2.15-1, identifies that the DAC/ITAAC for Section 6.3 are

applicable to the RPS and all subsystems. Accordingly, the NRC staff finds that Section 6.3 is adequately addressed for the RPS.

(5) Diversity and Defense-in-Depth

The NRC staff evaluated whether the RPS has adequate D3. The RPS should incorporate multiple means for responding to each event discussed in DCD, Tier 2, Chapter 15. At least one pair of these means for responses to each event should have the property of signal diversity (i.e., 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 are sensed incorrectly (see NUREG/CR-6303). NEDO-33251, Revision 2, states conformity to NUREG/CR-6303. DCD, Tier 1, Table 2.2.14-4, requires the applicant to perform FMEAs of the safety protection system platforms to validate the DPS functions. The NRC staff evaluation of conformance to D3 in Section 7.1.3.3 of this report is applicable to the RPS. Accordingly, the NRC staff finds that D3 is adequately addressed for the RPS.

(6) System Testing and Inoperable Surveillance (IEEE Std 603, Sections 5.7, 5.8, and 6.5)

The NRC staff evaluated whether the criteria related to system testing and inoperable surveillance, IEEE Std 603, Sections 5.7, 5.8, and 6.5, have been adequately addressed. IEEE Std 603, Section 5.7, is evaluated in Section 7.1.1.3.10 of this report, where the NRC staff finds that Section 5.7 is adequately addressed based on IEEE Std 603, Section 5.7, being included in the design basis and its verification in the DCD, Tier 1, Section 2.2.15, DAC/ITAAC. This evaluation is applicable to the RPS. IEEE Std 603, Section 5.7 states that the capability for testing and calibration of safety system equipment shall be provided during power operation and shall duplicate, as closely as practicable, performance of the safety function. The applicant identifies two exceptions to this criterion in the RPS,“1) confirm operation of MSIV and turbine stop valve limit switches and 2) independent functional testing of the air header dump valves during each refueling outage (not operation) and operation of at least one valve can be confirmed following each scram.” The RPS can be tested in overlapping segments when testing one safety function. The extent of test and calibration capability provided depends on whether the design meets the single failure criterion. SRP Appendix 7.1-C states that any failure that is not detectable must be considered concurrently with any random postulated, detectable, single failure. DCD, Tier 1, Table 2.2.15-2, provides DAC/ITAAC for IEEE Std 603, Section 5.1 for the applicant to perform an analysis, or FMEA, that confirms that the requirements of the single failure criterion are satisfied for the RPS. DCD, Tier 1, Table 2.2.15-1, identifies that the DAC/ITAAC for Section 5.7 is applicable to the RPS and all subsystems. Accordingly, the NRC staff finds that Section 5.7 is adequately addressed for the RPS.

The NRC staff evaluated whether IEEE Std 603, Section 5.8, has been adequately addressed. This criterion is evaluated in Section 7.1.1.3.10 of this report, where the NRC staff finds that the criterion is adequately addressed based on its inclusion in the safety system design basis and its verification in the DCD, Tier 1, Section 3.3, DAC/ITAAC. This evaluation is applicable to the RPS. In addition, Section 5.8, “Information Displays,” is part of system testing and inoperable surveillance. DCD, Tier 2, Chapter 18, describes the HFE design process to design information displays and is evaluated in Chapter 18 of this report. DCD, Tier 1, Section 3.3, includes the DAC/ITAAC for implementing the HFE design process, which includes the design and verification of controls and information displays for monitoring variables and systems in the control room. This verification is applicable to the RPS and includes verifying the inventory of displays for manually controlled actions, system status indications, and indications of bypasses. Accordingly, the NRC staff finds that Section 5.8 is adequately addressed for the RPS.

The NRC staff evaluated conformance with IEEE Std 603, Section 6.5. This criterion is evaluated in Section 7.1.1.3.10 of this report, where the NRC staff finds that Section 6.5 is adequately addressed based on its inclusion in the safety systems design basis and its verification in the DCD, Tier 1, Section 2.2.15, DAC/ITAAC. This evaluation is applicable to the RPS. Also, DCD, Tier 1, Table 2.2.15-1, identifies that the DAC/ITAAC for Section 6.5 are applicable to the RPS and all subsystems. Accordingly, the NRC staff finds that Section 6.5 is adequately addressed for the RPS.

(7) Use of Digital Systems (IEEE Std 7-4.3.2)

The NRC staff evaluated whether IEEE Std 7-4.3.2, as endorsed by RG 1.152, has been adequately addressed for the RPS. SRP Appendix 7.1-D provides guidance on the implementation of IEEE Std 7-4.3.2 concerning the use of digital systems. In Section 7.1.1.3.10 of this report, the NRC staff evaluated in parallel IEEE Std 7-4.3.2 and IEEE Std 603 using the guidance in SRP Appendix 7.1-D. The NRC staff evaluation of conformance to IEEE Std 7-4.3.2 in Section 7.1.1.3.10 of this report is applicable to the RPS.

The software development activities are described in NEDE-33226P and NEDE-33245P. DCD, Tier 1, Section 3.2, includes the DAC/ITAAC to confirm that the completion of these activities and products conforms to the processes described in NEDE-33226P and NEDE-33245P and the guidelines of BTP HCIB-14. The NRC staff evaluation of software development activities is provided in Section 7.1.2 of this report. Accordingly, the NRC staff finds that use of digital systems is adequately addressed for the RPS.

(8) Setpoint Determination

The setpoint determination methodology is evaluated in Section 7.1.4 of this report.

7.2.3.2 Evaluation of Reactor Protection System Conformance with Acceptance Criteria - Other Criteria

SRP Section 7.2 states that RPS design should be evaluated for conformance to IEEE Std 603. This section evaluates IEEE Std 603 criteria not previously evaluated in Section 7.2.3.1 of this report.

The NRC staff evaluated conformance with IEEE Std 603, Sections 5.2, 5.9, 5.10, 5.11, 5.12, 6.1, 6.2. 6.4, 6.6, 6.7, 6.8, 7.1, 7.2, 7.3, 7.4, 7.5, 8.1, 8.2, and 8.3. These criteria are evaluated in Section 7.1.1.3.10 of this report, where the NRC staff finds that these criteria are adequately addressed based on their inclusion in the safety system design basis and their verification in the DCD, Tier 1, Section 2.2.15, DAC/ITAAC. This evaluation is applicable to the RPS. Also, DCD, Tier 1, Table 2.2.15-1, identifies that the DAC/ITAAC for these criteria are applicable to the RPS. Accordingly, the NRC staff finds that conformance to IEEE Std 603, Sections 5.2, 5.9, 5.10, 5.11, 5.12, 6.1, 6.2. 6.4, 6.6, 6.7, 6.8, 7.1, 7.2, 7.3, 7.4, 7.5, 8.1, 8.2, and 8.3 are adequately addressed for the RPS.

The NRC staff evaluated conformance with IEEE Std 603, Section 5.4. This criterion is evaluated in Section 7.1.1.3.10 of this report, where the NRC staff finds that Section 5.4 is adequately addressed based on its inclusion in the safety system design basis and verification of the EQ in the DCD, Tier 1, Section 3.8 ITAAC. This evaluation is applicable to the RPS. Accordingly, the NRC staff finds that conformance to IEEE Std 603, Section 5.4 is adequately

addressed for the RPS.

The NRC staff evaluated conformance with IEEE Std 603, Section 5.5. This criterion is evaluated in Section 7.1.1.3.10 of this report, where the NRC staff finds that Section 5.5 is adequately addressed based on its inclusion in the safety system design basis and its verification in the DCD, Tier 1, Section 2.2.15 and Section 3.2 DAC/ITAAC and Section 3.8 ITAAC. This evaluation is applicable to the RPS. Accordingly, the NRC staff finds that conformance to IEEE Std 603, Section 5.5 is adequately addressed for the RPS.

The NRC staff evaluated conformance with IEEE Std 603, Section 5.13. This criterion is evaluated in Section 7.1.1.3.10 of this report. The multi-unit station criteria do not apply to the standard single unit plant design submitted for NRC certification. The NRC staff determines that IEEE Std 603, Section 5.13 is not applicable to design certification.

The NRC staff evaluated conformance with IEEE Std 603, Section 5.14. This criterion is evaluated in Section 7.1.1.3.10 of this report, where the NRC staff finds that Section 5.14 is adequately addressed on the basis of its inclusion in the safety system design basis and its verification in the DCD, Tier 1, Section 3.3, DAC/ITAAC. This evaluation is applicable to the RPS. Accordingly, the NRC staff finds that conformance to IEEE Std 603, Section 5.14 has been adequately addressed.

The NRC staff evaluated conformance with IEEE Std 603, Section 5.15. This criterion is evaluated in Section 7.1.1.3.10 of this report, where the NRC staff finds that Section 5.15 is adequately addressed on the basis of its inclusion in the safety system design basis and its verification in the DCD, Tier 1, Section 2.2.15 DAC/ITAAC for IEEE Std 603, Section 5.1, DCD, Tier 1, Section 3.2, DAC/ITAAC, and DCD, Tier 1, Section 3.6 ITAAC. This evaluation is applicable to the RPS. Accordingly, the NRC staff finds that Section 5.15 is adequately addressed for the RPS.

7.2.3.3 Evaluation of Reactor Protection System Compliance with Regulations and Conformance to the NRC Staff Requirements Memorandum on SECY-93-087

The NRC staff reviewed the regulations in the acceptance criteria for the RPS in accordance with SRP Section 7.2 and SRP Appendix 7.1-A. For several of the GDC, compliance can be satisfied by meeting IEEE Std 603 requirements, which the NRC staff evaluated in the previous two sections. Compliance with IEEE Std 603 is briefly discussed with the relevant GDC, including the use of DAC, consistent with both SRP sections.

GDC 1 requires quality standards and maintenance of appropriate records.
10 CFR 50.55a(a)(1) requires that structures, systems, and components must be designed, fabricated, erected, constructed, tested, and inspected to quality standards commensurate with the importance of the safety function to be performed. The NRC staff evaluated whether GDC 1 and 10 CFR 50.55a(a)(1) have been adequately addressed for the RPS per SRP Appendix 7.1-A. SRP Appendix 7.1-A states that the NRC staff review should confirm that the appropriate regulatory guides and endorsed standards are identified as applicable for each I&C system important to safety. DCD, Tier 2, Table 7.1-1 identifies that GDC GDC 1 and 10 CFR 50.55a(a)(1) are applicable to the RPS. The NRC staff evaluation of conformance to RGs and standards for 10 CFR 50.55a(a)(1) and GDC 1 in Section 7.1.1.3.3 and 7.1.1.3.6 of this report is applicable to the RPS. Accordingly, based on applicable codes and standards being identified as applicable to the RPS, the NRC staff finds that the requirements of GDC 1 and 10 CFR 50.55a(a)(1) have been adequately addressed.

GDC 2 requires design bases for protection against natural phenomena. GDC 4 requires environmental and dynamic effect design bases. The NRC staff evaluated whether GDC 2 and 4 have been adequately addressed for the RPS. SRP Section 7.2 identifies that GDC 2 and 4 are addressed by identification of those systems and components for the RPS designed to survive the effects of earthquakes, other natural phenomena, abnormal environments and missiles in the design bases. SRP Section 7.2 also identifies that GDC 2 and 4 are addressed by the review of the qualification program in DCD, Tier 2, Sections 3.10 and 3.11. DCD, Tier 2, Table 7.1-1 identifies that GDC 2 and 4 are applicable to the RPS. DCD, Tier 2, Table 3.2-1, identifies that the safety RPS are designed as seismic Category I systems. In DCD, Tier 2, Sections 3.10 and 3.11 describe the EQ programs for safety electrical and digital I&C equipment, which are evaluated in Chapter 3 of this report. In DCD, Tier 1, Table 3.8-1, Items 1 and 3 include ITAAC for the applicant to verify the EQ of safety electrical and digital I&C equipment. The evaluation of GDC 2 and GDC 4 in Section 7.1.1.3.6 of this report further addresses these topics and is applicable to the RPS. Accordingly, based on the applicant's identification of EQ programs consistent with the design bases for the RPS and their verification in the ITAAC, the NRC staff finds that the requirements of GDC 2 and 4 have been adequately addressed.

GDC 10 requires that the reactor core and associated coolant, control, and protection systems 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. GDC 15 requires that the reactor coolant system and associated auxiliary, control, and protection system be designed with sufficient margin to ensure that the design conditions of the reactor coolant pressure boundary are not exceeded during any condition of normal operation, including AOOs. The NRC staff evaluated whether GDC 10 and 15 have been adequately addressed for the RPS. SRP Appendix 7.1-A for GDC 10 and GDC 15 state that the NRC staff review should evaluate the I&C system contributions to design margin for reactor core and reactor coolant systems. DCD, Tier 2, Table 15.1-6, identifies systems, including RPS, required to mitigate AOOs affecting the reactor core and reactor coolant systems. DCD, Tier 2, Chapter 7, includes corresponding actions in the design bases of the RPS to maintain the reactor core and reactor coolant system within appropriate margins. In DCD, Tier 1, Sections 2.2.15, 3.2, 3.3, and 3.8 include the DAC/ITAAC for the applicant to verify that the RPS design implements these design bases. Accordingly, based on the applicant's identification of necessary protection and safety actuations in the design bases for the RPS and their verification in the DCD, Tier 1, DAC/ITAAC, the NRC staff finds that the requirements of GDC 10 and 15 have been adequately addressed.

GDC 13 requires providing instrumentation to monitor variables and systems over their anticipated ranges for normal operation, AOOs, and accident conditions to assure adequate safety. GDC 13 also requires providing appropriate controls to maintain these variables and systems within prescribed operating ranges. GDC 19 requires control room functionality, control room habitability, and remote shutdown capability. The NRC staff evaluated whether GDC 13 and 19 have been adequately addressed for the RPS. The evaluation of GDC 19 is provided in Section 7.1.1.3.6 of this report with the exception of RPS support functions necessary for operating the reactor. SRP Section 7.2 identifies that GDC 13 and 19 are addressed by the review of status information and manual initiation capabilities. DCD, Tier 2, Section 7.2.1.2.4.3 specifies that the MCR displays provide status information and alarms for RPS related variables. DCD, Tier 2, Section 7.2.1.5.2 specifies the automatic and manual bypass of selected scram functions for the RPS. DCD, Tier 2, Section 7.2.1.2.4.2 specifies the manual scram capabilities of the RPS. DCD, Tier 2, Section 7.2.1.5.3 specifies the RPS manual

controls and Section 7.2.1.5.4 specifies the features of the reactor mode switch. DCD, Tier 2, Section 7.2.2.5 specifies the NMS displays and alarms. In combination with the following identified interrelated processes to design the monitoring capability and controls for the RPS, the NRC staff finds these monitoring capabilities and controls acceptable. NEDE-33226P and NEDE-33245P, as part of a software life cycle process, define a process by which plant performance requirements under various operational conditions will be specified, implemented, and tested. DCD, Tier 1, Section 3.2, includes the DAC/ITAAC for verifying that the software plans were developed and implemented consistent with this process and produce acceptable design outputs. DCD, Tier 1, Section 3.3, includes the DAC/ITAAC for implementing an HFE design process, which includes the design and verification of controls and information displays for monitoring variables and systems in the control room. These verifications are applicable to the RPS and include verifying the controls for manual initiation and control of RPS functions necessary to support actions to operate the nuclear power unit safely under normal conditions and to maintain it in a safe condition under accident conditions. Accordingly, based on identified RPS monitoring and controls capabilities, the defined processes for completing the design and their verification in the DCD Tier 1, DAC/ITAAC, the NRC staff finds that the requirements of GDC 13 and 19 have been adequately addressed.

GDC 20 requires that the protection system be designed to (1) initiate automatically the operation of the appropriate systems including reactivity control systems, to ensure that specified acceptable fuel design limits are not exceeded as a result of AOOs and (2) sense accident conditions and initiate the operation of systems and components important to safety. The NRC staff evaluated whether GDC 20 has been adequately addressed for the RPS. SRP Appendix 7.1-A notes that GDC 20 is addressed for protection systems by conformance with IEEE Std 603, Sections 4, 5, 5.5, 6.1, 6.8, and 7.1. The applicant has committed to following the guidance of RG 1.105 and has provided a setpoint methodology in NEDE-33304P. The NRC staff also evaluated for the RPS design-basis requirements, general functional requirements, and system integrity, involving IEEE Std 603, Sections 4, 5, 5.5, 6.1, 6.8, and 7.1, in Section 7.2.3.1 of this report. DCD, Tier 1, Table 2.2.15-2, includes the DAC/ITAAC for verifying that the safety functions of setpoints are defined, determined, and implemented based on the defined setpoint methodology and that the design is completed in compliance with IEEE Std 603. DCD, Tier 1, Table 2.2.15-2 also includes DAC/ITAAC for applicable sections of IEEE Std 603, Section 4 for verifying that complete design basis information is identified and implemented for RPS related software projects. The NRC staff evaluation of conformance to IEEE Std 603 in Section 7.1.1.3.10 of this report is applicable to the RPS. Accordingly, based on the applicant's identification of design bases for the RPS, conformance to applicable guidance and IEEE Std 603 sections, and their verification in the DAC/ITAAC, the NRC staff finds that the requirements of GDC 20 has been adequately addressed.

GDC 21 requires that protection systems be designed for high functional reliability and in-service testability commensurate with the safety functions to be performed. The NRC staff evaluated whether GDC 21 has been adequately addressed for the RPS. SRP Appendix 7.1-A states that GDC 21 is addressed for protections systems by conformance to IEEE Std 603 criteria except for Sections 5.4, 6.1, and 7.1. In addition, SRP Section 7.2 identifies that GDC 21 is addressed by conformance to RGs 1.22, 1.47, 1.53, 1.118, and IEEE Std 379. DCD, Tier 2, Table 7.1-1, identifies that the guidelines for periodic testing in RG 1.22 and RG 1.118, applies to the RPS. The bypassed and inoperable status indication conforms to the guidelines of RG 1.47. DCD, Tier 2, Section 7.1.2.4, states that the DCIS conforms to the guidelines on the application for the single failure criterion in IEEE Std 379, as supplemented by RG 1.53. DCD, Tier 1, Section 7.1.6.6.1.2 states that FMEAs complying with IEEE Std. 379 will be used to confirm the safety-related systems designs' conformance to the IEEE Std 603, Section 5.1.

DCD, Tier 2, Section 7.2, describes the conformance of RPS to IEEE Std 603, which is evaluated in Section 7.2.3.1 of this report. DCD, Tier 1, Table 2.2.15-2, includes the DAC/ITAAC for verifying that the RPS design was completed in compliance with IEEE Std 603. In particular, DCD Tier 1, Table 2.2.15-2, provides DAC/ITAAC for IEEE Std 603, Sections 5.1, 5.7 and 6.5. DCD Tier, Table 2.2.15-2 also includes DAC/ITAAC for applicable sections of IEEE Std 603, Section 4 for verifying that complete design basis information is identified and implemented for RPS related software projects. Accordingly, based on the applicant's identification of design bases for the RPS, conformance to applicable guidance and IEEE Std 603 sections, and their verification in the DAC/ITAAC, the NRC staff finds that the requirements of GDC 21 has been adequately addressed.

GDC 22 requires, in the pertinent part, that protection systems 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. The NRC staff evaluated whether GDC 22 has been adequately addressed for the RPS. SRP Appendix 7.1-A states that GDC 22 is addressed for protection systems by conformance to IEEE Std 603, Sections 4, 5.1, 5.3, 5.4, 5.5, 5.6, 6.2, 6.3, 6.8, 7.2, and 8. In addition, SRP Section 7.2 identifies that GDC 22 is addressed by conformance to RG 1.75. DCD, Tier 2, Table 7.1-1, identifies that GDC 22 and RG 1.75 apply to the RPS. DCD, Tier 2, Section 7.2, describes the conformance of the RPS to IEEE Std 603, which is evaluated in Section 7.2.3.1 of this report. DCD, Tier 1, Table 2.2.15-2, includes the DAC/ITAAC for verifying that the RPS is in compliance with IEEE Std 603. In particular, DCD, Tier 1, Table 2.2.15-2, provides DAC/ITAAC for IEEE Std 60,3 Section 5.6. DCD Tier 1, Table 2.2.15-2 also includes DAC/ITAAC for applicable sections of IEEE Std 603, Section 4 for verifying that complete design basis information is identified and implemented for RPS related software projects. Accordingly, based on the applicant's identification of design bases for the RPS, conformance to applicable guidance and IEEE Std 603 sections, and their verification in the DCD Tier 1, DAC/ITAAC, the NRC staff finds that the requirements of GDC 22 has been adequately addressed.

GDC 23 requires that protection systems be designed to fail into a safe state or into a state demonstrated to be acceptable on some other defined basis, if certain conditions are experienced. The NRC staff evaluated whether GDC 23 has been adequately addressed for the RPS. SRP Appendix 7.1-A notes that GDC 23 is addressed for protection systems by conformance to IEEE Std 603, Section 5.5. DCD, Tier 2, Table 7.1-1, identifies that GDC 23 applies to the RPS. DCD, Tier 2, Section 7.1.6.6.1.6, states that the RPS fails to a tripped state. Hardware and software failures detected by self-diagnostics cause a trip signal to be generated in the RPS division in which the failure occurs. DCD Tier 1, Table 2.2.15-2 and Section 3.2, provide DAC/ITAAC and Section 3.8 provides ITAAC for verifying that the RPS design was completed in compliance with IEEE Std 603, Section 5.5. Accordingly, based on the conformance to the applicable guidance and IEEE Std 603 sections and their verification in the DCD Tier 1, DAC/ITAAC, the NRC staff finds that the requirements of GDC 23 have been adequately addressed.

GDC 24 requires that the protection system 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. GDC 24 requires that the interconnection of the protection and control systems be limited so as to assure that safety is not significantly impaired. The NRC staff evaluated whether GDC 24 has been adequately addressed for the RPS. SRP Appendix 7.1-A identifies that GDC 24 is addressed for protection systems by

conformance to IEEE Std 603, Sections 5.1, 5.6, 5.12, 6.3, 6.6, and 8, particularly Sections 5.6 and 6.3. DCD, Tier 2, Table 7.1-1, identifies that GDC 24 applies to the RPS. DCD, Tier 2, Section 7.2, describes the conformance of RPS to IEEE Std 603, which are evaluated in Sections 7.2.3.1 and 7.2.3.2 of this report. DCD, Tier 1, Table 2.2.15-2, includes the DAC/ITAAC for verifying that the applicable I&C systems design was completed in compliance with IEEE Std 603, including Sections 5.6 and 6.3. Accordingly, based on the applicant's identification of design bases for the RPS, conformance to applicable IEEE Std 603 sections, and their verification in the DCD Tier 1, DAC/ITAAC, the NRC staff finds that the requirements of GDC 24 has been adequately addressed.

GDC 25 requires that the protection system be designed to assure that specified acceptable fuel design limits are not exceeded for any single malfunction of the reactivity control systems, such as accidental withdrawal (not ejection or dropout) of control rods. The NRC staff evaluated whether GDC 25 has been adequately addressed for the RPS. SRP Appendix 7.1-A states that GDC 25 is addressed for protection systems by conformance to IEEE Std 603, Section 4, which is associated with safety system design-basis requirements. DCD, Tier 2, Section 7.2.1, provides design bases for the RPS that include protection from abnormal operational occurrences such as continuous control rod withdrawal. DCD, Tier 2, Chapter 15, includes analysis for continuous rod withdrawal in several scenarios; the RPS is designed to prevent fuel design limits from being exceeded. DCD, Tier 1, Tables 2.2.1-6 and 2.2.7-4, provide ITAAC for verification of these reactor protection functions. DCD, Tier 1, Table 2.2.15-2 includes DAC/ITAAC for applicable sections of IEEE Std 603, Section 4 for verifying that complete design basis information is identified and implemented for RPS related software projects. Accordingly, based on the applicant's identification of design bases for the RPS, conformance to applicable IEEE Std 603 sections, and their verification in the DCD Tier 1 ITAAC, the NRC staff finds that the requirements of GDC 25 has been adequately addressed.

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. The NRC staff evaluated whether GDC 29 has been adequately addressed for the RPS. SRP Appendix 7.1-A notes that GDC 29 is addressed by conformance as applicable to GDC 20–25 and GDC 28. However, GDC 28, which applies to reactivity control systems, is not applicable to the protection systems evaluated in this section. Accordingly, GDC 29 is addressed by conformance as applicable to GDC 20–25. DCD, Tier 2, Table 7.1-1 and Section 7.2, indicate that applicable sub-systems of RPS conform to GDC 29. In DCD, Tier 1, Sections 2.2.15, 3.2, 3.3, and 3.8 include the DAC/ITAAC for the applicant to verify that the applicable RPS designs implement these design criteria. Accordingly, based on the applicant's identification of design bases for the RPS, conformance to applicable guidance and IEEE Std 603 sections, and their verification in the ITAAC, the NRC staff finds that the requirements of GDC 29 has been adequately addressed.

The NRC staff evaluation of the I&C system in response to the SRM on SECY-93-087, is documented in Section 7.1.1.3.7 of this report. This evaluation is applicable to the RPS. Accordingly, the NRC staff finds that the guidelines of SRM on SECY-93-87 have been adequately addressed for the RPS.

The NRC staff evaluated whether 10 CFR 50.34(f)(2)(v) and (f)(2)(xxiii) have been adequately addressed for the RPS. As described in Section 7.1.1.3.4 of this report, the NRC staff evaluated the I&C system design's compliance with 10 CFR 50.34(f)(2)(v) and (f)(2)(xxiii) and found it acceptable. This evaluation is applicable to RPS. Accordingly the NRC staff finds that the requirements of 10 CFR 50.34(f)(2)(v) and (f)(2)(xxiii) have been adequately addressed for

the RPS.

The NRC staff evaluated whether 10 CFR 50.55a(h) has been adequately addressed for the RPS. 10 CFR 50.55a(h) requires compliance with IEEE Std 603-1991 and the correction sheet dated January 30, 1995, which is evaluated in Sections 7.2.3.1 and 7.2.3.2 of this report and are found to be adequately addressed. Accordingly, the NRC staff finds that 10 CFR 50.55a(h) has been adequately addressed for the RPS

The NRC staff evaluated whether the requirements of 10 CFR 52.47(b)(1) are met. This regulation requires that the application (for design certification) contain proposed ITAAC that are necessary and sufficient to provide reasonable assurance that, if the ITA are performed and the acceptance criteria are met, a plant that references the design certification has been constructed and will operate in accordance with the design certification, the Atomic Energy Act, and the Commission's rules and regulations. The ITAAC specific to the RPS are addressed throughout section 7.2.3 of this report. The NRC staff evaluation of conformance to 10 CFR 52.47 in Section 7.1.1.3.4 of this report is applicable to the RPS. Therefore, the NRC staff finds that the requirements of 10 CFR 52.47(b)(1) have been adequately addressed for the RPS.

7.2.4 Conclusion

Based on the above, the NRC staff concludes that the applicant adequately addresses the major design considerations for the RPS. As discussed in Sections 7.1.1.3.1 through 7.1.1.3.10 of this report and Section 7.2.3 above, the NRC staff concludes for the RPS, the applicant adequately addresses the relevant requirements of 10 CFR 50.55a(a)(1), 10 CFR 50.55a(h), 10 CFR 50.34(f), 10 CFR 52.47(b)(1), GDC 1, 2, 4, 10, 13, 15, 19 - 25, and 29; and the guidelines of SRM on SECY-93-087. The applicant has also identified adequate high-level functions and included sufficient DAC/ITAAC in Tier 1 to verify that RPS design is completed in compliance with the applicable requirements.

7.3 Engineered Safety Features Systems

7.3.1 Regulatory Criteria

The objective of the review of DCD, Tier 1, Section 2.2 and Tier 2, Section 7.3, is to confirm that the ESF actuation and control systems, VBIF, and all subsystems satisfy regulatory acceptance criteria, guidelines, and performance requirements. The review of the I&C aspects of the ESF systems includes the ESF actuation and control systems, VBIF, and all subsystems. The ESF actuation systems detect a plant condition requiring the operation of an ESF system and/or auxiliary supporting features and other auxiliary features and initiates operation of the systems. The ESF control systems regulate the operation of the ESF systems following automatic initiation by the protection system or manual initiation by the plant operator. In the design, the SSLC/ESF system performs the ESF actuation and control systems, VBIF, and all subsystem functions.

Acceptance criteria of the ESF actuation and control systems, VBIF, and all subsystems, and hence the SSLC/ESF system, are based on meeting the relevant requirements of 10 CFR 50.55a(a)(1); 10 CFR 50.55a(h); 10 CFR 50.34(f)(2)(v), (f)(2)(xii), and (f)(2)(xiv); 10 CFR 52.47(b)(1); GDC 1, 2, 4, 10, 13, 15, 16, 19, 20, 21, 22, 23, 24, 29, 33, 34, 35, 38, 41, and 44. The acceptance criteria are also based on conforming to the guidelines of IEEE Std 7-4.3.2, as endorsed by RG 1.152, and the SRM on SECY-93-087.

7.3.2 Summary of Technical Information

7.3.2.1 Engineered Safety Features Systems Description

The I&C ESF systems are part of a group of systems that are collectively referred to as the Q-DCIS. DCD, Tier 2, Section 7.3, describes the ESF systems. The ESF systems for the design include the following:

- ECCS
- PCCS
- LD&IS
- CRHS
- SSLC/ESF system
- Vacuum Breaker Isolation Function (VBIF)
- ICS DPV Isolation Function

7.3.2.1.1 Emergency Core Cooling System

The ECCS comprises the ADS, GDCS, ICS, and the SLC system. The ICS and the SLC system are evaluated in Section 7.4 of this report.

The ADS resides within the NBS. It depressurizes the reactor so that the low-pressure GDCS can provide makeup coolant to the RPV. The ADS I&C perform the following safety functions:

- detect reactor low water level, Level 1
- automatically actuate the SRVs and DPVs after Level 1 is reached or drywell pressure high is detected
- actuate the SRVs and DPVs sequentially and in groups to achieve the required depressurization characteristics
- indicate the status of SRVs and DPVs in the MCR

The GDCS I&C perform the following functions:

- automatically initiate the GDCS to prevent fuel cladding temperatures from reaching the limits of 10 CFR 50.46, “Acceptance Criteria for Emergency Core Cooling Systems for Light-Water Nuclear Power Reactors”
- respond to a need for emergency core cooling, following reactor depressurization, regardless of the physical location of the malfunction or break that causes the need
- be completely automatic in operation (that is, no operator action required). Manual initiation of GDCS is possible at any time, providing that protective interlocks have been satisfied (for example, the reactor is depressurized.)
- prevent the inadvertent actuation of the deluge valves thus preventing inadvertent draining of the GDCS pools

- prevent any single control logic and instrumentation failure from inadvertently opening a GDCS injection valve or equalizing valve

- display GDCS valve positions and GDCS pool levels on the mimic on the WDP in the MCR.

7.3.2.1.2 Passive Containment Cooling System

The PCCS consists of condensers that are an integral part of the containment pressure boundary. The PCCS heat exchanger tubes are located in the isolation condenser/passive containment cooling (IC/PCCS) pool of water outside the containment. A rise in containment (drywell) pressure above the suppression pool (wetwell) pressure, similar to the situation during a loss of reactor coolant into the drywell, forces flow through the PCCS condensers. Condensate from the PCCS drains to the GDCS pools. As the flow passes through the PCCS condensers, heat is rejected to the IC/PCCS pool, thereby cooling the containment atmosphere. This action occurs automatically, without the need for actuation of components. The PCCS does not have instrumentation, control logic, or power-actuated valves and does not need or use electrical power for its operation in the first 72 hours after a LOCA. While the PCCS has no instrumentation and controls (I&C) functions, it does rely on I&C functions in other systems, namely the ICS, SSLC/ESF, and FAPCS to perform its safety functions. The PCCS relies on the water in the Equipment Storage Pool and Reactor Well to perform its safety functions for 72 hours. Pool cross-connect valves are active safety components that open to allow water in the Equipment Storage Pool and Reactor Well to flow into the IC/PCCS pools. FAPCS provides four safety-related level sensors in each IC/PCCS inner expansion pool. The cross-connect valves are opened when a low level condition is detected by the sensors in either pool. FAPCS also provides four non-safety level sensors in each inner expansion pool which are used by DPS to open the cross-connect valves. The air operated cross-connect valves require pneumatic and electrical motive power to open, which is provided by a pneumatic accumulator, and the safety-related Uninterruptible Power System. The squib cross-connect valves are opened pyrotechnically and need only electrical motive power to open, which is provided by the safety-related Uninterruptible Power System. For long-term effectiveness of the PCCS, the vent fans and their isolation valves are manually initiated by operator action. For severe accident events, ignitors have been added to the lower drum of each PCCS heat exchanger to prevent the accumulation of explosive mixtures of hydrogen and oxygen with simultaneous containment high pressure conditions.

7.3.2.1.3 Leak Detection and Isolation System

The primary function of the LD&IS is to detect and monitor leakage from the RCPB and to initiate the appropriate safety action to isolate the source of the leak. The system is designed to automatically initiate the isolation of certain designated process lines penetrating the containment, to prevent release of radioactive material from the RCPB. The initiation of the isolation functions closes the appropriate containment isolation valves. The LD&IS functions are performed in two separate and diverse safety platforms. The MSIV isolation logic functions are performed in the RTIF platform (evaluated in Section 7.2 of this report), while all other containment isolation logic functions are performed in the SSLC/ESF platform. The containment isolation function of LD&IS logic design is fail as-is such that a loss of power to the logic of one division does not result in a trip. The LD&IS logic design is fail-safe, such that loss of electrical power to one LD&IS divisional logic channel initiates a channel trip. The LD&IS control and isolation logic uses 2/4 coincidence voting channels for each plant variable monitored for containment isolation. Various plant variables are monitored, such as flow,

temperature, pressure, RPV water level, and radiation level. These are used in the logic to initiate alarms and the required control signals for containment isolation. Two or more diverse leakage parameters are monitored for each specific isolation function. The LD&IS logic functions reside in the framework of the RTIF and the SSLC/ESF platforms, where trip signals are generated, initiating the isolation functions of the LD&IS. This system operates continuously during normal reactor operation, and during abnormal and accident plant conditions.

7.3.2.1.4 Main Control Room Habitability System

The CRHS is an ESF system that provides a safe environment within the MCR, allowing the operator(s) to do the following:

- control the nuclear reactor and its auxiliary systems during normal conditions
- safely shut down the reactor
- maintain the reactor in a safe condition during abnormal events and accidents

The CRHS safety I&C (part of the SSLC/ESF platform) are designed to isolate the MCR envelope on detection of the following signals and realign to the emergency filtration mode:

- high radiation in the inlet air supply (automatic action – safety function)

- loss of AC power, station blackout, (automatic action – safety function)

- smoke in the inlet air supply or smoke in the CRHS general area (manual isolation – non-safety function)

Additional CRHS safety instrumentation is designed to only swap over the operating emergency filtration train following:

- detection of high radiation downstream of the operating EFU filter train (automatic action) (non-safety function).

- detection of low flow at the outlet of the operating EFU filter train (automatic action) (safety function).

7.3.2.1.5 Safety System Logic and Control/Engineered Safety Features System

The SSLC/ESF system processes automatic and manual demands for ESF system actuations based on sensed plant process parameters or operator request. The SSLC/ESF runs without interruption in all modes of plant operation to support the required safety functions. The SSLC/ESF system includes the controls and instruments that implement the non-MSIV isolation functions of the LD&IS; CRHS; the ECCS functions that include ADS, GDCS, and the SLC system; and the ECCS and shutdown functions of the ICS.

The SSLC/ESF platform provides the following functions:

- monitor safety signals that provide automatic control of the plant safety protection systems

- perform processing of plant sensor and equipment interlock logic signals according to

the required trip and interlock logic, including time delays, of each safety interfacing plant system or system important to safe plant operation

- meet the performance requirements of each safety interfacing plant system or system important to safe plant operation, including transient response, delay time, and overall time to trip system actuators or initiate necessary system operation
- monitor safety manual control switches used for system or component test, protection system manual initiation, and individual control of equipment actuators
- furnish trip outputs signals to actuators driving safety system equipment (e.g., solenoids and squib explosive-actuated valves)
- furnish trip or initiation output signals to the logic of interfacing functions
- provide diagnostic capabilities for detecting failure of safety system components and provide an operator interface that facilitates quick repair
- provide safety accident monitoring display information, alarm, and status outputs to operator displays, annunciators and the plant computer

7.3.2.1.6 Containment System Wetwell-to-Drywell Vacuum Breaker Isolation Function

The VBIF is an independent control platform that, upon detection of excessive vacuum breaker (VB) leakage, prevents the loss of long-term containment integrity. The wetwell-to-drywell VB isolation function has the following safety requirements:

- It automatically isolates an excessively leaking VB using a VB isolation valve
- The VB and VB isolation valve are qualified for a harsh environment inside the drywell
- Manual opening and closing of a VB isolation valve are provided
- No single control logic and instrument failure will open/close more than one VB isolation valve
- VB and VB isolation valve positions are displayed in the MCR
- The safety function is met with one VB/VB isolation valve path isolated together with any active identifiable single failure
- Divisional instruments performing VB isolation valve logic are powered by the associated safety divisional power supplies
- VB isolation function logic controllers use independent platform that is independent and diverse from the RTIF-NMS and the SSLC/ESF platforms
- Containment system VBIF logic controllers are independent

7.3.2.1.7 ICS DPV Isolation Function

The ICS DPV isolation function which is implemented in the ICP prevents the loss of long-term containment integrity upon detection of DPV open position.

The ICS DPV isolation function has the following safety-related requirements:

- Automatically isolates all Isolation Condensers by closing the two steam admission isolation valves to each of the ICs.
- The two steam admission isolation valves per IC are qualified for a harsh environment inside the drywell.
- Manual opening and closing of the IC steam admission isolation valves is provided for in the design.
- No single control logic and instrumentation failure opens/closes more than one IC steam admission isolation valve.
- IC steam admission isolation valve positions are displayed in the MCR.
- The safety-related function is met with one IC steam admission valve path isolated together with any active identifiable single failure.
- Divisional instruments performing IC steam admission valve isolation valve logic are powered by the associated safety-related divisional power supplies.
- ICS DPV isolation function logic controllers are independent.

7.3.2.2 Safety System Logic and Control/Engineered Safety Features System Architecture

The SSLC/ESF resides in four independent and separated instrumentation divisions. The SSLC/ESF integrates the control logic of the safety systems in each division into microprocessor-based, software-controlled, processing modules located in divisional cabinets in the safety equipment room of the control building. Most SSLC/ESF input data are process variables multiplexed via the Q-DCIS in four physically and electrically isolated redundant instrumentation divisions. Each of the four independent and separated Q-DCIS divisions feeds separate and independent trains of SSLC/ESF equipment in the corresponding division. All input data are processed within the RMUs function of the Q-DCIS. The sensor data are transmitted through the DCIS network to the SSLC/ESF system's DTM function for setpoint comparison. A trip (or actuation) signal is generated from this function. Processed trip signals from a division and trip signals from the other three divisions are transmitted through the CIMs and are processed in the voter logic unit (VLU) function for 2/4 voting. There are two independent and redundant VLU functional trains (three for the DPV actuation logic) in each division of the SSLC/ESF equipment. The voter logic trip signals from each VLU functional train are transmitted to the RMUs, where a 2/4 (or two-out-of-three (2/3)) confirmation is performed. The redundant trains within a division are necessary to prevent single failures within a division from causing a squib initiator to fire; as a result, each VLU logic train is required to operate to get an output. Self-tests within the SSLC/ESF determine if any one VLU function has failed, and the failure is alarmed in the MCR. To prevent single I&C failure from causing inadvertent

actuations, a failed VLU function cannot be bypassed for any of the ECCS logic for squib valves initiation. Trip signals are hard-wired from the RMUs to the equipment actuator. The final trip signal (from two or more divisions) is then transmitted to the RMUs function via the Q-DCIS network to initiate mechanical actuation devices.

At the division level, the four redundant divisions provide a fault-tolerant architecture that allows single division of sensor bypass for online maintenance, testing, and repair with the intent of not losing trip capability. In bypass condition (i.e., when a division of sensor inputs is bypassed), the system automatically defaults to 2/3 coincident voting.

7.3.3 NRC Staff Evaluation

The NRC staff reviewed the SSLC/ESF system in accordance with SRP Section 7.3. The NRC staff also used acceptance criteria in SRP Section 7.1, SRP Table 7-1, SRP Appendix 7.1-A, and SRP Appendix 7.1-C, as directed by SRP Section 7.3. The acceptance criteria listing used as the basis for the NRC staff's review of the SSLC/ESF system is described in Section 7.3.1 of this report.

SRP Section 7.1 describes the procedures to be followed in reviewing any I&C system. SRP Section 7.3 highlights specific topics that should be emphasized in reviewing the ESF actuation and control systems, VBIF, and all subsystems and are addressed in Section 7.3.3.1 of this report. The NRC staff included the review of the DCD Tier 1, DAC/ITAAC during the review of this section because of the significant role of the DAC/ITAAC in determining the SSLC/ESF system conformance to all requirements.

As described in Section 7.1.1.3.1 of this report, the DCD does not provide the required SSLC/ESF system design information to comply with IEEE Std 603. Instead, the applicant has included the DAC/ITAAC in DCD, Tier 1, Section 2.2.15, to confirm that the completed SSLC/ESF system design complies with IEEE Std 603. DCD, Tier 1, Section 2.2.15 also includes an ITAAC applicability table (Table 2.2.15-1), which identifies the applicability of the IEEE Std 603 criteria DAC/ITAAC to the SSLC/ESF system. The NRC staff has accepted the DAC approach to addressing compliance with IEEE Std 603. The NRC staff evaluation of conformance to IEEE Std 603 in Section 7.1.1.3.10 of this report is applicable to the SSLC/ESF.

In RAI 7.1-99, the NRC staff asked the applicant to clarify the applicability of IEEE Std 603 criteria in a consistent manner throughout DCD Tier 2, Chapter 7. By letter MFN 09-089, dated February 19, 2009, the applicant submitted a response to RAI 7.1-99, along with responses to 7.1-100, 7.1-101, and 14.3-265, Supplement 1, all of which are incorporated in DCD Revision 6. Section 7.1.1.3.1 of this report provides additional discussion of these RAI responses. With regard to the NRC staff evaluation of the SSLC/ESF system, the applicant significantly revised DCD Tier 2, Tables 7.1-1 and 7.1-2 to clearly identify applicability of IEEE Std 603 criteria for each SSLC/ESF subsystem. Concurrently, many references to IEEE Std 603 criteria were revised or removed from the discussions of SSLC/ESF subsystems in DCD, Tier 2, Section 7.3 to address the consistency concerns. Accordingly, statements regarding applicability of IEEE Std 603 criteria provided in the NRC staff SER with open items have been updated or removed from the remainder of Section 7.3.3 of this report to be consistent with DCD Revision 6.

7.3.3.1 Evaluation of Engineered Safety Features Actuation and Control Systems Conformance with Acceptance Criteria - Major Design Considerations

Per SRP Section 7.3, the following are the major design considerations that should be

emphasized in the ESF actuation and control systems, VBIF, ICS DPVIF, and all subsystems review:

(1) Design Basis (IEEE Std 603, Section 4)

The NRC staff evaluated the ESF actuation and control systems, VBIF, and all subsystems design basis to determine whether IEEE Std 603, Section 4, was adequately addressed using SRP Appendix 7.1-C, Section 4, "Safety System Designation (IEEE Std 603)." For completeness, the SRP states, "As a minimum each of the safety system design basis aspects identified in IEEE Std 603, Sections 4.1 through 4.12 should be addressed." This criterion is evaluated in Section 7.1.1.3.10 of this report, where the NRC staff finds that Section 4 is adequately addressed based on its inclusion in the safety system design basis and the verification of applicable criteria in the DCD, Tier 1, Section 2.2.15, DAC/ITAAC. This evaluation is applicable to the SSLC/ESF system. Also, DCD, Tier 1, Table 2.2.15-1, identifies that the DAC/ITAAC for applicable criteria of Section 4 are applicable to the RPS and all subsystems.

DCD, Tier 2, Section 7.3, identifies individual parameters that determine operation of the ESF actuation and control systems, VBIF, ICS DPVIF, and all subsystems. As mentioned previously, NEDE-33226P and NEDE-33245P, as part of the software life cycle process, define a process by which plant performance requirements, including response times, under various operational conditions will be specified, implemented, and tested. DCD, Tier 1, Section 3.2, includes the DAC/ITAAC for verifying that the software plans were developed and implemented consistent with this process and produce acceptable design outputs. Accordingly, the NRC staff finds that Section 4 is adequately addressed for the ESF actuation and control systems, VBIF, ICS DPVIF, and all subsystems.

(2) Single Failure Criterion (IEEE Std 603, Section 5.1)

The NRC staff evaluated whether the single failure criterion, IEEE Std 603, Section 5.1, has been adequately addressed for the ESF actuation and control systems. This criterion requires that any single failure within the safety system shall not prevent proper protective action at the system level when required. This criterion is evaluated in Section 7.1.1.3.10 of this report where the NRC staff finds that Section 5.1 is adequately addressed based on its inclusion in the safety system design basis and its verification in the DCD, Tier 1, Section 2.2.15, DAC/ITAAC. This evaluation applicable to the ESF actuation and control systems, VBIF, ICS DPVIF, and all subsystems. Also, DCD Tier 1, Table 2.2.15-1, identifies that the DAC/ITAAC for Section 5.1 are applicable to the ESF actuation and control systems, VBIF, ICS DPVIF, and all subsystems. Accordingly, the NRC staff finds that Section 5.1 is adequately addressed for the ESF actuation and control systems, VBIF, ICS DPVIF, and all subsystems.

(3) Quality of Components and Modules (IEEE Std 603, Section 5.3)

The NRC staff evaluated whether the quality criterion, IEEE Std 603, Section 5.3, has been adequately addressed for the ESF actuation and control systems, VBIF, ICS DPVIF, and all subsystems. This criterion is evaluated in Section 7.1.1.3.10 of this report, where the NRC staff finds that Section 5.3 has been adequately addressed based on the inclusion of IEEE Std 7-4.3.2, Section 5.3, in the safety system design basis and the verification of the software development activities in the DCD, Tier 1, Section 3.2, DAC/ITAAC. Also, the applicant has stated that the quality assurance program conforms to GDC 1. The evaluation of the adequacy of the quality assurance program is addressed in Chapter 17 of this report. These evaluations

are applicable to the ESF actuation and control systems, VBIF, ICS DPVIF, and all subsystems. Also DCD, Tier 2, Section 7.1.6.6.1.4, discusses the applicability of this criterion to the Q-DCIS design. Accordingly, based on the applicant's use of an acceptable software development process, as evaluated in Section 7.1.2.3 of this report, and its verification in the DCD Tier 1, DAC/ITAAC, the NRC staff finds that 5.3 of IEEE Std 7-4.3.2 and Section 5.3 of IEEE Std 603 are adequately addressed for the ESF actuation and control systems, VBIF, ICS DPVIF, and all subsystems.

(4) Independence (IEEE Std 603, Sections 5.6 and 6.3)

The NRC staff evaluated whether the independence-related criteria, IEEE Std 603, Sections 5.6 and 6.3, were adequately addressed for the ESF actuation and control systems, VBIF, ICS DPVIF, and all subsystems. IEEE Std 603, Section 5.6, is evaluated in Section 7.1.1.3.10 of this report, where the NRC staff finds that Section 5.6 is adequately addressed based on its inclusion in the safety systems design basis and its verification in the DCD, Tier 1, Section 2.2.15, DAC/ITAAC. Also DCD, Tier 1,Table 2.2.15-1 identifies that the DAC/ITAAC for Section 5.6 is applicable to the ESF actuation and control systems, VBIF, ICS DPVIF, and all subsystems. Accordingly, the NRC staff finds that IEEE Std 603, Section 5.6, is adequately addressed for the ESF actuation and control systems, VBIF, ICS DPVIF, and all subsystems.

The NRC staff evaluated conformance with IEEE Std 603, Section 6.3. This criterion is evaluated in Section 7.1.1.3.10 of this report where the NRC staff finds that Section 6.3 is adequately addressed based on its inclusion in the safety systems design basis and its verification in the DCD, Tier 1, Section 2.2.15, DAC/ITAAC. This evaluation is applicable to the ESF actuation and control systems, VBIF, ICS DPVIF, and all subsystems. Also, DCD, Tier 1, Table 2.2.15-1 identifies that the DAC/ITAAC for Section 6.3 is applicable to the ESF actuation and control systems, VBIF, ICS DPVIF, and all subsystems. Accordingly, the NRC staff finds that IEEE Std 603, Section 6.3, is adequately addressed for the ESF actuation and control systems, VBIF, ICS DPVIF, and all subsystems.

(5) Completion of Protective Action (IEEE Std 603, Section 5.2)

The NRC staff evaluated whether the completion of the protective action criterion, IEEE Std 603, Section 5.2, has been adequately addressed for the ESF actuation and control systems, VBIF, ICS DPVIF, and all subsystems. This criterion is evaluated in Section 7.1.1.3.10 of this report where the NRC staff finds that Section 5.2 is adequately addressed based on its inclusion in the safety system design basis and its verification in the DCD, Tier 1, Section 2.2.15, DAC/ITAAC. This evaluation is applicable to the ESF actuation and control systems, VBIF, ICS DPVIF, and all subsystems. Also, DCD, Tier 1, Table 2.2.15-1, identifies that IEEE Std 603, Section 5.2, is applicable to the ESF actuation and control systems, VBIF, ICS DPVIF, and all subsystems. Accordingly, the NRC staff finds that IEEE Std 603, Section 5.2, has been adequately addressed for the ESF actuation and control systems, VBIF, ICS DPVIF, and all subsystems.

(6) Diversity and Defense-in-Depth

The NRC staff evaluated whether the D3 criteria have been adequately addressed for the ESF actuation and control systems, VBIF, ICS DPVIF, and all subsystems. A general evaluation of the conformance of safety I&C systems to the D3 criteria is provided in Section 7.1.3 of this report. For ESF systems, these criteria identify that the systems should incorporate multiple means for responding to each event discussed in DCD, Tier 2, Chapter 15. At least one pair of

these means for each event should have the property of signal diversity. In the ESBWR design, the applicant has implemented the diversity and defense-in-depth principle (i.e., 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 are sensed incorrectly (see NUREG/CR-6303). NEDO-33251, states conformity to NUREG/CR-6303. DCD Tier 1, Table 2.2.14-4, includes ITAAC for the applicant to complete an FMEA per NUREG/CR-6303 of the safety protection system platforms to validate the DPS functions. The NRC staff evaluation of conformance to D3 in Section 7.1.3.3 of this report is applicable to the SSLC/ESF system and the VB isolation function. Accordingly, the NRC staff finds that D3 is adequately addressed for the ESF actuation and control systems, VBIF, ICS DPVIF, and all subsystems.

(7) System Testing and Inoperable Surveillance (IEEE Std 603, Sections 5.7, 5.8, and 6.5)

The NRC staff evaluated whether the criteria related to system testing and inoperable surveillance, IEEE Std 603, Sections 5.7, 5.8, and 6.5, have been adequately addressed for ESF actuation and control systems, VBIF, ICS DPVIF, and all subsystems. IEEE Std 603, Section 5.7, is evaluated in Section 7.1.1.3.10 of this report, where the NRC staff finds that Section 5.7 is adequately addressed based on its inclusion in the safety systems design basis and its verification in the DCD, Tier 1, Section 2.2.15, DAC/ITAAC. This evaluation is applicable to the ESF actuation and control systems, VBIF, ICS DPVIF, and all subsystems. DCD Tier 1, Table 2.2.15-1 identifies that the DAC/ITAAC for Section 5.7 is applicable to the ESF actuation and control systems, VBIF, ICS DPVIF, and all subsystems. Accordingly, the NRC staff finds that IEEE Std 603, Section 5.7, is adequately addressed for the ESF actuation and control systems, VBIF, ICS DPVIF, and all subsystems.

The NRC staff evaluated whether IEEE Std 603, Section 5.8, has been adequately addressed for the ESF actuation and control systems, VBIF, ICS DPVIF, and all subsystems. This criterion is evaluated in Section 7.1.1.3.10 of this report, where the NRC staff finds that Section 5.8 is adequately addressed based on its inclusion in the safety systems design basis and its verification in the DCD, Tier 1, Section 3.3, DAC/ITAAC. This evaluation is applicable to the ESF actuation and control systems, VBIF, ICS DPVIF, and all subsystems. DCD, Tier 2, Chapter 18, describes the HFE design process to design information displays and is evaluated in Chapter 18 of this report. DCD, Tier 1, Section 3.3, includes the DAC/ITAAC for implementing the HFE design process, which includes the design and verification of controls and information displays for monitoring variables and systems in the control room. This verification is applicable to the ESF actuation and control systems, VBIF, ICS DPVIF, and all subsystems, and it includes the inventory of displays for manually controlled actions, system status indications, and indications of bypasses. Accordingly, the NRC staff finds that IEEE Std 603, Section 5.8, is adequately addressed for the ESF actuation and control systems, VBIF, ICS DPVIF, and all subsystems.

The NRC staff evaluated conformance with IEEE Std 603, Section 6.5. This criterion is evaluated in Section 7.1.1.3.10 of this report, where the NRC staff finds that Section 6.5 is adequately addressed based on its inclusion in the safety systems design basis and its verification in the DCD, Tier 1, Section 2.2.15, DAC/ITAAC. This evaluation is applicable to the ESF actuation and control systems, VBIF, ICS DPVIF, and all subsystems DCD, Tier 1, Table 2.2.15-1 identifies that the DAC/ITAAC for Section 6.5 is applicable to the ESF actuation and control systems, VBIF, ICS DPVIF, and all subsystems. Accordingly, the NRC staff finds that IEEE Std 603, Section 6.5, is adequately addressed for the ESF actuation and control systems, VBIF, ICS DPVIF, and all subsystems.

(8) Use of Digital Systems (IEEE Std 7-4.3.2)

The NRC staff evaluated whether IEEE Std 7-4.3.2, as endorsed by RG 1.152, has been adequately addressed for ESF actuation and control systems, VBIF, ICS DPVIF, and all subsystems. SRP Appendix 7.1-D provides guidance on the implementation of IEEE Std 7-4.3.2 concerning the use of digital systems. In Section 7.1.1.3.10 of this report, the NRC staff evaluated in parallel IEEE Std 7-4.3.2 and IEEE Std 603 using the guidance in SRP Appendix 7.1-D. The NRC staff evaluation of conformance to IEEE Std 7-4.3.2 in Section 7.1.1.3.10 of this report is applicable to the ESF actuation and control systems, VBIF, ICS DPVIF, and all subsystems.

The software development activities are described in NEDE-33226P and NEDE-33245P. DCD, Tier 1, Section 3.2, includes the DAC/ITAAC to confirm that the completion of these activities and products conforms to the processes described in NEDE-33226P and NEDE-33245P and the guidelines of BTP HCIB-14. The NRC staff evaluation of software development activities is provided in Section 7.1.2 of this report. Accordingly, the NRC staff finds that Use of Digital Systems is adequately addressed for the ESF actuation and control systems, VBIF, ICS DPVIF, and all subsystems.

(9) Setpoint Determination

The setpoint determination methodology is evaluated in Section 7.1.4 of this report.

7.3.3.2 Evaluation of the Conformance of Engineered Safety Features Actuation and Control Systems with Acceptance Criteria - Other Criteria

SRP Section 7.3 states that ESF actuation and control systems, VBIF, ICS DPVIF, and all subsystems designs should be evaluated for conformance to IEEE Std 603. This section evaluates IEEE Std 603 criteria not previously evaluated in Section 7.3.3.1 of this report. .

The NRC staff evaluated conformance with IEEE Std 603, Sections 5.9, 5.10, 5.11, 5.12, 6.1, 6.2. 6.4, 6.6, 6.7, 6.8, 7.1, 7.2, 7.3, 7.4, 7.5, 8.1, 8.2, and 8.3. These criteria are evaluated in Section 7.1.1.3.10 of this report, where the NRC staff finds that these criteria are adequately addressed based on their inclusion in the safety system design basis and their verification in the DCD, Tier 1, Section 2.2.15, DAC/ITAAC. This evaluation is applicable to the ESF actuation and control systems, VBIF, ICS DPVIF, and all subsystems. Also, DCD, Tier 1, Table 2.2.15-1, identifies that the DAC/ITAAC for these criteria are applicable to the ESF actuation and control systems, VBIF, ICS DPVIF, and all subsystems. Accordingly, the NRC staff finds that conformance to IEEE Std 603, Sections 5.9, 5.10, 5.11, 5.12, 6.1, 6.2. 6.4, 6.6, 6.7, 6.8, 7.1, 7.2, 7.3, 7.4, 7.5, 8.1, 8.2, and 8.3 are adequately addressed for the applicable to the ESF actuation and control systems, VBIF, ICS DPVIF, and all subsystems.

The NRC staff evaluated conformance to IEEE Std 603, Section 5.4. This criterion is evaluated in Section 7.1.1.3.10 of this report, where the NRC staff finds that Section 5.4 is adequately addressed based on its inclusion in the safety systems design basis and verification of the EQ in the DCD, Tier 1, Section 3.8, ITAAC. This evaluation is applicable to the ESF actuation and control systems, VBIF, ICS DPVIF, and all subsystems. Accordingly, the NRC staff finds that IEEE Std 603, Section 5.4, is adequately addressed for the ESF actuation and control systems, VBIF, ICS DPVIF, and all subsystems.

The NRC staff evaluated conformance to IEEE Std 603, Section 5.5. This criterion is evaluated in Section 7.1.1.3.10 of this report, where the NRC staff finds that Section 5.5 is adequately addressed based on its inclusion in the safety systems design basis and its verification in the DCD, Tier 1, Section 2.2.15 and Section 3.2, DAC/ITAAC and Section 3.8, ITAAC. This evaluation is applicable to the ESF actuation and control systems, VBIF, ICS DPVIF, and all subsystems. Accordingly, the NRC staff finds that IEEE Std 603, Section 5.5, is adequately addressed for the ESF actuation and control systems, VBIF, ICS DPVIF, and all subsystems.

The NRC staff evaluated conformance with IEEE Std 603, Section 5.13. This criterion is evaluated in Section 7.1.1.3.10 of this report. The multi-unit station criteria do not apply to the standard single unit plant design submitted for NRC certification. The NRC staff finds that IEEE Std 603, Section 5.13, is not applicable to the ESBWR design certification.

The NRC staff evaluated conformance with IEEE Std 603, Section 5.14. This criterion is evaluated in Section 7.1.1.3.10 of this report, where the NRC staff finds that Section 5.14 is adequately addressed based on its inclusion in the safety systems design basis and its verification in the DCD, Tier 1, Section 3.3, DAC/ITAAC. This evaluation is applicable to the ESF actuation and control systems, VBIF, ICS DPVIF, and all subsystems. Accordingly, the NRC staff finds that IEEE Std 603, Section 5.14, is adequately addressed for the ESF actuation and control systems, VBIF, ICS DPVIF, and all subsystems.

The NRC staff evaluated conformance with IEEE Std 603, Section 5.15. This criterion is evaluated in Section 7.1.1.3.10 of this report, where the NRC staff states that Section 5.15 is adequately addressed based on its inclusion in the safety systems design basis and its verification in the DCD, Tier 1, Section 2.2.15, DAC/ITAAC for IEEE Std 603, Section 5.1, DCD, Tier 1, Section 3.2, DAC/ITAAC, and DCD, Tier 1, Section 3.6, ITAAC. This evaluation is applicable to the ESF actuation and control systems, VBIF, ICS DPVIF, and all subsystems. Accordingly, the NRC staff finds that IEEE Std 603, Section 5.15, is adequately addressed for the ESF actuation and control systems, VBIF, ICS DPVIF, and all subsystems.

7.3.3.3 Evaluation of Engineered Safety Features Actuation and Control Systems Compliance with Regulations and Conformance to the NRC Staff Requirements Memorandum on SECY-93-087

The NRC staff reviewed the regulations in the acceptance criteria for the ESF actuation and control systems in accordance with SRP Section 7.3 and SRP Appendix 7.1-A. For several of the GDC, compliance can be satisfied by meeting IEEE Std 603 requirements, which the NRC staff evaluated in the previous two sections. Compliance with IEEE Std 603 is briefly discussed with the relevant GDC, including the use of DAC, consistent with both SRP sections.

GDC 1 requires quality standards and maintenance of appropriate records.
10 CFR 50.55a(a)(1) requires that structures, systems, and components must be designed, fabricated, erected, constructed, tested, and inspected to quality standards commensurate with the importance of the safety function to be performed. The NRC staff evaluated whether GDC 1 and 10 CFR 50.55a(a)(1) have been adequately addressed for the ESF actuation and control systems, VBIF, ICS DPVIF, and all subsystems per SRP Appendix 7.1-A, which states that the NRC staff review should confirm that the appropriate regulatory guides and endorsed standards are identified as applicable for each I&C system important to safety. DCD, Tier 2, Table 7.1-1 identifies that GDC 1 and 10 CFR 50.55a(a)(1) are applicable to the RPS. The NRC staff evaluation of conformance to RGs and standards for 10 CFR 50.55a(a)(1) and GDC 1 in Sections 7.1.1.3.3 and 7.1.1.3.6 of this report is applicable to the ESF actuation and control

systems, VBIF, ICS DPVIF, and all subsystems. Accordingly, based on applicable codes and standards being identified as applicable to the RPS, the NRC staff finds that the requirements of GDC 1 and 10 CFR 50.55a(a)(1) have been adequately addressed.

GDC 2 requires design bases for protection against natural phenomena. GDC 4 requires environmental and dynamic effect design bases. The NRC staff evaluated whether GDC 2 and 4 have been adequately addressed for the ESF actuation and control systems, VBIF, ICS DPVIF, and all subsystems. SRP Section 7.3 identifies that GDC 2 and 4 are addressed by the identification of those systems and components for the ESF actuation and control systems, VBIF, ICS DPVIF, and all subsystems designed to survive the effects of earthquakes, other natural phenomena, abnormal environments and missiles in the design bases. SRP Section 7.3 also identifies that GDC 2 and 4 are addressed by the review of the qualification program in DCD, Tier 2, Sections 3.10 and 3.11. DCD Tier 2, Table 7.1-1, identifies that GDC 2 and 4 are applicable to the ESF actuation and control systems, VBIF, ICS DPVIF, and all subsystems. DCD, Tier 2, Table 3.2-1, identifies that the safety ESF actuation and control systems, VBIF, ICS DPVIF, and all subsystems are designed as seismic Category I system. In DCD, Tier 2, Sections 3.10 and 3.11 describe the EQ programs for safety electrical and digital I&C equipment, which are evaluated in Chapter 3 of this report. DCD, Tier 1, Table 3.8-1, Items 1 and 3, include ITAAC for the applicant to verify the EQ of safety electrical and digital I&C equipment. The evaluation of GDC 2 and GDC 4 in Section 7.1.1.3.6 of this report further addresses these topics and is applicable to the ESF actuation and control systems, VBIF, ICS DPVIF, and all subsystems. Accordingly, based on the applicant's identification of EQ programs consistent with the design bases for the ESF actuation and control systems, VBIF, ICS DPVIF, and all subsystems, and their verification in the ITAAC, the NRC staff finds that the requirements of GDC 2 and 4 have been adequately addressed.

GDC 10 requires that the reactor core and associated coolant, control, and protection systems 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. GDC 15 requires that the reactor coolant system and associated auxiliary, control, and protection system be designed with sufficient margin to ensure that the design conditions of the reactor coolant pressure boundary are not exceeded during any condition of normal operation, including AOOs. The NRC staff evaluated whether GDC 10 and 15 have been adequately addressed for the ESF actuation and control systems, VBIF, ICS DPVIF, and all subsystems. SRP Appendix 7.1-A for GDC 10 and 15 states that the NRC staff review should evaluate the I&C system contributions to design margin for reactor core and reactor coolant systems. DCD, Tier 2, Table 15.1-6, identifies systems, including ESF actuation and control systems, VBIF, ICS DPVIF, and all subsystems, required to mitigate AOOs affecting the reactor core and reactor coolant systems. DCD, Tier 2, Chapter 7, includes corresponding actions in the design bases of the ESF actuation and control systems, VBIF, ICS DPVIF, and all subsystems to maintain the reactor core and reactor coolant system within appropriate margins. In DCD, Tier 1, Sections 2.2.15, 3.2, 3.3, and 3.8 include the DAC/ITAAC for the applicant to verify that the ESF actuation and control systems, VBIF, ICS DPVIF, and all subsystems design implement these design bases. Accordingly, based on the applicant's identification of necessary protection and safety actuations in the design bases for the ESF actuation and control systems, VBIF, ICS DPVIF, and all subsystems, and their verification in the DCD Tier 1, DAC/ITAAC, the NRC staff finds that the requirements of GDC 10 and 15 have been adequately addressed.

GDC 16 requires that reactor containment and associated systems be provided to establish an essentially leak-tight barrier against the uncontrolled release of radioactivity to the environment and to assure that the containment design conditions important to safety are not exceeded for

as long as postulated accident conditions require. The NRC staff evaluated whether GDC 16 has been adequately addressed for the ESF actuation and control system. SRP Appendix 7.1-A for GDC 16 states that GDC 16 imposes functional requirements on ESF actuation and control systems, VBIF, ICS DPVIF, and all subsystems to the extent that they support the requirement that the containment provide a leak tight barrier. DCD, Tier 2, Sections 7.3.3 and 7.3.5, identify the containment isolation functions in the LD&IS and ESF actuation and control systems, VBIF, ICS DPVIF, and all subsystems design bases. In DCD, Tier 1, Sections 2.2.15, 3.2, 3.3, and 3.8 include the DAC/ITAAC for the applicant to verify that the ESF actuation and control systems, VBIF, ICS DPVIF, and all subsystems designs implement these design bases. Accordingly, based on the applicant's identification of necessary containment isolation functions in the design bases of the ESF actuation and control systems, VBIF, ICS DPVIF, and all subsystems, and their verification in the DCD Tier 1, DAC/ITAAC, the NRC staff finds that the requirements of GDC 16 have been adequately addressed.

GDC 13 requires providing instrumentation to monitor variables and systems over their anticipated ranges for normal operation, AOOs, and accident conditions to assure adequate safety. GDC 13 also requires providing appropriate controls to maintain these variables and systems within prescribed operating ranges. GDC 19 requires control room functionality, control room habitability, and remote shutdown capability. The NRC staff evaluated whether GDC 13 and 19 have been adequately addressed for the ESF actuation and control systems, VBIF, ICS DPVIF, and all subsystems. The evaluation of GDC 19 is provided in Section 7.1.1.3.6 of this report with the exception of ESF actuation and control systems, VBIF, ICS DPVIF, and all subsystems support functions necessary for operating the reactor. SRP Section 7.3 identifies that GDC 13 and 19 are addressed by the review of the ESF actuation and control systems, VBIF, ICS DPVIF, and all subsystems status information, manual initiation capabilities, and control capabilities.

DCD, Tier 2, Sections 7.3.1.1.2, 7.3.1.2.2, and 7.3.6.2, specify the automatic and manual initiation and control capabilities of the ADS, GDCS, VBIF, and ICS DPVIF, respectively. DCD, Tier 2, Sections 7.3.1.1.5, 7.3.1.2.5, and 7.3.6.5, specify the status information and the alarms provided in the MCR for the ADS, GDCS, VBIF, and ICS DPVIF, respectively. DCD, Tier 2, Section 7.3.3.2, specifies the automatic controls of the LD&IS. DCD, Tier 2, Section 7.3.3.3, specifies the manual initiation and control of the LD&IS. DCD, Tier 2, Section 5.2.5.2, specifies the LD&IS monitoring capabilities. DCD, Tier 2, Section 5.2.5.2, specifies that (1) monitored plant leakage parameters are measured, recorded and displayed on the appropriate panels in the MCR, (2) all abnormal indications are annunciated for operator alert to initiate corrective action, and (3) all initiated automatic or manual isolation functions are also alarmed in the MCR. DCD, Tier 2, Section 7.3.4.2, specifies the automatic and manual initiation and control of the CRHS. Additional control information and status and alarm information is described in DCD, Tier 2, Sections 9.4.1.5 and 6.4.8. The identified DCD sections above address GDC 13 by identifying the ESF actuation and control systems monitoring and control functions. The identified DCD sections above address GDC 19 by identifying the that the monitoring and control functions are available in the MCR, By design of the Q-DCIS, all monitoring and controls in the MCR are available for remote shutdown.

In combination with the following identified interrelated processes to complete the design of the monitoring capability and controls for the ESF actuation and control systems, VBIF, ICS DPVIF, and all subsystems, the NRC staff finds these monitoring capabilities and controls acceptable. NEDE-33226P and NEDE-33245P, as part of a software life cycle process, define processes by which plant performance requirements under various operational conditions will be specified,

implemented, and tested. DCD, Tier 1, Section 3.2, includes the DAC/ITAAC for verifying that the software plans are developed and implemented consistent with this process and produce acceptable design outputs. DCD, Tier 1, Section 3.3, includes the DAC/ITAAC for implementing an HFE design process, which includes the design and verification of controls and information displays for monitoring variables and systems in the control room. These verifications are applicable to the ESF actuation and control systems, VBIF, ICS DPVIF, and all subsystems and include verifications of the controls for manual initiation and control of ESF functions necessary to support actions to operate the nuclear power unit safely under normal conditions and to maintain it in a safe condition under accident conditions. Accordingly, based on the identified monitoring capabilities and control room controls, as well as the defined processes for completing their design and their verification in the DCD Tier 1, DAC/ITAAC, the NRC staff finds that the requirements of GDC 13 and 19 have been adequately addressed.

GDC 20 requires that the protection system be designed to (1) initiate automatically the operation of the appropriate systems including reactivity control systems, to ensure that specified acceptable fuel design limits are not exceeded as a result of AOOs and (2) sense accident conditions and initiate the operation of systems and components important to safety. The NRC staff evaluated whether GDC 20 has been adequately addressed for the ESF actuation and control systems, VBIF, ICS DPVIF, and all subsystems. Appendix 7.1-A to the SRP states that GDC 20 is addressed for protection systems by conformance to IEEE Std 603, Sections 4, 5, 5.5, 6.1, 6.8, and 7.1. The applicant has committed to following the guidance of RG 1.105 , and has provided a setpoint methodology in NEDE-33304P. The NRC staff also evaluated the ESF actuation and control design basis requirements, general functional requirements, and system integrity, involving IEEE Std 603, Sections 4, 5, 5.5, 6.1, and 7.1, in Section 7.3.3.1 of this report. DCD, Tier 1, Table 2.2.15-2 includes the DAC/ITAAC for verifying that the safety functions of setpoints are defined, determined, and implemented based on the defined setpoint methodology and for completing the design in compliance with IEEE Std 603. DCD, Tier 1, Table 2.2.15-2 also includes DAC/ITAAC for applicable sections of IEEE Std 603, Section 4 for verifying that complete design basis information is identified and implemented for ESF actuation and control systems, VBIF and ICS DPVIF, related software projects. The NRC staff evaluation of conformance to IEEE Std 603 in Section 7.1.1.3.10 of this report is applicable to the ESF actuation and control systems, VBIF, ICS DPVIF, and all subsystems. Accordingly, based on the applicant's identification of design bases for the ESF actuation and control systems, VBIF, ICS DPVIF, and all subsystems, conformance to applicable guidance and IEEE Std 603 sections, and their verification in the DAC/ITAAC, the NRC staff finds that the requirements of GDC 20 has been adequately addressed.

GDC 21 requires that protection systems be designed for high functional reliability and in-service testability commensurate with the safety functions to be performed. The NRC staff evaluated whether GDC 21 has been adequately addressed for the ESF actuation and control systems, VBIF, ICS DPVIF, and all subsystems. SRP Appendix 7.1-A states that GDC 21 is addressed for protection systems by conformance to IEEE Std 603 criteria except for Sections 5.4, 6.1, and 7.1. In addition, SRP Section 7.3 identifies that GDC 21 is addressed by conformance to RGs 1.22, 1.47, 1.53, 1.118, and IEEE Std 379. DCD, Tier 2, Table 7.1-1, identifies that the guidelines for periodic testing in RG 1.22 and RG 1.118, applies to the ESF actuation and control systems, VBIF, ICS DPVIF, and all subsystems. The bypassed and inoperable status indication conforms to the guidelines of RG 1.47. DCD, Tier 2, Section 7.1.2.4, states that the DCIS conforms to the guidelines on the application for the single failure criterion in IEEE Std 379, as supplemented by RG 1.53. DCD, Tier 2, Section 7.3, describes the conformance of the ESF actuation and control systems, VBIF, ICS DPVIF, and all subsystems to IEEE Std 603, which is evaluated in Section 7.3.3.1 of this report. DCD, Tier 1,

Table 2.2.15-2 includes the DAC/ITAAC for verifying that the design of the ESF actuation and control systems, VBIF, ICS DPVIF, and all subsystems is completed in compliance with IEEE Std 603. In particular, Table 2.2.15-2, provides DAC/ITAAC for verifying that the capability for testing and calibration have been met for IEEE Std 603, Sections 5.7 and 6.5. DCD, Tier 1, Table 2.2.15-2 also includes DAC/ITAAC for applicable sections of IEEE Std 603, Section 4 for verifying that complete design basis information is identified and implemented for ESF actuation and control systems, VBIF, and ICS DPVIF related software projects. Accordingly, based on the applicant's identification of design bases for the ESF actuation and control systems, VBIF, ICS DPVIF, and all subsystems, conformance to applicable guidance and IEEE Std 603 sections, and their verification in the DAC/ITAAC, the NRC staff finds that the requirements of GDC 21 has been adequately addressed.

GDC 22 requires, in the pertinent part, that protection systems 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. The NRC staff evaluated whether GDC 22 has been adequately addressed for the ESF actuation and control systems, VBIF, ICS DPVIF, and all subsystems. SRP Appendix 7.1-A states that GDC 22 is addressed for protection systems by conformance to IEEE Std 603, Sections 4, 5.1, 5.3, 5.4, 5.5, 5.6, 6.2, 6.3, 6.8, 7.2, and 8. In addition, SRP Section 7.3 identifies that GDC 22 is addressed by conformance to RG 1.75. DCD, Tier 2, Table 7.1-1, identifies that GDC 22 and RG 1.75 apply to the ESF actuation and control systems, VBIF, ICS DPVIF, and all subsystems. DCD, Tier 2, Section 7.3, describes the conformance of ESF actuation and control systems, VBIF, ICS DPVIF, and all subsystems to IEEE Std 603, which is evaluated in Section 7.3.3.1 of this report. Table 2.2.15-2 includes the DAC/ITAAC for verifying that the ESF actuation and control systems, VBIF, ICS DPVIF, and all subsystems design is completed in compliance with IEEE Std 603. In particular, DCD, Tier 1, Table 2.2.15-2, provides DAC/ITAAC for IEEE Std 603, Section 5.6. DCD, Tier 1, Table 2.2.15-2 also includes DAC/ITAAC for applicable sections of IEEE Std 603, Section 4 for verifying that complete design basis information is identified and implemented for ESF actuation and control systems and VBIF ICS DPVIF, related software projects. Accordingly, based on the applicant's identification of design bases for the ESF actuation and control systems, VBIF, ICS DPVIF, and all subsystems, conformance to applicable guidance and IEEE Std 603 sections, and their verification in the DAC/ITAAC, the NRC staff finds that the requirements of GDC 22 has been adequately addressed.

GDC 23 requires that protection systems be designed to fail into a safe state or into a state demonstrated to be acceptable on some other defined basis, if certain conditions are experienced. The NRC staff evaluated whether GDC 23 has been adequately addressed for the ESF actuation and control systems, VBIF, ICS DPVIF, and all subsystems. Appendix 7.1-A to the SRP states that GDC 23 is addressed for ESF actuation and control systems, VBIF, ICS DPVIF, and all subsystems by conformance to IEEE Std 603, Section 5.5. DCD, Tier 2, Table 7.1-1, identifies that GDC 23 applies to the ESF actuation and control systems, VBIF, ICS DPVIF, and all subsystems. DCD, Tier 2, Section 7.1.6.6.1.6, states that the SSLC/ESF fails to a state where the activated component remains "as-is" to prevent a control-system-induced LOCA. For the same reason, hardware and software failures detected by self-diagnostics do not initiate a signal in a failed SSLC/ESF division. DCD, Tier 1, Table 2.2.15-2 and Section 3.2, provide DAC/ITAAC and Section 3.8 provides ITAAC for verifying that the ESF actuation and control systems, VBIF, and ICS DPVIF design was completed in compliance with IEEE Std 603, Section 5.5. Accordingly, based on the conformance to the applicable guidance and IEEE Std 603 sections and their verification in the DCD Tier 1, DAC/ITAAC, the NRC staff finds that the requirements of GDC 23 have been adequately addressed.

GDC 24 requires that the protection system 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. GDC 24 requires that the interconnection of the protection and control systems be limited so as to assure that safety is not significantly impaired. The NRC staff evaluated whether GDC 24 has been adequately addressed for the ESF actuation and control systems, VBIF, ICS DPVIF, and all subsystems. SRP Appendix 7.1-A states that GDC 24 is addressed for protection systems by conformance to IEEE Std 603, Sections 5.1, 5.6, 5.12, 6.3, 6.6, and 8, particularly Sections 5.6 and 6.3. DCD, Tier 2, Section 7.3, describes the conformance of the ESF actuation and control systems, VBIF, ICS DPVIF, and all subsystems to IEEE Std 603, Sections 5.6 and 6.3, which are evaluated in Section 7.3.3.1 of this report. Table 2.2.15-2 includes the DAC/ITAAC for verifying that the applicable I&C systems design is completed in compliance with IEEE Std 603, including Sections 5.6 and 6.3. Accordingly, based on the applicant's identification of design bases for the ESF actuation and control systems, VBIF, ICS DPVIF, and all subsystems, conformance to applicable IEEE Std 603 sections, and their verification in the DAC/ITAAC, the NRC staff finds that the requirements of GDC 24 has been adequately addressed.

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. The NRC staff evaluated whether GDC 29 has been adequately addressed for the ESF actuation and control systems, VBIF, ICS DPVIF, and all subsystems. SRP Appendix 7.1-A states that GDC 29 is addressed by conformance as applicable to GDC 20-25 and GDC 28. However, GDC 25, which applies to protection systems requirements for reactivity control malfunctions, and GDC 28 which applies to reactivity control systems, are not applicable to the ESF actuation and control systems evaluated in this section. Accordingly, GDC 29 is addressed by conformance as applicable to GDC 20–24. In DCD, Tier 1, Sections 2.2.15, 3.2, 3.3, and 3.8 include the DAC/ITAAC for the applicant to verify that the applicable protection and control systems designs implement these design criteria. Accordingly, based on the applicant's identification of design bases for the ESF actuation and control systems, VBIF, ICS DPVIF, and all subsystems, conformance to applicable guidance and IEEE Std 603 sections, and their verification in the DAC/ITAAC, the NRC staff finds that the requirements of GDC 29 has been adequately addressed.

The NRC staff evaluated whether GDC 33, 34, 35, and 38 have been adequately addressed. According to SRP Appendix 7.1-A, GDC 33 imposes functional requirements on ESF I&C systems provided to initiate, control, and protect the integrity of reactor coolant makeup systems for protection against small breaks in the RCPB. GDC 33 also requires that necessary I&C systems are operable using either onsite or offsite power (assuming only one source is available). DCD, Tier 2, Section 3.1.4.4, identifies that the ICS, ADS, and GDCS provide the reactor coolant makeup functions for the ESBWR to meet the requirements of GDC 33. The ICS is described in DCD, Tier 2, Section 5.4.6, and the ADS and GDCS are described in DCD, Tier 2, Section 6.3. The staff reviewed the descriptions of their control systems in DCD, Tier 2, Section 7.4.4 for the ICS and Section 7.3.1 for the ADS and GDCS and confirmed that these sections identify the corresponding reactor coolant makeup initiation, control, and protection functions. Based on the review of documentation in the above DCD Tier 2 sections, the staff finds that the ESBWR design has provided functions, performance, and reliability necessary to initiate and control the reactor coolant makeup system. Therefore, the safety functions described in GDC 33 are met.

According to SRP Appendix 7.1-A, GDC 34 imposes functional requirements on ESF systems provided to initiate, control, and protect the integrity of residual heat removal systems. GDC 34 also requires that necessary I&C systems are operable using either onsite or offsite power (assuming only one source is available). DCD, Tier 2, Section 3.1.4.5, identifies that the ICS provides the residual heat removal functions for the ESBWR to meet the requirements of GDC 34. The ICS is described in DCD, Tier 2, Section 5.4.6. The staff reviewed the descriptions of its control system in DCD, Tier 2, Section 7.4.4, and confirmed that this section identifies the corresponding residual heat removal initiation, control, and protection functions. Based on the review of documentation in the above DCD Tier 2 sections, the staff finds that the ESBWR design has provided functions, performance, and reliability necessary to initiate and control the residual heat removal system. Therefore, the safety functions described in GDC 34 are met.

According to SRP Appendix 7.1-A, GDC 35 imposes functional requirements on ESF systems provided to initiate, control, and protect the integrity of the ECCS. GDC 35 also requires that necessary I&C systems are operable using either onsite or offsite power (assuming only one source is available). DCD, Tier 2, Section 3.1.4.6, identifies that the ECCS, including the ICS, SLC system, GDCS, and ADS provides the ECCS functions for the ESBWR to meet the requirements of GDC 35. The ECCS, including the ICS, SLC system, GDCS, and ADS, is described in DCD, Tier 2, Section 6.3. The staff reviewed the descriptions of its control system in DCD, Tier 2, Section 7.3.1 (ADS and GDCS), and confirmed that this section identifies the corresponding ESF-related ECCS initiation, control, and protection functions. Based on the review of documentation in the above DCD Tier 2 sections, the staff finds that the ESBWR design has provided functions, performance, and reliability necessary to initiate and control the ESF systems. Therefore, the safety functions described in GDC 35 are met.

According to SRP Appendix 7.1-A, GDC 38 imposes functional requirements on ESF I&C systems provided to initiate, control, and protect the integrity of containment heat removal systems. GDC 38 also requires that necessary I&C systems are operable using either onsite or offsite power (assuming only one source is available). DCD, Tier 2, Section 3.1.4.9, identifies that the PCCS provides the containment heat removal functions for the ESBWR to meet the requirements of GDC 38. DCD, Tier 2, Section 3.1.4.9, also identifies that while the PCCS has no controls, the ICS provides control functions for the PCCS to fulfill its safety functions. The staff reviewed the descriptions of ICS control system in DCD, Tier 2, Section 7.4.4,3 and confirmed that this section has provided necessary containment heat removal, initiation, control, and protection functions to address GDC 38 in the design bases of the ICS. Based on the review of documentation in the above DCD, Tier 2, Section 7.4.4.3, the staff finds that the ESBWR design has provided functions, performance, and reliability necessary to initiate and control the containment heat removal system. Therefore, the safety functions described in GDC 38 are met.

In addition, SRP Section 7.3 states that GDC 33, GDC 34, GDC 35, and GDC 38 are addressed by conformance to requirements for testability, operability with onsite and offsite electrical power, and single failures. The single failure and testability requirements correspond to IEEE Std 603. Sections 5.1, 5.7, and 6.5. The NRC staff evaluated conformance of the GDCS and ADS to IEEE Std 603, Sections 5.1, 5.7, and 6.5 in Section 7.3.3.1 of this report and found it acceptable. The NRC staff evaluated conformance of the ICS to IEEE Std 603, Sections 5.1, 5.7, and 6.5 in Section 7.4.3.1 of this report and found it acceptable. In DCD, Tier 1, Sections 2.2.15, 3.2, 3.3, and 3.8 include the DAC/ITAAC for the applicant to verify that the ICS, ADS, and GDCS designs implement these design bases and conform to IEEE Std 603. For operability with onsite and offsite electrical power, DCD, Tier 2, Section 8.1.3, notes that the Q-DCIS, which includes the ICS, ADS, and GDCS, is normally powered by the safety 120-VAC

power distribution system or, if power is lost, by safety batteries for 72 hours. Therefore, these systems are operable using either onsite or offsite power (assuming only one source is available). The safety 120-VAC power distribution system and batteries are evaluated in Chapter 8 of this report. Accordingly, based on the applicant's identification of the necessary reactor coolant makeup, residual heat removal, ECCS, and containment heat removal initiation, control, and protection functions in the design bases of the ICS, ADS, and GDCS, and their verification in the DCD Tier 1, DAC/ITAAC, the NRC staff finds that the requirements of GDC 33, GDC 34, GDC 35 and GDC 38 have been adequately addressed.

As described in section 7.1.1.3.6 of this report, the NRC staff finds that GDC 41 and 44 are not applicable to the I&C design.

The NRC staff evaluation of the I&C system conformance to the SRM on SECY-93-087, is documented in Section 7.1.1.3.7 of this report. This evaluation includes the ESF actuation and control systems, VBIF, ICS DPVIF, and all subsystems. Accordingly, the NRC staff finds that the guidelines of SRM on SECY-93-87 have been adequately addressed for the ESF actuation and control systems, VBIF, and all subsystems.

The NRC staff evaluated whether 10 CFR 50.34(f)(2)(v), (f)(2)(xii), and (f)(2)(xiv) have been adequately addressed. As described in Section 7.1.1.3.4 of this report, the NRC staff evaluated the I&C system design's compliance with 10 CFR 50.34(f)(2)(v), (f)(2)(xii), and (f)(2)(xiv). Accordingly, the NRC staff found that 10 CFR 50.34(f)(2)(v), (f)(2)(xii), and (f)(2)(xiv) have been adequately addressed for the ESF actuation and control systems, VBIF, and all subsystems.

The NRC staff evaluated whether 10 CFR 50.55a(h) has been adequately addressed for the ESF actuation and control systems, VBIF, ICS DPVIF, and all subsystems. 10 CFR 50.55a(h) requires compliance with IEEE Std 603-1991 and the correction sheet dated January 30, 1995, which is evaluated in Section 7.3.3.1 and 7.2.3.2 of this report and are found to be adequately addressed. Accordingly, the NRC staff finds that 10 CFR 50.55a(h) has been adequately addressed for the ESF actuation and control systems, VBIF, ICS DPVIF, and all subsystems.

The NRC staff evaluated whether the requirements of 10 CFR 52.47(b)(1) have been met. This regulation requires that the application (for design certification) contain proposed ITAAC that are necessary and sufficient to provide reasonable assurance that, if the ITA are performed and the acceptance criteria are met, a plant that references the design certification has been constructed and will operate in accordance with the design certification, the Atomic Energy Act, and the Commission's rules and regulations. The ITAAC specific to the ESF actuation and control systems, VBIF, ICS DPVIF, and all subsystems are addressed throughout section 7.2.3 of this report. The NRC staff evaluation of conformance to 10 CFR 52.47 in Section 7.1.1.3.4 of this report is applicable to the ESF actuation and control systems, VBIF, ICS DPVIF, and all subsystems. Therefore, the NRC staff finds that the requirements of 10 CFR 52.47(b)(1) have been adequately addressed for the ESF actuation and control systems, VBIF, ICS DPVIF, and all subsystems.

7.3.4 Conclusion

Based on the above, the NRC staff concludes that the applicant adequately addresses the major design considerations for the ESF actuation and control systems, VBIF, and ICS DPVIF. As discussed in Sections 7.1.1.3.1 through 7.1.1.3.10 of this report and Section 7.3.3 above, the NRC staff concludes for the ESF actuation and control systems, VBIF, and ICS DPVIF, the applicant adequately addresses the relevant requirements of 10 CFR 50.55a(a)(1),

10 CFR 50.55a(h), 10 CFR 50.34(f), 10 CFR 52.47(b)(1), GDC 1, 2, 4, 10, 13, 15, 16, 19-24, 29, 33, 34, 35 and 38; and the guidelines of SRM on SECY-93-087. The applicant has also identified adequate high-level functions and included sufficient DAC/ITAAC in Tier 1 to verify that ESF design is completed in compliance with the applicable requirements. The staff also concludes that the requirements of GDC 41 and 44 are not applicable to the ESBWR I&C design.

7.4 Safe Shutdown Systems

7.4.1 Regulatory Criteria

The objective of the review of DCD, Tier 1, Section 2.2, and DCD, Tier 2, Section 7.4, is to confirm that the safe shutdown systems satisfy the requirements of the acceptance criteria and guidelines applicable to safety systems and that they will meet their safety regulatory acceptance criteria, guidelines, and performance requirements. 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. During safe shutdown, reactivity control systems must maintain a subcritical condition of the core, and residual heat removal systems must operate to maintain adequate cooling of the core.

SRP acceptance criteria for the safety safe shutdown systems are based on meeting the relevant requirements of 10 CFR 50.55a(a)(1); 10 CFR 50.55a(h); GDC 1, 2, 4, 13, 19, 24, 34, 35, and 38; and 10 CFR 52.47(b)(1). The SRP acceptance criteria are also based on conforming to the guidelines of IEEE Std 7-4.3.2, as endorsed by RG 1.152.

SRP acceptance criteria for the non-safety safe shutdown systems are based on the relevant requirements of 10 CFR 50.55a(h) and IEEE Std 603, Sections 5.6.3 and 6.3.

7.4.2 Summary of Technical Information

The safe shutdown systems are those I&C systems used to achieve and maintain a safe-shutdown condition of the plant. The safety systems ICS and SLC use natural circulation in the performance of their shutdown functions. I&C design in these systems are part of the Q-DCIS which conforms to the safety criteria (IEEE Std 603). The two safety RSS panels use manual and the DCIS indication and controls. These two panels are located outside the MCR and are separate from each other. In addition to safety systems, some non-safety systems are used to perform cold shutdown functions. I&C design in these systems is part of the N-DCIS. For those N-DCIS systems, provision of redundant trains and single failure protection are implemented.

DCD, Tier 2, Section 7.4, describes the safe shutdown systems. The safe shutdown systems for the design include the following:

- SLC
- RSS
- RWCU/SDC
- ICS
- HP CRD isolation bypass function

7.4.2.1 Standby Liquid Control System

The SLC system, an ECCS, provides (1) a diverse, backup means to shut down the reactor from full power to subcritical condition, using soluble boron injection, and maintain the reactor subcritical while the reactor is brought to a cold shutdown condition, and (2) system actuation upon receipt of manual and automatic initiation signals in response to either ATWS events or DBEs requiring ECCS operation.

The SLC system contains two identical and separate trains. Each train provides 50-percent injection capacity. The SLC also includes a non-safety nitrogen charging subsystem that includes a liquid nitrogen tank, vaporizer, and high pressure pump for initial accumulator charging and makeup for the normal system losses during normal plant operation.

Four divisions of safety sense and command logic are used for automatic SLC initiation and for automatic SLC accumulator isolation. Redundant SLC accumulator level and pressure instrumentation is provided to monitor system performance. Valve position indication and continuity monitoring of the SLC squib injection valves are provided in the MCR. Safety SLC components are designed for the environmental conditions applicable to their location. Safety SLC components are also designed to preclude adverse interaction from the non-safety portion of the system.

The SLC is initiated automatically as part of the ECCS to provide mitigation for LOCA events. The SLC receives an actuation command following a confirmed LOCA signal plus a 50-second time delay after a sustained RPV Level 1 signal for 10 seconds. The SLC also receives a diverse ECCS initiation signal from the DPS.

The SLC also starts automatically on an ATWS mitigation signal persisting for 180 seconds. The ATWS mitigation logic performs the diverse emergency shutdown function. The ATWS/SLC logic uses sensors, hardware, and software platforms diverse from the SSLC/ESF, the RPS, and the DPS hardware/software platforms.

To avoid boron dilution during SLC operation, the SLC system logic transmits an isolation signal to the RWCU/SDC via the LD&IS. To avoid the injection of nitrogen into the RPV system, four divisional, safety level sensors per SLC accumulator are used to provide automatic isolation of series accumulator shutoff valves on (a voted 2/4) low accumulator level. The SLC system processors of the ATWS/SLC independent control logic platform perform the shutoff valve isolation logic. Accumulator temperature, solution level, and accumulator pressure are indicated locally inside the accumulator room. Boron injection and shutoff valve position status is provided in the MCR.

7.4.2.2 Remote Shutdown System

The safety RSS provides operators with the means to safely shut down the reactor from a place outside the MCR if it becomes uninhabitable. The RSS provides remote control of the systems needed to bring the reactor to a hot shutdown after a scram. The RSS also provides the subsequent capability to bring the plant to (and maintain) a cold shutdown condition.

The RSS has two redundant and independent panels. All parameters displayed and/or controlled from Division 1 and Division 2 in the MCR also are displayed and/or can be controlled from any of the two RSS panels. Each panel contains the following:

- Division 1 manual scram switch
- Division 2 manual scram switch
- Division 1 manual MSIV isolation switch
- Division 2 manual MSIV isolation switch
- Division 1 safety VDUs
- Division 2 safety VDUs
- PIP A non-safety VDUs
- PIP B non-safety VDUs
- Non-safety communications equipment

All data from the Q-DCIS and the N-DCIS networks are available for display on the RSS panels. Because the VDUs on the RSS panels are connected to the Q-DCIS or the N-DCIS through the same networks serving corresponding VDUs at the MCR, all Division 1 and 2 safety and Non-safety display/control functions at the MCR also are available at the RSS panels.

The two RSS panels are located in different rooms inside the reactor building. Each RSS panel room has a sliding fire door with a minimum fire rating of 3 hours. The RSS panel room environment is typically similar to the MCR environment. Access to and use of the RSS panels are administratively controlled.

The RSS provides sufficient redundancy in its control and monitoring capability, to accommodate a single failure in the interfacing systems, a single failure in the RSS controls, and the event that caused the MCR evacuation. The RSS is designed such that any failure within it does not degrade the capability of interfacing safety systems.

7.4.2.3 Reactor Water Cleanup/Shutdown Cooling System

The RWCU/SDC is a non-safety system that provides cooling for the reactor to reach cold shutdown condition. There are two redundant RWCU/SDC trains. The loss of one complete RWCU/SDC train could extend the time needed for the reactor to reach cold shutdown condition. The RWCU/SDC system is one of the dual-redundant PIP systems whose instrumentation belongs to the N-DCIS.

The RWCU/SDC system performs three basic plant functions—(1) it provides a continuous purifying treatment of the reactor coolant during startup, normal operation, cooldown, hot standby, and shutdown modes of plant operation, (2) it removes core decay heat in conjunction with the main condenser or the isolation condensers during plant shutdown modes, and (3) it (with the feedwater system) provides reactor coolant heatup during cold startup. The I&C of the RWCU/SDC system maintains the process conditions within the limits necessary to control the system and satisfy its design bases.

7.4.2.4 Isolation Condenser System

The ICS removes core decay heat from the reactor following any of the following events:

- Station blackout
- ATWS event
- Loss-of-coolant-accident (LOCA)

The ICS is capable of passive decay heat removal and achieving and maintaining safe stable conditions for at least 72 hours without operator action following non-LOCA events. Operator action is credited after 72 hours to refill isolation condenser pools or initiate non-safety shutdown cooling.

The ICS is one of the ESF systems whose instrumentation belongs to the Q-DCIS. The ICS consists of four independent trains, each containing an isolation condenser that condenses steam on the tube side and transfers heat to the IC/PCCS pool, which is vented to the atmosphere. The isolation condenser, connected by piping to the RPV, is placed at an elevation above the source of steam (vessel), and when the steam is condensed, the condensate is returned to the vessel via a condensate return pipe. The steam side connection between the vessel and the isolation condenser is normally open, and the condensate line is normally closed. This allows the isolation condenser and drain piping to fill with condensate, which is maintained at a subcooled temperature by the pool water during normal reactor operation. The isolation condenser is started into operation by opening condensate return valves and draining the condensate to the reactor, thus causing steam from the reactor to fill the tubes which transfer heat to the cooler pool water.

The ICS is designed to operate from safety power sources. The system instrumentation is powered by four divisionally separated sources of safety power. The ICS uses 2/4 logic for automatic operation or isolation of each of the four separate isolation condenser trains. The actuating logic and actuator power for the inner isolation valves for the four ICS trains are on two safety 120-VAC divisional power sources different from the two divisional power sources for the outer isolation valves.

Each of the four ICS trains has three of the four safety power sources. Consequently, the loss of 2/4 safety power supplies does not result in the loss of any one ICS train. However, second and third sources of safety power are provided to operate the ICS automatic venting system during long-term ICS operation; otherwise, the manually controlled backup venting system, which uses one of the divisional power sources starting the ICS, can be used for long-term operation. If the three safety power supplies used to start an individual ICS train fail, then the isolation condenser would automatically start, because of the “fail open” actuation of the condensate return bypass valves upon loss of electrical power to the solenoids controlling its nitrogen-actuated valves.

The ICS receives an actuation command following a confirmed LOCA signal after a time delay corresponding to the first depressurization valve actuation.

The ICS starts operating automatically upon high reactor pressure, low reactor water level (Level 2) with time delay, low reactor water level (Level 1), loss of power generation buses, loss of feedwater flow in reactor run mode, or MSIV position indication (indicating closure) whenever the reactor mode switch is in the run position. Each ICS train also can be manually initiated, and so the operator is able to stop any individual ICS train whenever the RPV pressure is below a reset value override to the ICS automatic actuation signal following MSIV closure.

The residual heat removal function of the safety ICS is further backed up by the safety ESF combination of ADS, PCCS, and GDCS; by the non-safety RWCU/SDC loops; or by the makeup function of the CRD system operating in conjunction with SRVs and the suppression pool cooling system (SPCS). The DPS provides diverse non-safety signals for ICS actuation and other ICS functions.

7.4.2.5 High Pressure Control Rod Drive Isolation Bypass Function

The control rod drive hydraulic subsystem supplies high pressure makeup water to the reactor vessel in response to a low RPV water level (Level 2) condition, or in the event GDCS fails to inject following a LOCA. The HP CRD isolation bypass function is designed to mitigate the beyond design basis failure of the GDCS to inject following a LOCA. The HP CRD Isolation Bypass Function has the following requirements and 10 CFR 50.2 Design Basis:

- Using safety logic inputs, the normally closed HP CRD isolation bypass valves are opened automatically on failure of GDCS to inject water in to the reactor.
- Non-safety manual control of the HP CRD isolation bypass valve is provided and isolation bypass valve positions are displayed in the MCR.
- Divisional instrumentation performing the HP CRD isolation bypass function logic is powered by the associated safety divisional power supply.
- Bypass of a division of sensors is annunciated in the MCR.
- The HP CRD isolation bypass function logic executed in the ICP and is independent and diverse from SSLC/ESF.

7.4.3 NRC Staff Evaluation

The NRC staff reviewed the safe shutdown systems in accordance with SRP Section 7.4. The NRC staff also used acceptance criteria in SRP Section 7.1, SRP Table 7-1, SRP Appendix 7.1-A, and SRP Appendix 7.1-C, as directed by SRP Section 7.4. The acceptance criteria listing used as the basis for the NRC staff's review of the safe shutdown systems is described in Section 7.4.1 of this report.

SRP Section 7.1 describes the procedures to be followed in reviewing any I&C system. SRP Section 7.4 highlights specific topics that should be emphasized in reviewing the safe shutdown systems and the specific topics are addressed in Section 7.4.3.1 of this report. The NRC staff included the review of the DAC/ITAAC during the review of this section because of the significant role of the DAC/ITAAC in determining the conformance of safe shutdown systems to all requirements. GDC 44 requires a system to transfer heat from structures, systems, and components important to safety, to an ultimate heat sink. According to SRP Appendix 7.1-A, GDC 44 imposes functional requirements on the safe shutdown systems.

As described in Section 7.1.1.3.1 of this report, the DCD does not provide the required safe shutdown systems design information to comply with IEEE Std 603. Instead, the applicant has included the DAC/ITAAC in DCD, Tier 1, Section 2.2.15, to confirm that the completed safe shutdown systems design complies with IEEE Std 603. DCD, Tier 1, Section 2.2.15, also includes an ITAAC applicability table (Table 2.2.15-1), which identifies the applicability of the IEEE Std 603 criteria DAC/ITAAC to the safe shutdown systems. The NRC staff has accepted the DAC approach to addressing compliance with IEEE Std 603. The NRC staff evaluation of conformance to IEEE Std 603 in Section 7.1.1.3.10 of this report is applicable to the safe shutdown systems.

In RAI 7.1-99, the NRC staff asked the applicant to clarify the applicability of IEEE Std 603 criteria in a consistent manner throughout DCD, Tier 2, Chapter 7. By letter MFN 09-089, dated February 19, 2009, the applicant submitted a response to RAI 7.1-99, along with responses to 7.1-100, 7.1-101, and 14.3-265, Supplement 1, all of which are incorporated in DCD Revision 6. Section 7.1.1.3.1 of this report provides additional discussion of these RAI responses. With regard to the NRC staff evaluation of the safe shutdown systems, the applicant significantly revised DCD, Tier 2, Tables 7.1-1 and 7.1-2 to clearly identify applicability of IEEE Std 603 criteria for each safe shutdown system. Concurrently, many references to IEEE Std 603 criteria were revised or removed from the discussions of safe shutdown systems in DCD, Tier 2, Section 7.4 to address the consistency concerns. Accordingly, statements regarding applicability of IEEE Std 603 criteria provided in the NRC staff SER with open items have been updated or removed from the remainder of Section 7.4.3 of this report to be consistent with DCD Revision 6.

7.4.3.1 Evaluation of Safe-Shutdown Systems Conformance with Acceptance Criteria - Major Design Considerations

Per SRP Section 7.4, the following are the major design considerations that should be emphasized in the safe shutdown systems review:

(1) Independence (IEEE Std 603, Sections 5.6 and 6.3)

The NRC staff evaluated whether Sections 5.6 and 6.3 of IEEE Std 603 have been adequately addressed for the safe shutdown systems. These criteria are evaluated in Section 7.1.1.3.10 of this report, where the NRC staff finds that Sections 5.6 and 6.3 are adequately addressed based on their inclusion in the safety systems design basis and their verification in the DCD, Tier 1, Section 2.2.15, DAC/ITAAC. This evaluation is applicable to the safe shutdown systems. Also, DCD, Tier 1, Table 2.2.15-1, identifies that Sections 5.6 and 6.3 of IEEE Std 603 are applicable to the SLC, ICS, and HP CRD IBF that make up the applicable safe shutdown systems. Accordingly, based on the inclusion of IEEE Std 603, Sections 5.6 and 6.3, in the applicable safe shutdown systems design basis and their verification in the DCD Tier 1, DAC/ITAAC, the NRC staff finds that IEEE Std 603, Sections 5.6 and 6.3, are adequately addressed for the safe shutdown systems.

(2) Use of Digital Systems (IEEE Std 7-4.3.2)

The NRC staff evaluated whether IEEE Std 7-4.3.2, as endorsed by RG 1.152, has been adequately addressed for the safe shutdown systems. SRP Appendix 7.1-D provides guidance on the implementation of IEEE Std 7-4.3.2 concerning the use of digital systems. In Section 7.1.1.3.10 of this report, the NRC staff evaluated in parallel IEEE Std 7-4.3.2 and IEEE Std 603 using the guidance in Appendix 7.1-D to the SRP. The NRC staff evaluation of conformance to IEEE Std 7-4.3.2 in Section 7.1.1.3.10 of this report is applicable to the safe shutdown systems.

The software development activities are described in NEDE-33226P and NEDE-33245P. DCD, Tier 1, Section 3.2, includes the DAC/ITAAC to confirm that the completion of these activities and products conforms to the processes described in NEDE-33226P and NEDE-33245P and the guidelines of BTP HCIB-14. The NRC staff evaluation of the software development activities is provided in Section 7.1.2 of this report. Accordingly, the NRC staff finds that use of digital systems is adequately addressed for the applicable safe shutdown systems.

(3) Periodic Testing (IEEE Std 603, Sections 5.7 and 6.5)

The NRC staff evaluated whether conformance with IEEE Std 603, Sections 5.7 and 6.5, has been adequately addressed for the safe shutdown systems. These criteria are evaluated in Section 7.1.1.3.10 of this report, where the NRC staff finds that Sections 5.7 and 6.5 are adequately addressed based on their inclusion in the safety systems design basis and their verification in the DCD, Tier 1, Section 2.2.15, DAC/ITAAC. DCD, Tier 1, Table 2.2.15-1, identifies that Sections 5.7 and 6.5 of IEEE Std 603 are applicable to the SLC, , ICS, and HP CRD IBF that make up the applicable safe shutdown systems. Accordingly, based on the inclusion of IEEE Std 603, Sections 5.7 and 6.5, in the applicable safe shutdown systems design basis and their verification in the DCD Tier 1, DAC/ITAAC, the NRC staff finds that IEEE Std 603, Sections 5.7 and 6.5, are adequately addressed for the safe shutdown systems.

(4) Remote Shutdown Capability

Shutdown remote from the MCR is not an event analyzed in the accident analysis in DCD, Tier 2, Chapter 15. Specific scenarios have not been identified for which the adequacy of shutdown capability from the RSS is evaluated. However, smoke resulting from a fire in the MCR has long been recognized as the event that could force the evacuation of the MCR and result in a need to shut down the reactor remotely from the MCR. RG 1.189, establishes the bases for safe shutdown with respect to fire protection. On the basis of DCD, Tier 2, Sections 15.5.6.2 and 15.5.6.3, which provide the assumptions and results of safe shutdown fire analysis, only a manual scram of the plant from the MCR is required to reach and maintain Mode 3 (hot shutdown).

The NRC staff evaluated whether the design provides for control in locations remote from the MCR that may be used for manual control and alignment of the safe shutdown system equipment needed to achieve and maintain hot and cold shutdown. The NRC staff also evaluated whether this control equipment is capable of operating independently of (i.e., without interaction with) the equipment in the MCR.

DCD, Tier 2, Section 7.4, states that the RSS is a safety system used to provide operators with the means to safely shut down the reactor from a place outside the MCR if the MCR becomes uninhabitable. RSS provides remote control of the systems that are needed to bring the reactor to a hot shutdown condition after a scram. RSS also provides the subsequent capability to bring the plant to and maintain the reactor plant in a cold shutdown condition. The NRC staff finds this acceptable.

The NRC staff evaluated whether the design of the RSS provides appropriate displays so that the operator can monitor the status of the shutdown. SRP Section 7.4 states that typical RSS displays include reactor vessel water level and pressure, suppression pool level and temperature, isolation condenser level indication for tanks involved in shutdown, and shutdown system diagnostic instrumentation.

DCD, Tier 2, Section 7.4, states that the RSS has two redundant and independent panels. All parameters that are displayed and/or controlled from Division 1 and Division 2 in the MCR are also displayed and/or can be controlled from any of the two RSS panels.

The NRC staff evaluated whether the remote shutdown capability is capable of accommodating expected plant response following a reactor trip, including protective system actions that could occur as a result of plant cooldown. DCD, Tier 2, Section 7.4.2.3, states, “The RSS provides

instrumentation and controls (I&C) outside the MCR to allow prompt hot shutdown of the reactor after a scram and to maintain safe conditions during hot shutdown. It also provides capability for subsequent cold shutdown of the reactor through the use of suitable operating procedures." The NRC staff finds this acceptable.

The NRC staff evaluated whether access to RSSs is under administrative controls. DCD, Tier 2, Section 7.4.2.2.1, states, "Access to and use of the RSS panels is administratively controlled." The NRC staff finds this acceptable.

The NRC staff evaluated whether the equipment in the RSSs is designed to the same standards as the corresponding equipment in the MCR. DCD, Tier 2, Section 7.4.2.3, states, "The RSS is classified as a safety system that can control safety systems or equipment," and Section 7.4.2.2.1 states, "All parameters displayed and/or controlled from Division 1 and Division 2 in the MCR also are displayed and/or can be controlled from any of the two RSS panels." The NRC staff finds this acceptable.

The NRC staff evaluated whether the RSS-control transfer devices should be located remote from the MCR and whether their use should initiate an alarm in the control room. DCD, Tier 2, Section 7.4.2.2.3, states, "When evacuation of the MCR is necessary, the reactor is manually scrammed. If there has been no loss of off-site power, the turbine bypass valves automatically control reactor pressure, and the reactor feedwater system automatically maintains RPV water level. These functions will remain operable because the safety and non-safety controllers are not located in the same fire area as the MCR nor are they affected by the adverse impacts on the MCR VDUs and switches after an MCR evacuation; as a result, reactor cooldown is achieved through the normal heat sinks. However, if the reactor feedwater system is not available due to loss of off-site power, control of the CRD system from the RSS may be utilized. Control of the high pressure makeup injection capability of the CRD system ensures that the RPV water level remains above the ADS trip setpoint and above the elevation of the RWCU/SDC mid-vessel suction line nozzle. The ICS automatically controls reactor pressure. ICS operation is not affected by an MCR evacuation. With the ICS in operation, the isolation condensers provide initial decay heat removal, and further reactor cooldown is achieved from the RSS panels using the RWCU/SDC." Therefore, no remote transfer devices are necessary for the design. The NRC staff finds this acceptable.

The NRC staff evaluated whether the location is consistent with the procedures for remote, alternative, and dedicated shutdown, as appropriate. DCD, Tier 2, Section 7.4.2.2.1, states, "The two RSS panels are located in different rooms inside the Reactor Building (RB). Each RSS Panel room has a sliding fire door with a minimum fire rating of three hours. The RSS panel room environment typically is similar to the MCR environment." The NRC staff finds this acceptable.

The NRC staff evaluated whether, in cases where the control functions are transferred between the control room and the RSS, the design maintains parameter indications such that the operators at the control room and the RSS both have access to the same parameters that are being relied upon. DCD, Tier 2, Section 7.4.2.2.1, states, "All parameters displayed and/or controlled from Division 1 and Division 2 in the MCR also are displayed and/or can be controlled from any of the two RSS panels." Therefore, transfer of control functions is not necessary for the design. The NRC staff finds this acceptable.

If the MCR evacuation is necessary, the remote shutdown panels provide complete redundancy in terms of control and monitoring for safe-shutdown functions. The transfer of operation from

the MCR to the remote shutdown panel is not required since the remote shutdown panels are designed to have all the functions available at the MCR. The MCR is located in the control building, and remote shutdown panels are located in separate fire areas in the reactor building. The MCR has its own dedicated ventilation system, and the remote shutdown panel area ventilation system will be using the reactor building ventilation system. The safety and non-safety electrical cabinets are located in the separate DCIS rooms, which are in different fire areas. Communications between the MCR, remote shutdown panels, and these DCIS rooms use fiber optic cables. The HFE process ultimately decides the hard-wired controls in the MCR or in the RSS.

In DCD, Tier 1, Section 2.2.6, the applicant documented the RSS design requirements and the ITAAC for the RSS. The RSS is a safety, seismic Category I system. The RSS has two redundant, independent panels, and panels are located in two separate rooms in different divisional quadrants of the reactor building. Safety systems in each RSS panel receive power from divisionally separate safety power supplies; non-safety systems in each RSS panel receive power from non-safety power supplies. Based on the design described in DCD, Tier 2, Section 7.4.2, and DCD, Tier 1, Section 2.2.6, the NRC staff finds the I&C design for RSS acceptable.

(5) Safe Shutdown

The NRC staff evaluated whether the single failure criterion, IEEE Std 603, Section 5.1, has been adequately addressed for the safe shutdown systems. IEEE Std 603, Section 5.1 is evaluated in Section 7.1.1.3.10 of this report, where the NRC staff finds that Section 5.1 is adequately addressed based on its inclusion in the safety systems design basis and their verification in the DCD, Tier 1, Section 2.2.15, DAC/ITAAC. DCD, Tier 1, Table 2.2.15-1, identifies that Section 5.1 of IEEE Std 603 is applicable to the SLC, ICS, and HP CRD IBF that make up the applicable safe shutdown systems. Accordingly, based on the inclusion of IEEE Std 603, Section 5.1 in the applicable safe shutdown systems design basis and its verification in the DCD Tier 1, DAC/ITAAC, the NRC staff finds that IEEE Std 603, Section 5.1 is adequately addressed for the safe shutdown systems.

The NRC staff evaluated whether the safe shutdown systems provide the required capacity and reliability to perform intended safety functions on demand in conformance with IEEE Std 603, Section 5. IEEE Std 603, Section 5, was previously evaluated in Section 7.1.1.3.10 of this report and found acceptable. The NRC staff evaluation of conformance to IEEE Std 603 in Section 7.1.1.3.10 of this report is applicable to the safe shutdown systems. Accordingly, the NRC staff finds that IEEE Std 603, Section 5 is adequately addressed for the safe shutdown systems.

The NRC staff evaluated whether the safe shutdown systems provide the required capacity to function during and after DBEs such as earthquakes and AOOs in conformance with IEEE Std 603, Sections 5.4 and 5.5. The NRC staff evaluated conformance with IEEE Std 603, Section 5.4 for the safety safe shutdown systems. This criterion is evaluated in Section 7.1.1.3.10 of this report, where the NRC staff finds that Section 5.4 is adequately addressed based on its inclusion in the safety system design basis and verification of the EQ in the DCD, Tier 1, Section 3.8, ITAAC. This evaluation is applicable to the safety safe shutdown systems. Accordingly, the NRC staff finds that Section 5.4 is adequately addressed for the safety safe shutdown systems.

The NRC staff evaluated conformance with IEEE Std 603, Section 5.5 for the safety safe shutdown systems. This criterion is evaluated in Section 7.1.1.3.10 of this report, where the NRC staff finds that Section 5.5 is adequately addressed based on its inclusion in the safety system design basis and its verification in the DCD, Tier 1, Section 2.2.15 and Section 3.2, DAC/ITAAC. This evaluation is applicable to the safety safe shutdown systems. Accordingly, the NRC staff finds that IEEE Std 603, Section 5.5, is adequately addressed for the safety safe shutdown systems.

The NRC staff evaluated whether the safe shutdown systems operate with onsite electric power available (assuming offsite power is not available) and with offsite electric power available (assuming onsite power is not available). Electric power is evaluated in Chapter 8 of this report. Additionally, in DCD, Tier 2, Sections 7.4.1.2.1, 7.4.2.2.2, 7.4.3.2.2, and 7.4.4.3 state the following:

- "Power for the safety functions of the SLC system is derived from safety 120 VAC electrical systems UPS. Divisional assignments are made to ensure the availability of each SLC system loop, assuming one safety division of power is not in service in addition to a single active failure. Additionally, a squib initiator in each loop is activated by the DPS as part of the D3 strategy. To avoid adverse interaction, electrical isolation is maintained between the safety divisions, and between the safety divisions and the DPS."

- "The RSS panel is powered from buses supplied by uninterruptible safety and non-safety 120 VAC systems."

- "The RWCU/SDC pumps are supplied from separate and preferred power sources. The power supplies are automatically switched to dual on-site standby diesel-generators following the loss of preferred power (LOPP)."

- "The actuating logic and actuator power for the inner isolation valves for the four ICS trains are on two safety 120 VAC divisional power sources UPS different from the two divisional power sources for the outer isolation valves."

Also, DCD, Tier 1, Table 2.2.15-1, identifies that the DAC/ITAAC for IEEE Std 603, Section 8.1, is required for the safe shutdown systems. The NRC staff finds that the electric power supply is adequately addressed for the safe shutdown systems.

The NRC staff evaluated whether the safe shutdown systems provide the capability to be tested during reactor operation in conformance with IEEE Std 603, Sections 5.7 and 6.5. As described in Item 3 above, based on the inclusion of IEEE Std 603, Sections 5.7 and 6.5, in the safe shutdown systems design basis and their verification in the DCD Tier 1, DAC/ITAAC, the NRC staff finds that IEEE Std 603, Sections 5.7 and 6.5, are adequately addressed for the safe shutdown systems.

7.4.3.2 Evaluation of Safe Shutdown System Conformance with Acceptance Criteria - IEEE Std 603 and IEEE Std 7-4.3.2 Criteria

SRP Section 7.4 states that the safe shutdown systems design should be evaluated for conformance to IEEE Std 603. This section evaluates IEEE Std 603 criteria not previously evaluated in Section 7.4.3.1 of this report. The applicable safe shutdown systems with regard to

IEEE Std 603 are the SLC, ICS, and HP CRD IBF.

The NRC staff evaluated the RPS design basis to determine whether IEEE Std 603, Section 4, was adequately addressed using SRP Appendix 7.1-C, Section 4, "Safety System Designation (IEEE Std 603)." For completeness, the SRP states, "As a minimum each of the safety system design basis aspects identified in IEEE Std 603, Sections 4.1 through 4.12 should be addressed." This criterion is evaluated in Section 7.1.1.3.10 of this report, where the NRC staff finds that Section 4 is adequately addressed based on its inclusion in the safety system design basis and the verification of applicable criteria in the DCD, Tier 1, Section 2.2.15, DAC/ITAAC. This evaluation is applicable to the safe shutdown systems. Also, DCD, Tier 1, Table 2.2.15-1, identifies that the DAC/ITAAC for applicable criteria of Section 4 are applicable to the safe shutdown systems.

DCD, Tier 2, Section 7.4 identifies individual parameters that determine operation of the safe shutdown systems. As mentioned previously, NEDE-33226P and NEDE-33245P, as part of the software life cycle process, define a process by which plant performance requirements, including response times, under various operational conditions will be specified, implemented, and tested. DCD, Tier 1, Section 3.2, includes the DAC/ITAAC for verifying that the software plans were developed and implemented consistent with this process and produce acceptable design outputs. Accordingly, the NRC staff finds that Section 4 is adequately addressed for the safe shutdown systems.

The NRC staff evaluated conformance with IEEE Std 603, Sections 5.2, 5.9, 5.10, 5.11, 5.12, 6.1, 6.2. 6.4, 6.6, 6.7, 6.8, 7.1, 7.2, 7.3, 7.4, 7.5, 8.1, 8.2, and 8.3. These criteria are evaluated in Section 7.1.1.3.10 of this report, where the NRC staff finds that these criteria are adequately addressed based on their inclusion in the safety system design basis and their verification in the DCD, Tier 1, Section 2.2.15, DAC/ITAAC. This evaluation is applicable to the safe shutdown systems. Also, DCD, Tier 1, Table 2.2.15-1, identifies that the DAC/ITAAC for these criteria are applicable to the RPS. Accordingly, the NRC staff finds that conformance to IEEE Std 603, Sections 5.2, 5.9, 5.10, 5.11, 5.12, 6.1, 6.2. 6.4, 6.6, 6.7, 6.8, 7.1, 7.2, 7.3, 7.4, 7.5, 8.1, 8.2, and 8.3 are adequately addressed for the safe shutdown systems.

The NRC staff evaluated whether the quality criterion, IEEE Std 603, Section 5.3, has been adequately addressed for the safety safe shutdown systems. This criterion is evaluated in Section 7.1.1.3.10 of this report, where the NRC staff finds that Section 5.3 has been adequately addressed based on the inclusion of IEEE Std 7-4.3.2, Section 5.3, in the safety system design basis and the verification of the software development activities in the DCD, Tier 1, Section 3.2, DAC/ITAAC. Also, the applicant has stated that the quality assurance program conforms to GDC 1. The evaluation of the adequacy of the quality assurance program is addressed in Chapter 17 of this report. These evaluations are applicable to the safety safe shutdown systems. DCD, Tier 2, Section 7.1.6.6.1.4, also discusses the applicability of this criterion to the Q-DCIS design. Accordingly, based on the applicant's use of an acceptable software development process, as evaluated in Sections 7.1.2.3 and 7.1.1.3.10.2 of this report, and its verification in the DCD Tier 1, DAC/ITAAC, the NRC staff finds that Section 5.3 of IEEE Std 7-4.3.2 and Section 5.3 of IEEE Std 603 are adequately addressed for the safety safe shutdown systems.

The NRC staff evaluated whether IEEE Std 603, Section 5.8, has been adequately addressed. This criterion is evaluated in Section 7.1.1.3.10 of this report, where the NRC staff finds that the criterion is adequately addressed based on its inclusion in the safety system design basis and its verification in the DCD, Tier 1, Section 3.3, DAC/ITAAC. This evaluation is applicable to the

safety safe shutdown systems. In addition, Section 5.8, “Information Displays,” is part of system testing and inoperable surveillance. DCD, Tier 2, Chapter 18, describes the HFE design process to design information displays and is evaluated in Chapter 18 of this report. DCD, Tier 1, Section 3.3, includes the DAC/ITAAC for implementing the HFE design process, which includes the design and verification of controls and information displays for monitoring variables and systems in the control room. This verification is applicable to the safety safe shutdown systems and includes verifying the inventory of displays for manually controlled actions, system status indications, and indications of bypasses. Accordingly, the NRC staff finds that IEEE Std 603, Section 5.8 is adequately addressed for the safety safe shutdown systems.

The NRC staff evaluated conformance with IEEE Std 603, Section 5.13. This criterion is evaluated in Section 7.1.1.3.10 of this report. The multi-unit station criteria do not apply to the standard single unit plant design submitted for NRC certification as stated in DCD, Tier 2, Section 7.1.6.6.1.14. The NRC staff determines that IEEE Std 603, Section 5.13, is not applicable to design certification.

The NRC staff evaluated conformance with IEEE Std 603, Section 5.14. This criterion is evaluated in Section 7.1.1.3.10 of this report, where the NRC staff finds that Section 5.14 is adequately addressed based on its inclusion in the safety systems design basis and its verification in the DCD, Tier 1, Section 3.3, DAC/ITAAC. This evaluation is applicable to the safety safe shutdown systems. Accordingly, the NRC staff finds that IEEE Std 603, Section 5.14, is adequately addressed for the safety safe shutdown systems.

The NRC staff evaluated conformance with IEEE Std 603, Section 5.15. This criterion is evaluated in Section 7.1.1.3.10 of this report, where the NRC staff states that Section 5.15 is adequately addressed based on its inclusion in the safety systems design basis and its verification in the DCD Tier 1, DAC/ITAAC for IEEE Std 603, Sections 5.1, DCD, Tier 1, Section 3.2, DAC/ITAAC, and DCD, Tier 1, Section 3.6, ITAAC. This evaluation is applicable to the safety safe shutdown systems. Accordingly, the NRC staff finds that IEEE Std 603, Section 5.15, is adequately addressed for the safety safe shutdown systems.

7.4.3.3 Evaluation of Safe-Shutdown System Compliance with GDC

The NRC staff reviewed the acceptance criteria for safe shutdown systems in accordance with SRP Section 7.4 and SRP Appendix 7.1-A. For several of the GDC, compliance can be satisfied by meeting IEEE Std 603 requirements, which the NRC staff evaluated in the previous two sections. Compliance with IEEE Std 603 is briefly discussed with the relevant GDC, including the use of DAC, consistent with both SRP sections.

GDC 1 requires quality standards and maintenance of appropriate records.
10 CFR 50.55a(a)(1) requires that structures, systems, and components must be designed, fabricated, erected, constructed, tested, and inspected to quality standards commensurate with the importance of the safety function to be performed. The NRC staff evaluated whether GDC 1 and 10 CFR 50.55a(a)(1) have been adequately addressed for the safe shutdown systems per SRP Appendix 7.1-A. SRP Appendix 7.1-A states that the NRC staff review should confirm that the appropriate regulatory guides and endorsed standards are identified as applicable for each I&C system important to safety. DCD, Tier 2, Table 7.1-1 identifies that GDC GDC 1 and 10 CFR 50.55a(a)(1) are applicable to the safe shutdown systems. The NRC staff evaluation of conformance to RGs and standards for 10 CFR 50.55a(a)(1) and GDC 1 in Sections 7.1.1.3.3 and 7.1.1.3.6 of this report is applicable to the safe shutdown systems. Accordingly, based on the review of updated DCD information, the applicant’s identification of design bases for the

safe shutdown systems and their verification in the ITAAC, the NRC staff finds that the requirements of GDC 1 has been adequately addressed for the safe shutdown systems.

GDC 2 requires design bases for protection against natural phenomena. GDC 4 requires environmental and dynamic effect design bases. The NRC staff evaluated whether GDC 2 and 4 have been adequately addressed for the safe shutdown systems. SRP Section 7.4 identifies that GDC 2 and 4 are addressed by the identification of those systems and components for the safe shutdown systems designed to survive the effects of earthquakes, other natural phenomena, abnormal environments, and missiles in the design bases. SRP Section 7.4 also identifies that GDC 2 and 4 are addressed by the review of the qualification program in DCD, Tier 2, Sections 3.10 and 3.11. DCD, Tier 2, Table 7.1-1, identifies that GDC 2 and 4 are applicable to the safe shutdown systems. DCD, Tier 2, Table 3.2-1, identifies that the safety safe shutdown systems are designed as seismic Category I systems. In DCD, Tier 2, Sections 3.10 and 3.11 describe the EQ programs for safety electrical and digital I&C equipment, which are evaluated in Chapter 3 of this report. In DCD, Tier 1, Table 3.8-1, "ITAAC for Environmental Qualification of Mechanical and Electrical Equipment," Items 1 and 3 include the ITAAC for the applicant to verify the environmental qualification of safety electrical and digital I&C equipment. The evaluation of GDC 2 and GDC 4 in Section 7.1.1.3.6 of this report further addresses these topics and is applicable to the safe shutdown systems. Accordingly, based on the applicant's identification of EQ programs consistent with the design bases for the safe shutdown systems and their verification in the ITAAC, the NRC staff finds that the requirements of GDC 2 and 4 have been adequately addressed.

GDC 13 requires providing instrumentation to monitor variables and systems over their anticipated ranges for normal operation, AOOs, and accident conditions to assure adequate safety. GDC 13 also requires providing appropriate controls to maintain these variables and systems within prescribed operating ranges. GDC 19 requires control room functionality, control room habitability, and remote shutdown capability. The NRC staff evaluated whether GDC 13 and 19 have been adequately addressed for the safe shutdown systems. The evaluation of GDC 19 is provided in Section 7.1.1.3.6 of this report with the exception of the safe shutdown systems support functions necessary for shutting down the reactor and remote shutdown capability. SRP Section 7.4 identifies that GDC 13 and 19 are addressed by the review of I&C required for safe shutdown and within the control room to allow actions to be taken to maintain the nuclear power unit in a safe condition during shutdown, including a shutdown following an accident. GDC 19 also requires that equipment at appropriate locations outside the control room has been 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 RWCU/SDC is the non-safety shutdown system that has the capability of bringing the reactor to safe shutdown and cold shutdown during normal operations. The SLC and ICS are safety systems that provide for safe shutdown during anticipated occurrences and accidents. DCD, Tier 2, Sections 7.4.3.2.2, 7.4.1.2, 7.4.4.3, and 7.4.5.2 specify the automatic and manual initiation controls of the RWCU/SDC, SLC, ICS, and HP CRD IBF respectively. DCD, Tier 2, Section 7.4.3.5, 7.4.1.5, 7.4.4.5, and 7.4.5.5 specify the status indication and the alarms provided for the RWCU/SDC, SLC, ICS, and HP CRD IBF respectively. In combination with the following identified interrelated processes to complete the design of the monitoring capability and control room controls for the safe shutdown systems, the NRC staff finds that the safe shutdown systems provide the I&C needed to maintain variables and systems that can affect the fission process, the integrity of the reactor core, the RCPB, and the containment and its

associated systems within prescribed operating ranges during plant shutdown. In addition, the safe shutdown systems provide within the MCR the I&C needed to allow actions to be taken to maintain the nuclear power unit in a safe condition during shutdown, including a shutdown following an accident. NEDE-33226P and NEDE-33245P, as part of a software life cycle process, define a process by which plant performance requirements under various operational conditions will be specified, implemented, and tested. DCD, Tier 1, Section 3.2, includes the DAC/ITAAC for verifying that the software plans were developed and implemented consistent with this process and produce acceptable design outputs. DCD, Tier 1, Section 3.3, includes the DAC/ITAAC for implementing an HFE design process, which includes the design and verification of controls and information displays for monitoring variables and systems in the control room. These verifications are applicable to the safe shutdown systems and include verification of the controls for manual initiation and control of safe shutdown functions necessary to support actions to operate the nuclear power unit safely under normal conditions and to maintain it in a safe condition under accident conditions.

DCD, Tier 2, Section 7.4.2.5, specifies that the parameters displayed and/or controlled from Division 1 and Division 2 in the MCR also are displayed and/or can be controlled from either of the RSS panels, the conclusions made for the MCR concerning monitoring and controls apply to the remote shutdown capability. The remote shutdown capability is evaluated in Section 7.4.3.1, Item (4), of this report and found acceptable. Therefore the NRC staff finds that equipment at appropriate locations outside the MCR has been 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. Accordingly, based on the identified monitoring capabilities and controls, the defined processes for completing their design, and their verification in the DCD Tier 1, DAC/ITAAC, the NRC staff finds that the requirements of GDC 13 and 19 have been adequately addressed.

GDC 24 requires that the protection system 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. GDC 24 requires that the interconnection of the protection and control systems be limited so as to assure that safety is not significantly impaired. The NRC staff evaluated whether GDC 24 has been adequately addressed for the safe shutdown systems. Appendix 7.1-A to the SRP states that GDC 24 is addressed for safety systems by conformance to IEEE Std 603, Sections 5.1, 5.6, 5.12, 6.3, 6.6, and 8, particularly Sections 5.6 and 6.3. DCD, Tier 2, Table 7.1-1, identifies that GDC 24 applies to the safe shutdown systems. DCD Tier 2, Section 7.4, describes the conformance of safe shutdown systems to IEEE Std 603, Sections 5.6 and 6.3, which are evaluated in Section 7.1.1.3.10 of this report. DCD, Tier 1, Table 2.2.15-2, includes the DAC/ITAAC for verifying that the applicable I&C systems design was completed in compliance with IEEE Std 603, including Sections 5.6 and 6.3. Accordingly, based on the applicant's identification of design bases for the safe shutdown systems, conformance to applicable IEEE Std 603 sections, and their verification in the ITAAC, the NRC staff finds that the requirements of GDC 24 has been adequately addressed.

The NRC staff evaluated whether GDC 34, 35, and 38 have been adequately addressed. According to SRP Appendix 7.1-A, GDC 34 imposes functional requirements on safe shutdown systems provided to initiate, control, and protect the integrity of residual heat removal systems. GDC 34 also requires that necessary I&C systems are operable using either onsite or offsite

power (assuming only one source is available). DCD, Tier 2, Section 3.1.4.5, states that GDC 34 is applicable to the ICS, described in DCD Tier 2, Section 5.4.6. DCD, Tier 2, Section 7.4.4, identifies the corresponding residual heat removal initiation, control, and protection functions in the design bases. According to SRP Appendix 7.1-A, GDC 35 imposes functional requirements on safe shutdown systems provided to initiate, control, and protect the integrity of the ECCS. GDC 35 also requires that necessary I&C systems are operable using either onsite or offsite power (assuming only one source is available). DCD, Tier 2, Section 3.1.4.6, states that GDC 35 is applicable to the ECCS, including the ICS, SLC system, GDCS, and ADS, as described in DCD, Tier 2, Section 6.3. In DCD, Tier 2, Sections 7.4.4 (ICS) and 7.4.1 (SLC system) identify the corresponding safe-shutdown-related ECCS initiation, control, and protection functions in the design bases. According to SRP Appendix 7.1-A, GDC 38 imposes functional requirements on safe shutdown systems provided to initiate, control, and protect the integrity of containment heat removal systems. GDC 38 also requires that necessary I&C systems are operable using either onsite or offsite power (assuming only one source is available). DCD, Tier 2, Section 7.4.4.3 identifies the ICS containment heat removal initiation, control, and protection functions in the design bases.

In addition, SRP Section 7.4 identifies that GDC 34, GDC 35, and GDC 38 are addressed by review for conformance to requirements for testability, operability with onsite and offsite electrical power, and single failures. The single failure and testability requirements correspond to IEEE Std 603, Sections 5.1, 5.7, and 6.5. The NRC staff evaluated conformance of the ICS and SLC system to IEEE Std 603, Sections 5.1, 5.7, and 6.5 in Section 7.4.3.1 of this report and found them adequately addressed. In DCD, Tier 1, Sections 2.2.15, 3.2, 3.3, and 3.8 include the DAC/ITAAC for the applicant to verify that the ICS and the SLC system design implements these design bases and conforms to IEEE Std 603.

For operability with onsite and offsite electrical power, DCD, Tier 2, Section 8.1.3, identifies that the Q-DCIS, which includes the ICS and SLC system I&C systems, is powered by the safety power distribution system normally or by safety batteries for 72 hours if power is lost. Therefore, these systems are operable using either onsite or offsite power (assuming only one source is available). The safety power distribution system and batteries are evaluated in Chapter 8 of this report. Accordingly, based on the applicant's identification of necessary residual heat removal, ECCS, and containment heat removal initiation, control, and protection functions in the design bases of the ICS and their verification in the DCD Tier 1, DAC/ITAAC, the NRC staff finds that the requirements of GDC 34, GDC 35, and 38 have been adequately addressed for the safe shutdown systems.

The NRC staff evaluated whether 10 CFR 50.55a(h) has been adequately addressed for the safe shutdown systems. 10 CFR 50.55a(h) requires compliance with IEEE Std 603-1991 and the correction sheet dated January 30, 1995, which is evaluated in Sections 7.4.3.1 and 7.4.3.2 of this report and found to be adequately addressed. Accordingly, the NRC staff finds that 10 CFR 50.55a(h) has been adequately addressed for the for the safe shutdown systems.

The NRC staff evaluated whether the requirements of 10 CFR 52.47(b)(1) are met. This regulation requires that the application for design certification must contain proposed ITAAC that are necessary and sufficient to provide reasonable assurance that, if the ITA are performed and the acceptance criteria are met, a plant that references the design certification has been constructed and will operate in accordance with the design certification, the Atomic Energy Act, and the Commission's rules and regulations. The ITAAC specific to the safe shutdown systems are addressed throughout section 7.2.3 of this report. The NRC staff evaluation of conformance to 10 CFR 52.47 in Section 7.1.1.3.4 of this report is applicable to the safe shutdown systems.

Therefore, the NRC staff finds that the requirements of 10 CFR 52.47(b)(1) have been adequately addressed for the safe shutdown systems.

7.4.4 Conclusion

Based on the above, the NRC staff concludes that the applicant adequately addresses the major design considerations for the safe shutdown systems. As discussed in Sections 7.1.1.3.1 through 7.1.1.3.10 of this report and Section 7.4.3 above, the NRC staff concludes for the safe shutdown systems, the applicant adequately addresses the relevant requirements of 10 CFR 50.55a(a)(1), 10 CFR 50.55a(h), 10 CFR 52.47(b)(1), GDC 1, 2, 4, 13, 19, 24, 34, 35, and 38. The applicant has also identified adequate high-level functions and included sufficient DAC/ITAAC in Tier 1 to verify that safe shutdown systems design is completed in compliance with the applicable requirements.

7.5 Information Systems Important to Safety

7.5.1 Introduction

The NRC staff reviewed the information systems important to safety in accordance with SRP Section 7.5, Revision 5, "Information Systems Important to Safety," to confirm that these systems will provide the information to ensure plant safety during all plant conditions for which they are required.

SRP Section 7.5 provides acceptance criteria for the following types of systems:

- accident monitoring instrumentation
- bypassed or inoperable status indication (BISI) for safety systems
- plant annunciator (alarm) systems
- SPDS and information systems associated with the emergency response facilities (ERF) and ERDS

7.5.1.1 Summary of Regulatory Criteria

Specific acceptance criteria are identified for each type of system. Accordingly, acceptance criteria are identified that are applicable to all information systems important to safety, followed by the additional acceptance criteria particular to each of the types of information systems important to safety.

Acceptance criteria for all information systems important to safety:

Acceptance criteria for all information systems important to safety are based on meeting the relevant requirements of 10 CFR 50.55a(a)(1); 10 CFR 50.55a(h); and GDC 1 and 24; and 10 CFR 52.47(b)(1). The acceptance criteria are also based on conforming to the guidelines of IEEE Std 7-4.3.2, as endorsed by RG 1.152.

Additional acceptance criteria for accident monitoring instrumentation:

In addition to the requirements listed above for the information systems important to safety, acceptance criteria for the accident monitoring instrumentation are based on meeting the relevant requirements of 10 CFR 50.34(f)(2), Subparts (v) [I.D.3], (xi) [II.D.3], (xvii) [II.F.1], (xviii) [II.F.2], (xix) [II.F.3], and (xxiv) [II.K.3.23]; and GDC 2, 4, 13, and 19.

Additional acceptance criteria for BISI for safety systems:

In addition to the requirements for the information systems important to safety, acceptance criteria for the BISI are based on meeting the relevant requirements of 10 CFR 50.34(f)(2)(v) [I.D.3].

Additional acceptance criteria for plant annunciator (alarm) systems:

In addition to the requirements for the information systems important to safety, acceptance criteria for the annunciator systems are based on meeting the relevant requirements of GDC 13 and 19, and the SRM on SECY-93-087, Item II.T.

SRP Section 7.5 does not identify additional requirements for SPDS, ERF information systems, and ERDS information systems.

In addition to using SRP Section 7.5, the NRC staff reviewed I&C systems with accident monitoring functions in accordance with BTP HICB-10, "Guidance on Application of Regulatory Guide 1.97." RG 1.97, describes methods acceptable to the NRC staff for providing instrumentation to monitor variables for accident conditions. BTP HICB-10 requires use of the regulatory criteria in 10 CFR 50.34(f)(2)(xvii) and GDC 13, 19, and 64, "Monitoring Radioactivity Releases." Note that the acceptance criteria in BTP HICB-10 are redundant to the criteria in SRP Section 7.5, with the exception of GDC 64.

The applicant has identified a CMS as an information system important to safety. In addition to the requirements for the accident monitoring instrumentation, acceptance criteria for the CMS are based on meeting the relevant requirements of 10 CFR 50.44(c)(4).

7.5.1.2 Method of Review

As noted above, SRP Section 7.5 provides acceptance criteria for four types of systems. DCD, Tier 2, Section 7.5, directly describes one of the systems, accident monitoring instrumentation. For the remaining three types of systems, DCD, Tier 2, Section 7.5, mentions them briefly and identifies where they are discussed in greater detail in the DCD. This report evaluates each of these systems.

In addition to the PAM instrumentation, DCD Tier 2 identifies four information systems (CMS, process radiation monitoring system, area radiation monitoring system, and pools monitoring system) that are not directly covered by SRP Section 7.5. For the CMS, the NRC staff used the criteria for accident monitoring instrumentation, with the exception of criteria related to RG 1.97, since these criteria are addressed for the PAM instrumentation. The NRC staff also identifies where the remaining three systems are evaluated in this report.

Since the DCD and the SRP do not fully match, the evaluation of information systems important to safety is evaluated in a hybrid manner. For each applicable system, the NRC staff provides a summary of technical information and an evaluation of major design considerations. The NRC staff then provides a general evaluation of the regulatory criteria.

7.5.2 Post Accident Monitoring Instrumentation

7.5.2.1 Regulatory Criteria

Acceptance criteria for the accident monitoring instrumentation are based on meeting the relevant requirements of 10 CFR 50.55a(a)(1); 10 CFR 50.55a(h); 10 CFR 50.34(f)(2), Subparts (v) [I.D.3], (xi) [II.D.3], (xvii) [II.F.1], (xviii) [II.F.2], (xix) [II.F.3], and (xxiv) [II.K.3.23]; GDC 1, 2, 4, 13, 19, 24, and 64; and 10 CFR 52.47(b)(1). The acceptance criteria are also based on conforming to the guidelines of IEEE Std 7-4.3.2, as endorsed by RG 1.152.

7.5.2.2 Summary of Technical Information

The safety portion of the PAM systems consists of those systems that provide information for the safe operation of the plant during normal operation, AOOs, and accidents, to help ensure performance of manual safety functions. The safety information systems include those systems that provide information for manual initiation and control of safety systems, indicate that safety plant functions are being accomplished, and provide information from which appropriate actions can be taken to mitigate the consequences of accidents.

The non-safety portion of the PAM systems includes the SPDS, information systems associated with the ERF, and the ERDS, none of which performs safety functions.

RG 1.97 endorses (with certain exceptions specified in Section C of the RG) IEEE Std 497"IEEE Standard Criteria for Accident Monitoring Instrumentation for Nuclear Power Generating Stations". IEEE Std 497 establishes flexible, performance-based criteria for the selection, performance, design, qualification, display, and quality assurance of accident monitoring variables. IEEE Std 497 identifies five types of variables for accident monitoring and the criteria for the selection of each type of variable.

The PAM instrumentation design is part of the overall HFE process. The HFE process includes the functional requirements analysis, allocation of functions, and task analysis that address critical safety functions, and provides an independent list of the required RG 1.97 parameters via their respective results summary reports. The functional requirements analysis (FRA), allocation of functions (AOF), and task analysis (TA) are iteratively integrated into the design process to provide a final design that effectively balances human factors and system design. The list of parameters, generated by the HFE process, is compared with the information generated from the design process and the differences are entered into the HFE issue tracking system for resolution.

The PAM variable list is prepared as a separate document, using inputs from the design process, licensing design basis, and HFE process, including the development of the emergency procedure guidelines and/or emergency operating procedures and abnormal operating procedures. The PAM variable list document provides summary information for each PAM variable as applicable. Typical information provided includes the following:

- PAM variable name
- type
- range
- extended range (Type C)

- instrument channel accuracy
- required instrument duration
- power source
- required number of channels
- qualification criteria
- type of monitoring channel display

In DCD, Tier 1, Section 3.7, the applicant documented the DAC for the PAM instrumentation as follows:

Performance Criteria

- range
- accuracy
- response time
- required instrument duration
- reliability
- performance assessment documentation

Design Criteria

- single failure
- CCFs
- independence and separation
- isolation
- information ambiguity
- power supply
- calibration
- testability
- direct measurement
- control of access
- maintenance and repair
- auxiliary supporting features
- portable instruments
- documentation of design criteria

Qualification Criteria

- Type A variables
- Type B variables
- Type C variables
- Type D variables
- Type E variables
- portable instruments
- post-event operating time
- documentation of qualification criteria

Display Criteria

- information characteristics
- human factors
- anomalous indications
- continuous versus on-demand display
- trend or rate information
- display identification
- type of monitoring channel display
- display location
- information ambiguity
- recording
- digital display signal validation
- display criteria documentation

In DCD, Tier 1, Section 3.7, the applicant documented that the ITAAC will be performed using the FRA, AOF, and TA to support closure of the referenced ITAAC that will provide the final list of the required RG 1.97 parameters via their respective results summary reports, to verify that the PAM instrumentation is installed consistent with the selected variables as described above.

7.5.2.3 Evaluation of Accident Monitoring Systems Conformance with Acceptance Criteria - Major Design Considerations

Per SRP Section 7.5, the following are the major design considerations that should be emphasized in the accident monitoring systems review.

(1) Conformance with RG 1.97 and BTP HCIB-10

The NRC staff evaluated whether the guidelines of RG 1.97 have been adequately addressed. RG 1.97 endorses IEEE Std 497. DCD, Tier 2, Section 7.5.1.3.4, states that the ESBWR conforms to RG 1.97 and IEEE Std 497 (with certain exceptions specified in Section C of RG 1.97). DCD, Tier 2, Section 7.5.1.3, also describes the performance-based criteria that the ESBWR uses for the selection, performance, design, qualification, display, and quality assurance of accident monitoring variables. These criteria are consistent with RG 1.97 and IEEE Std 497. Conformance with the specific IEEE Std 497 Sections 6.2 and 8 is described under Item (2) below. The selection of accident monitoring variables is integrated with the HFE design as described in DCD Chapter 18. DCD, Tier 1, Section 3.7, includes these criteria and ITAAC to confirm that the PAM instrumentation is installed and consistent with the selected variables. DCD, Tier 1, Section 3.8, includes the DAC/ITAAC to confirm that the HFE design is implemented in accordance with the process described in DCD Chapter 18. Accordingly, the NRC staff finds that the guidelines of RG 1.97 have been adequately addressed.

The NRC staff evaluated whether the guidelines of BTP HCIB-10 have been adequately addressed. BTP HCIB-10 includes acceptance criteria that supplement the design and qualification criteria identified in RG 1.97, Revisions 2, 3, and 4. This includes (1) environmental qualification, (2) seismic qualification, (3) redundancy, (4) independence of redundant instrumentation, (5) display and recording, (6) range, (7) minimizing measurements, (8) alternate variables, (9) guidance for BWR and PWR variables, (10) conversion to Revision 4, and (11) modifications to Revision 4. However, several of these considerations are applicable only to current plants using RG 1.97 Revisions 2 or 3. As the ESBWR is applying RG 1.97 Revision 4, the only applicable criteria that apply are environmental qualification, seismic qualification, independence of redundant instrumentation, range, and minimizing

measurements. Each of these considerations is evaluated below.

DCD, Tier 2, Section 7.5.1.3.5, discusses conformance of the PAM instrumentation to BTP HICB-10. The section references RG 1.97, Revision 4, Section A, which states, "Branch Technical Position HICB 10 will require updates for consistency with Revision 4 of RG 1.97. Conformance to these requirements is addressed during the detailed design phase." In RAI 7.5-7, the staff requested the applicant to clarify conformance to RG 1.97 and BTP HICB-10. RAI 7.5-7 was being tracked as an open item in the SER with open items. In its response, the applicant clarified the PAM design basis and made corresponding changes to DCD Revision 6. DCD, Tier 1, Section 3.7, Post Accident Monitoring Instrumentation, committed that the installed PAM instrumentation (scope as determined by the HFE process as described in DCD, Tier 1, Section 3.3) conforms with the requirements (variables, types, performance criteria, design criteria, qualification criteria, display criteria, and quality assurance) as outlined in RG 1.97. Accordingly, the NRC staff finds that the PAM instrumentation design has followed the guidelines of RG 1.97 and BTP HCIB-10. The staff determined that the response was acceptable since the applicant addressed conformance to RG 1.97 and BTP HICB-10. Based on the applicant's response RAI 7.5-7 is resolved.

BTP HICB-10 also identifies GDC 64 as part of the regulatory basis, which requires, in part that means be provided to monitor (1) the reactor containment atmosphere, (2) spaces containing components for recirculation of LOCA fluid, (3) effluent discharge paths, and (4) the plant environs for radioactivity that may be released from postulated accidents. DCD, Tier 2, Section 7.5.1.3.2, states that GDC 64 is applicable to the PAM instrumentation. DCD, Tier 2, Section 7.3.3, describe the LD&IS which provides monitoring radioactivity inside and outside containment. The LD&IS also receives information from the RCPB leak detection systems as described in DCD Section 5.2.5. In DCD, Tier 2, Sections 7.5.3 and 11.5, describe the PRMS, which provides a capability for determining the content of radioactive material in various gaseous and liquid process and effluent streams. DCD, Tier 2, Section 11.5.5.4, specifically identifies ESBWR areas that are monitored in conformance with GDC 64 that include spaces containing components for recirculation of LOCA fluid. Information from the LD&IS and PRMS are available to the PAM instrumentation through the DCIS. DCD, Tier 2, Section 7.5.1.3, describes the criteria that the ESBWR uses for the selection of accident monitoring variables. In the ESBWR design, the LOCA fluid is passively recirculated through the GDCS, which receives condensed steam from the PCCS. Since both the GDCS and PCCS are inside containment, the monitoring is provided by the LD&IS. The selection of accident monitoring variables is integrated with the HFE design process, as described in DCD Chapter 18. DCD, Tier 1, Section 3.7, includes these criteria and ITAAC to confirm that the PAM instrumentation is described consistently with the selected variables. DCD, Tier 1, Section 3.8, includes the DAC/ITAAC to confirm that the HFE design is implemented according to the process described in DCD Chapter 18. Accordingly, the NRC staff finds that the requirements of GDC 64 have been adequately addressed.

(2) Use of Digital Systems (IEEE Std 497-2002, Sections 6.2 and 8)

SRP Section 7.5 identifies that the review of computer-based digital systems should focus on IEEE Std 497, Sections 6.2 and 8. IEEE Std 497-2002, Section 6.2, "Common Cause Failure," states that the design should address the concern of CCFs of the digital system. The applicant submitted NEDO-33251 to demonstrate that defense-in-depth exists against the consequences of a software CCF. The NRC staff evaluation of the D3 assessment is documented in Section 7.1.3 of this report.

IEEE Std 497, Section 6.2, states that use of identical software in redundant instrumentation channels is acceptable, provided that the licensee conducts an analysis to demonstrate D3 exists against CCFs. For accident monitoring instrumentation from the safety sources, the Q-DCIS provides the required signal path to process this information. This information then is shown on the Q-DCIS divisional safety displays. The safety information can also be transmitted via isolated safety gateways to the N-DCIS for input to non-safety displays, PCF, and AMS. Type A, Type B, and Type C variables are powered from safety sources. For Type D and Type E variables, which are powered from non-safety sources, the N-DCIS provides the required signal paths to process information. As discussed in Section 7.1 of this report, the DCIS design satisfies the separation and isolation guidelines. The NRC staff finds this arrangement acceptable.

IEEE Std 497, Section 8, specifies the "display criteria" for accident monitoring variables that should include the results of an analysis of the system functions required to respond to an accident and analysis of the tasks required of the operator to implement those functions during DBEs. Display characteristics should be identified that include, as a minimum; range, instrument accuracy, precision, display format (e.g., status, value, or trend), units, and response time.

In DCD, Tier 1, Section 3.7, "Post Accident Monitoring Instrumentation," the applicant documented the design requirements for the ESBWR PAM instrumentation. The DCIS (both the Q-DCIS and the N-DCIS) provides the required signal paths to process this information. For variables associated with critical safety functions and powered from a safety power source, the Q-DCIS provides the required signal paths to process this information. The information is then displayed on the Q-DCIS divisional safety displays. The safety information can also be transmitted via isolated non-safety gateways to the N-DCIS for input to non-safety displays, PCF, and the alarm management system. Type A, Type B, and Type C variables are powered from safety sources. Type D and Type E variables will have their power source determined as part of the design process.

DCD, Tier 2, Section 7.5.1.3, describes the criteria that the ESBWR uses for the selection of accident monitoring variables. The selection of accident monitoring variables is integrated with the HFE design process, as described in DCD, Tier 2, Chapter 18. DCD, Tier 1, Section 3.7, includes these criteria and the ITAAC to confirm that the PAM instrumentation is installed consistently with the selected variables. DCD, Tier 1, Section 3.3, includes the DAC/ITAAC to confirm that the HFE design is implemented in accordance with the process described in DCD Chapter 18. Accordingly, the NRC staff finds that the requirements of IEEE Std 497, Section 8, have been adequately addressed.

The NRC staff evaluated whether IEEE Std 7-4.3.2, as endorsed by RG 1.152, has been adequately addressed for the PAM instrumentation. SRP Appendix 7.1-D provides guidance on the implementation of IEEE Std 7-4.3.2 concerning the use of digital systems. In Section 7.1.1.3.10 of this report, the NRC staff evaluated in parallel IEEE Std 7-4.3.2 and IEEE Std 603 using the guidance in SRP Appendix 7.1-D. The NRC staff evaluation of conformance to IEEE Std 7-4.3.2 in Section 7.1.1.3.10 of this report is applicable to the PAM system.

The software development activities are described in NEDE-33226P and NEDE-33245P. DCD, Tier 1, Section 3.2, includes the DAC/ITAAC to confirm that the completion of these activities and products conforms to the processes described in NEDE-33226P and NEDE-33245P and the guidelines of BTP HCIB-14. The NRC staff evaluation of software development activities is

provided in Section 7.1.2 of this report.

(3) Emergency Operating Procedure (EOP) Action Points

SRP Section 7.5 states that a basis should be provided for the EOP action points that account for measurement uncertainties. EOP action points are type B accident monitoring variables under RG 1.97, Revision 4. DCD, Tier 2, Section 7.5.1.3 describes the performance criteria and design criteria to be used accident monitoring instrumentation, including instrumentation for type B accident monitoring variables. The performance criteria and design criteria include considerations for variable accuracy, information ambiguity, and calibration. DCD, Tier 1, Section 3.7 provides ITAAC to confirm that the accident monitoring instrumentation meets the performance and design criteria of RG 1.97. Based on the above, the staff finds that the EOP action points and their measurement uncertainties are adequately addressed.

(4) Monitoring for Severe Accidents

SRP Section 7.5 states the following:

> The accident monitoring instrumentation should be demonstrated to perform their intended function for severe accident protection. They need not be subject to additional 10 CFR 50.49 environmental qualification requirements. However, they should be designed so that there is reasonable assurance that they will operate in the severe accident environment for which they are intended and over the time span for which they are needed.

This guidance is based on SECY-93-087, "Item L Equipment Survivability."

DCD, Tier 2, Section 19.3.4, summarizes the ESBWR severe accident equipment survivability analysis. Appendix 8D to NEDO-33201, "ESBWR Certification Probabilistic Risk Assessment," provides a more detailed severe accident equipment survivability analysis. NEDO-33201, Table 8.D.2-1, identifies the required functions and associated monitored variables. In NEDO-33201, Section 8D.4.6, provides the equipment capability evaluation of the PAM equipment. Section 19.2.3.3.7 of this report provides the NRC staff evaluation of the severe accident equipment survivability analysis and finds that the analysis provides reasonable assurance that the equipment necessary to achieve a controlled, stable plant condition will function over the time span in which it is needed. Accordingly, the NRC staff finds that the guidance on monitoring for severe accidents has been adequately addressed.

(5) Performance Assessment

SRP Section 7.5 identifies that the review should confirm that the performance assessment fulfills the goals outlined in IEEE Std 497-2002, Section 5.6, "Performance Assessment Documentation," which states that an assessment for each of the performance criteria shall be conducted to assure that the as-designed performance meets or exceeds the performance criteria. DCD, Tier 2, Section 7.5.1.3.4, states that performance criteria (identified in IEEE Std 497, Section 5) are developed during the design process using input from the HFE process together with other design and accident analysis inputs. The performance criteria for each required variable are documented in the PAM variable list. Performance is verified to meet the as-designed performance criteria of DCD, Tier 2, Section 18.11, "Human Factor Verification and Validation." DCD, Tier 1, Section 3.7, includes these performance criteria and ITAAC to confirm that the PAM instrumentation is installed consistent with the selected variables. DCD, Tier 1,

Section 3.8, includes the DAC/ITAAC to confirm that the HFE design is implemented in accordance with the process described in DCD Chapter 18. Accordingly, the NRC staff finds that the guidance on performance assessment has been adequately addressed.

The remaining criteria are evaluated in Section 7.5.11 of this report.

7.5.3 Containment Monitoring System

7.5.3.1 Regulatory Criteria

The CMS is classified as a safety and seismic Category I system. Acceptance criteria for the CMS are based on meeting the relevant requirements of 10 CFR 50.55a(a)(1); 10 CFR 50.55a(h); 10 CFR 50.34(f)(2), Subparts (v) [I.D.3], (xi) [II.D.3], (xvii) [II.F.1], (xviii) [II.F.2], (xix) [II.F.3], and (xxiv) [II.K.3.23]; 10 CFR 50.44(c)(4), GDC 1, 2, 4, 13, 19, and 24; and 10 CFR 52.47(b)(1). The acceptance criteria are also based on conforming to the guidelines of IEEE Std 7-4.3.2, as endorsed by RG 1.152.

7.5.3.2 Summary of Technical Information

The CMS provides the instrumentation to monitor the following:

- atmosphere in the containment for high gross gamma radiation levels
- pressure of the drywell and wetwell
- drywell/wetwell differential pressure
- lower and upper drywell water level (post-LOCA)
- temperature of the suppression pool water
- suppression pool water level
- drywell/wetwell hydrogen/oxygen concentration
- containment area radiation

These parameters are monitored during both normal reactor operations and post accident conditions to evaluate the integrity and safe conditions of the containment. Abnormal measurements and indications initiate alarms in the MCR.

The CMS is divisional and segregated (safety/non-safety). The specific system features are as follows:

- Radiation monitoring and hydrogen and oxygen sampling are provided for the drywell and for the air space above the suppression pool.

- Each radiation monitoring channel uses one gamma-sensitive ion chamber and one digital log radiation monitor. Four channels are provided, two for the drywell and two for the suppression pool (wetwell) air space.

- During normal plant operation, both the radiation monitoring and gas sampling subsystems are operating. For PAM, the gas sampling subsystem is automatically activated by the LOCA signal to alternate its sampling between the drywell and the wetwell. The area of sampling can be selected manually or sequentially controlled.

- Heat tracing is provided on the gas sampling lines for control of moisture and condensation.

- Two isolation valves are provided on each sample and return line that penetrates the containment. Each line has one manual inner valve and one remote-control outer valve.

- Each gas sampling analyzer has dual redundant pumps. One is used during normal operation; the other is used for added capacity or backup.

- Separate oxygen and hydrogen gas sources are provided in each CMS sampling rack with known compositions for monitor calibration.

- CMS piping connections are provided.

- The drywell pressure instrumentation taps are located throughout the containment and the sensors are located outside the containment.

- Four drywell pressure transmitters are provided for safety signals for use by the RPS for reactor scram. Four additional safety drywell pressure signals are made available to the LD&IS, where they are used to initiate isolation of containment valves, transfer pump suction, and initiate SPCS.

- Two wide-range safety pressure transmitters are used for providing safety drywell pressure information meeting the requirements of PAM.

- Four non-safety drywell pressure transmitters are used by the DPS for diverse scram protection monitoring and by the CIS for controlling the position of the nitrogen makeup pressure control valve.

- The suppression pool water level is monitored during all plant operating conditions and post accident conditions. Suppression pool water level monitoring consists of 10 channels of water level detection sensors distributed into 4 safety narrow-range and 4 non-safety wide-range instruments. The narrow-range suppression pool water level signals are used to detect the uncovering of the first set of suppression pool temperature sensors below the pool surface. When the suppression pool water level drops below the elevation of a particular set of temperature sensors, those sensor signals are not used in computing the average pool temperature.

- Two of the wide-range water level signals are used for displaying suppression pool water level on the RSS panels.

- Suppression pool temperatures are monitored.

7.5.3.3 NRC Staff Evaluation

The SPTM function of the CMS is part of the RPS and is evaluated in Section 7.2 of this report.

The NRC staff evaluated whether the I&C portions of 10 CFR 50.44(c)(4) have been adequately addressed. 10 CFR 50.44(c)(4)(i) requires that equipment be provided for monitoring oxygen in containments that use an inerted atmosphere for combustible gas control. Equipment for

monitoring oxygen must be functional, reliable, and capable of continuously measuring the concentration of oxygen in the containment atmosphere following a significant beyond DBA for combustible gas control and accident management, including emergency planning. 10 CFR 50.44(c)(4)(ii) requires that equipment be provided for monitoring hydrogen in the containment. Equipment for monitoring hydrogen must be functional, reliable, and capable of continuously measuring the concentration of hydrogen in the containment atmosphere following a significant beyond DBA for accident management, including emergency planning.

DCD, Tier 2, Section 6.2.5, describes the design of the oxygen and hydrogen monitors, which is evaluated in Section 6.2.5 of this report. DCD, Tier 2, Section 7.5.2.3.1 specifies that the CMS conforms to 10 CFR 50.44(c)(4). DCD, Tier 2, Section 7.5.2.3 identifies that the CMS provides continuous monitoring during normal reactor operation, as well as during and after DBEs. DCD, Tier 2, Section 7.5.2.1, indicates that the safety hydrogen/oxygen analyzers are active during normal operation. Additional sampling capacity is automatically initiated by a LOCA signal for PAM of oxygen and hydrogen content in the containment. DCD, Tier 2, Section 7.5.2.5 describes the surveillance testing of the CMS, which includes instrument channel checks of the radiation and gas monitors, functional tests to verify equipment operability, sensor calibration and response tests, and leakage tests of the gas sampling lines. DCD, Tier 2, Table 7.5-5 identifies the instrument ranges for hydrogen and oxygen analyzers. The staff finds that these design bases address the functionality, reliability, and capability requirements in 10 CFR 50.44(c)(4). Accordingly, the NRC staff finds that the requirements of 10 CFR 50.44(c)(4) have been adequately addressed for the CMS.

The remaining criteria are evaluated in Section 7.5.11 of this report.

7.5.4 Process Radiation Monitoring System

The PRMS provides the instrumentation for radiological monitoring, sampling, and analysis in the following areas:

- turbine building
- TSC
- radwaste building
- control building
- reactor building
- fuel building
- reactor building/fuel building stack
- turbine building stack, and
- radwaste building stack

The PRMS alerts operators to radiation levels in excess of preset limits and initiates automatically the required protection action to isolate, contain, or redirect radioactivity releases to the environs. Some subsystems of the PRMS are safety. The evaluation of the PRMS is provided in Section 11.5 of this report.

7.5.5 Area Radiation Monitoring System

The primary function of the non-safety ARMS is to continuously monitor the gamma radiation levels within the various areas of the plant and to provide an early warning that predetermined radiation levels are exceeded. The ARMS consists of area radiation detectors located at

accessible areas of the plant and utilizes local and MCR alarms for immediate warning. The gross gamma radiation levels are monitored on a continuous basis, because changes are caused by operational transients or maintenance activities. Any high radiation levels are indicated by audible area alarms and MCR alarms. The evaluation of these systems is addressed in Section 12.3 of this report.

7.5.6 Pool Monitoring Subsystem Evaluation

Safety temperature and level instrumentation is provided in the CMS to monitor suppression pool water temperature and water level, respectively. The CMS is evaluated in Section 7.5.3 of this report.

Safety level instrumentation is provided in the GDCS for the GDCS pools to provide necessary information to the operator for maintaining the GDCS water level required for the safety ECCS function. The instrumentation for the GDCS is evaluated in Section 7.3 of this report.

Safety level instrumentation is provided in the fuel and FAPCS for the spent fuel pool, the buffer pool, and the IC/PCCS pools to detect a low water level that would indicate a loss of decay heat removal ability. The FAPCS is evaluated in Section 9.1.3 of this report.

7.5.7 Not Used

7.5.8 Bypassed and Inoperable Status Indication for Safety Systems

7.5.8.1 Regulatory Criteria

Acceptance criteria for BISI for safety systems are based on meeting the relevant requirements of 10 CFR 50.55a(a)(1); 10 CFR 50.55a(h); 10 CFR 50.34(f)(2)(v) [I.D.3]; 10 CFR Part 50, Appendix A, GDC 1 and 24; and 10 CFR 52.47(b)(1). The acceptance criteria are also based on conforming to the guidelines of IEEE Std 7-4.3.2, as endorsed by RG 1.152.

7.5.8.2 Summary of Technical Information

DCD Tier 2 does not directly address BISI for safety systems consistent with SRP Section 7.5. DCD, Tier 2, Section 7.5, mentions BISI for safety systems briefly and identifies where they are discussed in greater detail in the DCD. DCD, Tier 2, Table 1A-1, discusses BISI for safety systems in the context of conformance to 10 CFR 50.34(f)(2)(v) and identifies where information is provided in more detail in DCD, Tier 2, Sections 7.2, 7.3, 7.5, and 7.8. BISI for safety systems is also discussed in the context of conformance to IEEE Std 603, Section 5.8.3, and RG 1.47 in associated sections.

7.5.8.3 Evaluation of BISI for Safety Systems Conformance with Acceptance Criteria - Major Design Considerations

Per SRP Section 7.5, the following are the major design considerations that should be emphasized in the BISI for safety systems review:

(1) Scope of Bypassed and Inoperable Status Indication

SRP Section 7.5 notes that, at a minimum, BISI should be provided for four sets of systems; however, only the first sets of systems, the RPS and ESF actuation systems, are applicable to

the design. DCD, Tier 2, Table 7.1-1, states that 10 CFR 50.34(f)(2)(v), which is the requirement to provide for automatic indication of the bypassed and inoperable status of safety systems, is applicable to all safety systems, including the RPS and ESF. Section 7.1.1.3.4 of this report provides an evaluation of the I&C systems against the requirements of 10 CFR 50.34(f)(2)(v). SRP Section 7.5 notes that the indication of bypasses should conform to IEEE Std 603, Section 5.8.3.

As described in Sections 7.1.1.3.4 (for 10 CFR 50.34(f)(2)(v)) and 7.1.1.3.10 (for IEEE Std 603, Section 5.8.3) of this report, the NRC staff found that IEEE Std 603, Section 5.8.3, has been adequately addressed based on its inclusion in the safety systems design bases and DCD, Tier 1, Section 2.2.15, including the DAC/ITAAC for the applicant to verify conformance to these IEEE Std 603 criteria. Information displays are designed using the HFE design process as described in DCD, Tier 2, Chapter 18, and evaluated in Chapter 18 of this report. DCD, Tier 1, Section 3.3, includes the DAC/ITAAC for verifying the implementation of the HFE design process, which includes the design and verification of controls and information displays for monitoring variables and systems in the control room. This verification is applicable to all safety systems and includes BISI. Accordingly, based on applicable criteria being included in the safety systems design basis and their confirmation in the DAC/ITAAC, the NRC staff finds that the guideline for the scope of BISI has been adequately addressed.

(2) Conformance with Regulatory Guide 1.47

RG 1.47, provides more specific guidance on BISI. DCD, Tier 2, Table 7.1-1, indicates that RG 1.47 is applicable to the safety systems consistent with SRP Table 7-1. DCD, Tier 2, Section 7.1.6.4, in the discussion regarding conformance to RG 1.47, notes that bypass indications are designed to satisfy the guidance of IEEE Std 603, Section 5.8.3, and RG 1.47. This section also states that bypass indications use isolation devices that preclude the possibility of any adverse electrical effect of the bypass indication circuits on the plant safety system. The NRC staff finds this acceptable.

(3) Independence (IEEE Std 603, Sections 5.6 and 6.3)

SRP Section 7.5 states that the BISI for safety systems should be designed and installed in a manner that precludes the possibility of adverse effects on plant safety systems in conformance with IEEE Std 603, Sections 5.6 and 6.3. As described in Section 7.1.1.3.10 of this report, which is applicable to BISI for safety systems, the NRC staff finds that IEEE Std 603, Sections 5.6 and 6.3, have been adequately addressed based on their inclusion in the safety systems design basis and their confirmation in the DAC/ITAAC. Accordingly, the NRC staff finds IEEE Std 603, Sections 5.6 and 6.3, adequately addressed for BISI.

(4) Use of Digital Systems

The NRC staff evaluated whether IEEE Std 7-4.3.2, as endorsed by RG 1.152, has been adequately addressed for BISI. SRP Appendix 7.1-D provides guidance on the implementation of IEEE Std 7-4.3.2 concerning the use of digital systems. In Section 7.1.1.3.10 of this report, the NRC staff evaluated in parallel IEEE Std 7-4.3.2 and IEEE Std 603 using the guidance in SRP Appendix 7.1-D. The NRC staff evaluation of conformance to IEEE Std 7-4.3.2 in Section 7.1.1.3.10 of this report is applicable to the BISI system.

The software development activities are described in NEDE-33226P and NEDE-33245P. DCD, Tier 1, Section 3.2, includes the DAC/ITAAC to confirm that the completion of these activities

and products conforms to the processes described in NEDE-33226P and NEDE-33245P and the guidelines of BTP HCIB-14. The NRC staff evaluation of software development activities is provided in Section 7.1.2 of this report.

The remaining criteria are evaluated in Section 7.5.11 of this report.

7.5.9 Plant Annunciator (Alarm) Systems

7.5.9.1 Regulatory Criteria

SRP Section 7.5 acceptance criteria for information systems important to safety are based on meeting the relevant requirements of 10 CFR 50.55a(a)(1); 10 CFR 50.55a(h); GDC 1, 13, 19, and 24; and 10 CFR 52.47(b)(1). The acceptance criteria are also based on conforming to the guidelines of IEEE Std 7-4.3.2, as endorsed by RG 1.152, and the SRM on SECY-93-087, Item II.T.

7.5.9.2 Summary of Technical Information

DCD Tier 2 does not directly address annunciator systems consistent with SRP Section 7.5. Annunciator systems are described in the context of the AMS and its conformance to the SRM on SECY-93-087, Item II.T. In DCD, Tier 2, Sections 7.1.5.3 and 7.1.6.3 state that the AMS has the following attributes:

- The AMS follows the guidance in SECY-93-087, Item II.T, including following the guidance for redundancy, independence, and separation.
- Alarm points are sent through dual networks to redundant message processors on dual power supplies.
- The processors are dedicated to only performing alarm processing.
- The alarms are displayed on multiple independent VDUs each of which has dual power supplies.
- The alarm tiles, or their equivalent, are driven by redundant datalinks (with dual power).
- There are redundant alarm processors.
- There are no alarms that require manually controlled actions for safety systems to accomplish their function.
- There is one horn and one voice speaker.
- Test buttons test the horn and the lights.
- The requirements for safety equipment and circuits are not applicable.

7.5.9.3 Evaluation of Plant Annunciator Systems Conformance with Acceptance Criteria - Major Design Considerations

Per SRP Section 7.5, the following are the major design considerations that should be emphasized in the plant annunciator systems review:

(1) Reliability (IEEE Std 603, Section 5.15)

SRP Section 7.5 states that the applicant should justify that the degree of redundancy, diversity, testability, and quality provided in annunciator systems is adequate to support normal and emergency operations. DCD, Tier 2, Section 7.1.5.3, notes that the AMS conforms to the SRM on SECY-93-087, Item II.T, including following the guidance for redundancy, independence, and separation. The NRC staff evaluated conformance to the SRM on SECY-93-087, Item II.T in Section 7.1.1.3.7 of this report and found it acceptable. Since the AMS is a non-safety system, IEEE 603, criterion is not a requirement for the AMS. Therefore, the NRC staff performed a general review of the AMS. The NRC staff finds that the AMS attributes identified in Section 7.5.9.2 of this report, in combination with the implementation of the digital system guidelines and self-test provisions in Items (2) and (5) below, support adequate redundancy, diversity, testability, and quality.

DCD, Tier 2, Section 7.1.6.3, indicates that there are no alarms that require manually controlled actions for safety systems to accomplish their function. Accordingly the NRC staff concurs with the applicant that the requirements for manually controlled safety equipment and circuits are not applicable.

DCD, Tier 2, Section 7.1.5.4, describes the testability of the N-DCIS, which includes the annunciator systems. The N-DCIS controllers are equipped with online diagnostic capabilities for cyclically monitoring the operability of input/output (I/O) signals, buses, power supplies, processors, and interprocessor communications and that the online diagnostics are performed without interrupting the normal operation of the N-DCIS. The staff finds these testability features acceptable for non-safety systems since online diagnostic equipment is routinely applied for such applications.

The applicant has described an integrated development process that is confirmed by ITAAC to ensure that the annunciator systems have the necessary reliability and functionality. The MCR, including the annunciator systems, is designed using the HFE design process as described in DCD, Tier 2, Chapter 18, and evaluated in Chapter 18 of this report. DCD, Tier 1, Section 3.3, includes the DAC/ITAAC for implementing the HFE design process, which includes the design and verification of controls and information displays for monitoring variables and systems in the control room. The software for the MCR, including the annunciator systems, is developed using the software development activities described in NEDE-33226P and NEDE-33245P. DCD, Tier 1, Section 3.2, includes the DAC/ITAAC to confirm that the completion of these activities and products conforms to the processes described in NEDE-33226P and NEDE-33245P and the guidelines of BTP HCIB-14. Section 7.1.2.3.7 of this report provides the staff evaluation of the development process for software for non-safety systems, which includes the annunciator systems. Based on the above, the NRC staff finds that the reliability guidelines have been adequately addressed.

(2) Use of Digital Systems

The software development activities are described in NEDE-33226P and NEDE-33245P. DCD, Tier 1, Section 3.2, includes the DAC/ITAAC to confirm that the completion of these activities and products conforms to the processes described in NEDE-33226P and NEDE-33245P and the guidelines of BTP HCIB-14. The NRC staff evaluation of software development activities is provided in Section 7.1.2 of this report. As described in Item (1) above, these software development activities are applicable to the MCR and its alarms. Accordingly, based on the applicability of the software development activities to the annunciator system and the confirmation of their implementation in the DAC/ITAAC, the NRC staff finds that the use of digital systems guidelines has been adequately addressed.

(3) Independence (IEEE Std 603, Sections 5.6 and 6.3)

SRP Section 7.5 notes that the annunciator systems should be evaluated for isolation between safety systems and other systems in conformance with IEEE Std 603, Sections 5.6 and 6.3. As described in Section 7.1.1.3.10 of this report, which is applicable to the annunciator systems, the NRC staff finds that IEEE Std 603, Sections 5.6 and 6.3, have been adequately addressed based on their inclusion in the safety systems design basis and their confirmation in the DAC/ITAAC. Accordingly, the NRC staff finds that IEEE Std 603, Sections 5.6 and 6.3, have been adequately addressed for annunciator systems.

(4) Redundancy

As described in Item (1) above, DCD, Tier 2, Section 7.1.5.3, indicates that the AMS conforms to the SRM on SECY-93-087, Item II.T, including following the guidance for redundancy, independence, and separation. The NRC staff evaluated conformance to the SRM on SECY-93-087, Item II.T in Section 7.1.1.3.7 of this report and found it acceptable. The AMS has several redundant features, including (1) sending alarm points through dual networks to redundant message processors on dual power supplies, (2) displaying alarms on multiple independent VDUs that each have dual power supplies, (3) driving alarm tiles, or their equivalent, by redundant datalinks (with dual power), and (4) using redundant alarm processors. The MCR, including the alarms, is designed using the HFE design process as described in DCD, Tier 2, Chapter 18, and evaluated in Chapter 18 of this report. DCD, Tier 1, Section 3.3, includes the DAC/ITAAC for implementing the HFE design process, which includes the design and verification of controls and information displays for monitoring variables and systems in the control room. Based on the above, the NRC staff finds that the redundancy guidelines have been adequately addressed.

(5) Self-Test Provisions (BTP HCIB-17)

BTP HCIB-17 provides self-test provisions for safety and protections. Provisions applicable to the non-safety annunciator systems include self-test features and actions upon failure detection. DCD, Tier 2, Section 7.1.5.4, notes that the N-DCIS controllers are equipped with online diagnostic capabilities to identify and isolate failure of I/O signals, buses, power supplies, processors, and interprocessor communications and that these online diagnostics can be performed without interrupting the normal operation of the N-DCIS. Accordingly, the NRC staff finds that the redundancy self-test provisions have been adequately addressed.

(6) Compliance with IEEE Std 603[1991]

SRP Section 7.5 indicates that IEEE Std 603 is applicable where alarms are provided for manually controlled actions for which no automatic control is provided and that are required for the safety systems to accomplish their safety functions. As described in Item (1) above, this is not applicable to the design. The annunciator systems are non-safety and therefore must be isolated from the safety systems. As described in Item (3) above and Section 7.1.1.3.10 of this report, which is applicable to the annunciator systems, the NRC staff finds that Sections 5.6 and 6.3 of IEEE Std 603 have been adequately addressed based on their inclusion in the safety systems design basis and their confirmation in the DAC/ITAAC. Accordingly, the NRC staff finds that compliance with IEEE Std 603 has been adequately addressed for annunciator systems.

The remaining criteria are evaluated in Section 7.5.11 of this report.

7.5.10 Safety Parameter Display System, Emergency Response Facilities Information Systems, and Emergency Response Data System Information Systems

7.5.10.1 Regulatory Criteria

Acceptance criteria for information systems important to safety are based on meeting the relevant requirements of 10 CFR 50.55a(a)(1); 10 CFR 50.55a(h); GDC 1 and 24; and 10 CFR 52.47(b)(1). The acceptance criteria are also based on conforming to the guidelines of IEEE Std 7-4.3.2, as endorsed by RG 1.152.

7.5.10.2 Summary of Technical Information

In DCD, Tier 2, Section 7.1.5.1.2 indicate that the SPDS, the ERF and the ERDS information systems are non-safety and part of the N-DCIS.

7.5.10.3 Evaluation of the Safety Parameter Display System and the Emergency Response Facility and Emergency Response Data System Information Systems Conformance with Acceptance Criteria - Major Design Considerations

Per SRP Section 7.5, the following are the major design considerations that should be emphasized in the SPDS and the ERF and ERDS information systems review:

(1) Independence (IEEE Std 603, Sections 5.6 and 6.3)

DCD, Tier 2, Section 7.1.4.2, states that the SPDS and the ERF and ERDS information systems are non-safety and part of the N-DCIS. SRP Section 7.5 notes that, for the SPDS and the ERF and ERDS information systems isolated from the protection system, the applicable requirements of 10 CFR 50.55a(h) for IEEE Std 603 are Sections 5.6.3 and 6.3. In DCD, Tier 2, Sections 7.1.6.6.1.7 and 7.1.6.6.1.19 both indicate that the safety systems are separated and independent from non-safety systems in conformance with IEEE Std 603, Sections 5.6.3 and 6.3. Section 7.1.1.3.10 of this report provides an evaluation of IEEE Std 603, Sections 5.6.3 and 6.3, that is applicable to the SPDS and the ERF and ERDS information systems. In Section 7.1.1.3.10 of this report, the NRC staff finds that Sections 5.6.3 and 6.3 of IEEE Std 603 are adequately addressed based on their inclusion in the safety systems design basis and their confirmation in the DAC/ITAAC. Accordingly, the NRC staff finds that

Sections 5.6.3 and 6.3 in IEEE Std 603 are adequately addressed for the SPDS and the ERF and ERDS information systems.

The remaining criteria are evaluated in Section 7.5.11 of this report.

7.5.11 General NRC Staff Evaluation of Information Systems Important to Safety

The NRC staff reviewed the applicable regulations for the information systems important to safety in accordance with SRP Sections 7.5 and 7.1-A.

GDC 1 requires quality standards and maintenance of appropriate records.
10 CFR 50.55a(a)(1) requires that structures, systems, and components must be designed, fabricated, erected, constructed, tested, and inspected to quality standards commensurate with the importance of the safety function to be performed. The NRC staff evaluated whether GDC 1 and 10 CFR 50.55a(a)(1) have been adequately addressed for the information systems important to safety per SRP Appendix 7.1-A. SRP Appendix 7.1-A states that the NRC staff review should confirm that the appropriate regulatory guides and endorsed standards are identified as applicable for each I&C system important to safety. The NRC staff evaluation of conformance to RGs and standards for 10 CFR 50.55a(a)(1) and GDC 1 in Section 7.1.1.3.3 and 7.1.1.3.6 of this report is applicable to the information systems important to safety. In RAI 7.5-8, the staff requested the applicant to update references to 10 CFR 52 to be consistent with the changes that became effective on September 27, 2007, For example, DCD, Tier 2, Section 7.5.1.3.1 references are part of the rule that was deleted. RAI 7.5-8 was being tracked as an open item in the SER with open items. In its response, the applicant corrected citations to the revised rule throughout the DCD. The staff determined the response was acceptable since the applicant cites the appropriate portions of the 10 CFR 52. Based on the applicant's response, RAI 7.5-8 is resolved. Based on the review of updated DCD information, the NRC staff finds the DCD has properly addressed RG and IEEE standard compliance. The NRC staff finds that requirements of 10 CFR 50.55a(a)(1) and GDC 1 have been adequately addressed.

10 CFR 50.55a(h) requires compliance with IEEE Std 603-1991 and the correction sheet dated January 30, 1995. The NRC staff evaluated whether the information systems important to safety conform to 10 CFR 50.55a(h) and IEEE Std 603. The NRC staff evaluation of IEEE Std 603 in Section 7.1.1.3.10 of this report is applicable to the information systems important to safety. As described in Sections 7.5.9 and 7.5.10 of the report, for the non-safety annunciator systems, SPDS, and ERF and ERDS information systems, SRP Section 7.5 indicates that the applicable requirements of 10 CFR 50.55a(h) for IEEE Std 603 are Sections 5.6.3 and 6.3. Section 7.1.1.3.10 of this report provides an evaluation of IEEE Std 603, Sections 5.6.3 and 6.3, that is applicable to the non-safety information systems. Based on the review of information documented in DCD, Tier 2, Subsections 7.1.6.6.1.7 and 7.1.6.6.1.19, DCD, Tier 1, Section 2.2.15, Item 10, the NRC staff finds that requirements of IEEE Std 603, Sections 5.6.3 and 6.3, have been adequately addressed.

The NRC staff evaluated whether 10 CFR 50.34(f)(2)(v), (f)(2)(xii), and (f)(2)(xiv) have been adequately addressed for the information systems important to safety. As described in Section 7.1.1.3.4 of this report, the NRC staff evaluated the I&C system design's compliance with 10 CFR 50.34(f)(2)(v), (f)(2)(xii), and (f)(2)(xiv). Based on the review of information documented in DCD, Tier 2, Subsection 7.1.6.6.1, DCD, Tier 1, Table 2.2.15-1, and DCD, Tier 1, Table 2.2.15-2, the NRC staff concludes that IEEE Std 603 requirements have adequately addressed for the information systems important to safety.

The NRC staff evaluated whether 10 CFR 50.34(f)(2), Subparts (v) [I.D.3], (xi) [II.D.3], (xvii) [II.F.1], (xviii) [II.F.2], (xix) [II.F.3], and (xxiv) [II.K.3.23], have been adequately addressed for the PAM instrumentation and CMS. Section 7.1.1.3.4 of this report provides an evaluation of these requirements that is applicable to the PAM instrumentation and CMS. The NRC staff found that 10 CFR 50.34(f)(2) Subparts (v), (xi), (xvii), (xviii), (xix), and (xxiv) have been adequately addressed.

GDC 2 requires design bases for protection against natural phenomena. GDC 4 requires environmental and dynamic effect design bases. The NRC staff evaluated whether GDC 2 and 4 have been adequately addressed for the information systems important to safety. SRP Section 7.2 identifies that GDC 2 and 4 are addressed by the identification of those systems and components for the RPS designed to survive the effects of earthquakes, other natural phenomena, abnormal environments, and missiles in the design bases. SRP Section 7.2 also identifies that GDC 2 and 4 are addressed by the review of the qualification program in DCD, Tier 2, Sections 3.10 and 3.11. DCD, Tier 2, Table 7.1-1 identifies that GDC 2 and 4 are applicable to the information systems important to safety. DCD, Tier 2, Table 3.2-1, identifies that the safety information systems important to safety are designed as seismic Category I systems. In DCD, Tier 2, Sections 3.10 and 3.11 describe the EQ programs for safety electrical and digital I&C equipment, which are evaluated in Chapter 3 of this report. DCD, Tier 1, Table 3.8-1, "ITAAC for Environmental Qualification of Mechanical and Electrical Equipment," Items 1 and 3, include the ITAAC for the applicant to verify the environmental qualification of safety electrical and digital I&C equipment. The evaluation of GDC 2 and GDC 4 in Section 7.1.1.3.6 of this report further addresses these topics and is applicable to the ESF actuation and control systems, VBIF, and all subsystems.

SRP Section 7.5 identifies that the review should verify that the instrumentation provided for monitoring severe accident conditions has been designed to operate in the severe accident environment for which it is intended and over the time span for which it is needed.

As discussed in Section 7.5.2.3 of this report, the NRC staff evaluated whether there was reasonable assurance that accident monitoring instrumentation would perform its intended function in severe accident environments. In NEDO-33201, Table 8.D.2-1 identifies the required functions and associated monitored variables. NEDO-33201, Section 8D.4.6, provides the equipment capability evaluation of the PAM equipment. In Section 19.2.3.3.7 of this report, the NRC staff provides its evaluation of the severe accident equipment survivability analysis and finds that the analysis provides reasonable assurance that the equipment necessary to achieve a controlled, stable plant condition will function over the time span in which it is needed. Accordingly, based on the applicant's identification of EQ programs consistent with the design bases for the information systems important to safety and their verification in the ITAAC, the NRC staff finds that the requirements of GDC 2 and 4 have been adequately addressed.

GDC 13 requires providing instrumentation to monitor variables and systems over their anticipated ranges for normal operation, AOOs, and accident conditions to assure adequate safety. GDC 13 also requires providing appropriate controls to maintain these variables and systems within prescribed operating ranges. GDC 19 requires control room functionality, control room habitability, and remote shutdown capability. The NRC staff evaluated whether GDC 13 and 19 and the SRM on SECY-93-087 have been adequately addressed for the information systems important to safety. The evaluation of GDC 19 is provided in Section 7.1.1.3.6 of this report. SRP Section 7.5 identifies that GDC 13 and GDC 19 are addressed in part by the conformance of the accident monitoring instrumentation to RGs 1.75, 1.97, 1.105 and 1.151. Conformance to RG 1.97 is evaluated in Section 7.5.2.3 of this report and found acceptable.

DCD, Tier 2, Table 7.1-1 documented the conformance to RGs 1.75, 1.105 and 1.151 for information systems important to safety.

SRP Section 7.5 also identifies that GDC 13 and GDC 19 are addressed in part by verifying that (1) the control room annunciator systems are sufficiently reliable to support normal and emergency plant operations, (2) redundant annunciator systems are provided and the independence of these redundant systems complies with the independence requirements of IEEE Std 603, Section 5.6, (3) alarms provided for manually controlled actions for which no automatic control is provided and that are required for the safety systems to accomplish their safety functions comply with the guidance of IEEE Std 603, and (4) the guidance of the SRM on SECY-93-087, Item II.T, is satisfied. The NRC staff evaluated each of these topics in Section 7.5.9.3 of this report and finds them adequately addressed.

SRP Section 7.5 also identifies that GDC 13 and 19 are addressed in part by findings above for individual information systems important to safety. The NRC staff finds that (1) the guidelines of RG 1.97 have been adequately addressed for the PAM instrumentation as described in Section 7.5.2.3 of this report, (2) RG 1.47, scope of indications, and independence have been adequately addressed for BISI for safety systems as described in Section 7.5.8.3 of this report, and (3) reliability, independence, redundancy and the SRM on SECY-93-087, Item II.T, have been adequately addressed as described in Sections 7.5.9.3 and 7.1.1.3.7 of this report.

The findings discussed above and conformance to GDC 13 and 19 are supported by or depend on an identified interrelated process to design and verify the monitoring capability, particularly (1) the inclusion of applicable IEEE Std 603 criteria in the systems design bases, (2) DCD, Tier 1, Section 2.2.15, including the DAC/ITAAC for the applicant to verify conformance to these IEEE Std 603 criteria, (3) DCD, Tier 1, Section 3.7, including performance criteria and ITAAC to confirm that the post accident instrumentation is installed consistent with the selected variables, (4) DCD, Tier 1, Section 3.3, including the DAC/ITAAC to confirm that the HFE design is implemented based on the process described in DCD Chapter 18, (5) the development of software for the MCR, including the alarms, using the software development activities described in NEDE-33226P and NEDE-33245P, and (6) DCD, Tier 1, Section 3.2, including the DAC/ITAAC to confirm that the completion of these activities and products conforms to the processes described in NEDE-33226P and NEDE-33245P and the guidelines of BTP HCIB-14. These verifications are applicable to the information systems important to safety and include verification of the controls for manual initiation of functions necessary to support actions to operate the nuclear power unit safely under normal conditions and to maintain it in a safe condition under accident conditions. Based on the above, the NRC staff concludes that requirements of GDC 13 and 19 have been adequately addressed for the information systems important to safety.

GDC 24 requires that the protection system 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. GDC 24 requires that the interconnection of the protection and control systems be limited so as to assure that safety is not significantly impaired. The NRC staff evaluated whether GDC 24 has been adequately addressed for the information systems important to safety. SRP Appendix 7.1-A notes that GDC 24 is addressed for protection systems by conformance to IEEE Std 603, Sections 5.1, 5.6, 5.12, 6.3, 6.6, and 8, particularly Sections 5.6 and 6.3. DCD, Tier 2, Table 7.1-1, identifies that GDC 24 applies to the information systems important to safety. In DCD, Tier 2, Sections 7.1.6.6.1.7 and 7.1.6.6.1.19

describe conformance with IEEE Std 603, Sections 5.6 and 6.3. IEEE Std 603 ,Sections 5.6 and 6.3, are evaluated in Section 7.1.1.3.10 of this report. DCD, Tier 1, Table 2.2.15-2, includes the DAC/ITAAC for verifying that the applicable I&C systems design was completed in compliance with IEEE Std 603, including Sections 5.6 and 6.3. In addition, SRP Section 7.5 identifies that GDC 24 is addressed in part by the SPDS and the ERF and ERDS information systems, and the non-safety portions of the accident monitoring instrumentation, BISI, and annunciator systems being appropriately isolated from safety systems. The independence or isolation of the SPDS and the ERF and ERDS information systems, BISI, and annunciator systems is evaluated in Sections 7.5.10.3, 7.5.8.3, and 7.5.9.3, and found acceptable. Accordingly, based on their conformance to the applicable guidance and IEEE Std 603 and their verification in the DAC/ITAAC, the NRC staff finds that the requirements of GDC 24 have been adequately addressed.

The NRC staff evaluated whether the requirements of 10 CFR 52.47(b)(1) were met. This regulation requires that the application (for design certification) contain proposed ITAAC that are necessary and sufficient to provide reasonable assurance that, if the ITA are performed and the acceptance criteria are met, a plant that references the design certification has been constructed and will operate in accordance with the design certification, the Atomic Energy Act, and the Commission's rules and regulations. The ITAAC specific to the information systems important to safety are addressed throughout this section and are found to be acceptable. Accordingly, the NRC staff finds that the requirements of 10 CFR 52.47(b)(1) have been adequately addressed.

The NRC staff evaluated whether IEEE Std 7-4.3.2, as endorsed by RG 1.152, has been adequately addressed. SRP Appendix 7.1-D provides guidance on the implementation of IEEE Std 7-4.3.2. In Section 7.1.1.3.10 of this report, the NRC staff evaluated in parallel IEEE Std 7-4.3.2 and IEEE Std 603 using the guidance in SRP Appendix 7.1-D. The NRC staff evaluation of IEEE Std 7-4.3.2 in Section 7.1.1.3.10 of this report is applicable to the information systems important to safety, including the safety PAM instrumentation, CMS, and BISI for safety systems.

7.5.12 Conclusion

Based on the above, the NRC staff concludes that the applicant adequately addresses the major design considerations for the information systems important to safety. As discussed in Sections 7.1.1.3.1 through 7.1.1.3.10 of this report and Sections 7.5.2 through 7.5-11 above, the NRC staff concludes for the information systems important to safety, the applicant adequately addresses the relevant requirements of requirements of 10 CFR 50.55a(a)(1); 10 CFR 50.55a(h); 10 CFR 50.34(f)(2)(v), (f)(2)(xi), (f)(2)(xvii), (f)(2)(xviii), (f)(2)(xix), (f)(2)(xxiv), 10 CFR 52.47(b)(1); GDC 1, 2, 4, 13, 19, and 24. The NRC staff also finds that the information systems important to safety design meets the guidelines of IEEE Std 7-4.3.2 as endorsed by RG 1.152. The applicant has also identified adequate high-level functions and included sufficient DAC/ITAAC in Tier 1 to verify that the important to safety systems design is completed in compliance with the applicable requirements.

7.6 Interlock Logic

7.6.1 Regulatory Criteria

The objective of the review of the interlock logic is to confirm that design considerations such as redundancy, independence, single failures, qualification, bypasses, status indication, and testing

are consistent with the design bases of this logic and commensurate with the importance of the safety functions to be performed.

Acceptance criteria for interlock logic are based on meeting the relevant requirements of 10 CFR 50.55a(a)(1); 10 CFR 50.55a(h); 10 CFR 50.34(f)(2)(v); 10 CFR 52.47(b)(1); and GDC 1, 2, 4, 13, 19, 24, and 25.

7.6.2 Summary of Technical Information

In DCD, Tier 2, Section 7.6, the applicant addressed the high pressure/low pressure (HP/LP) interlock logic. The FAPCS is a low-pressure piping system. It has the following interfaces with the high pressure RWCU/SDC system.

- Its LPCI line is connected to the RWCU/SDC system Loop B discharge line, which is connected to the RPV via the Feedwater Loop A discharge line.

- Crosstie connections are provided from the FAPCS suppression pool suction to the RPV RWCU line to the regenerative heat exchanger (RHX) (RWCU suction) and from the RWCU return line (discharge line to the RPV) to the FAPCS discharge line to the suppression pool, GDCS pools, and containment spray line.

During reactor power operation, the high pressure in the RWCU/SDC system piping exceeds the design pressure of the low-pressure FAPCS piping. The LPCI line isolation valves consist of parallel pairs of air-operated, testable check valves and motor-operated block valves to protect the FAPCS low-pressure piping from overpressurization during reactor power operation. These valves are normally closed. The testable check valves and the motor-operated valves (MOV) are non-safety. Parallel valves are provided for redundancy and fire zone separation. Both sets of parallel valves have identical interlock logic for operation; however, the power supplies for operation of these valves are provided from different sources, the PIP A and PIP B buses, for redundancy and fire zone separation. The logic for operation of the valves is implemented in the PIP A, N-DCIS and PIP B, N-DCIS.

The HP/LP interlock logic prevents the isolation valves from opening, and closes them if opened, whenever there is a high pressure signal from the RPV pressure transmitters of the NBS. The high pressure signal also prevents testing of the air-operated testable check valves and closes them if they are open for testing. It also prevents the operation of the LPCI mode of the FAPCS. The FAPCS modes are described in DCD, Tier 2, Section 9.1.3.2. An SRV is provided upstream of the LPCI line check valves to protect against overpressurization of the pipe by leakage through the check valves. The relief valve discharge line is monitored to detect any leakage through the check valves. The crosstie from the FAPCS to the RWCU/SDC system is used only following a LOCA. These connections allow the RWCU/SDC system to provide containment cooling after a LOCA to bring the plant to a cold shutdown. Each FAPCS to RWCU/SDC system crosstie connection is isolated with a spectacle flange, a check valve, and an MOV providing a positive isolation. The flange removal and the operation of the crosstie are under administrative control.

The power supplies for non-safety pressure instruments, logic, and solenoids (for operation of testable check valves) are provided by the PIP A and PIP B. The power supplies for operation of the LPCI line's non-safety, motor-operated parallel valves are provided from different sources, the PIP A and PIP B buses, for redundancy and fire zone separation. These non-safety power supplies are backed up by non-safety batteries and diesel generators.

The high reactor pressure signals from the NBS processed in the N-DCIS are used to determine whether a high pressure condition exists in the RWCU/SDC discharge line to the RPV feedwater inlet line. If a high pressure condition exists the interlock logic sends a signal to close the MOV. This signal also prevents testing of the check valves and prevents the LPCI mode of operation of the FAPCS.

7.6.3 NRC Staff Evaluation

DCD, Tier 2, Section 7.6, includes one interlock to prevent overpressurization of low-pressure systems. DCD, Tier 2, Section 7.6, does not include any of the four other interlocks identified in SRP Section 7.6. In RAIs 7.6-1 and 7.6-2, the NRC staff requested that DCD, Tier 2, Section 7.6, include all interlock logic important to safety, in particular, interlock logic to isolate safety systems from non-safety systems. The RAI responses describe the basis for the one interlock logic and the design feature that has built-in interlock provisions within the Q-DCIS platform design, which the NRC staff found acceptable. Accordingly, this evaluation only addresses the acceptance criteria for an interlock logic to prevent overpressurization of low-pressure systems. Based on the applicant's responses RAIs 7.6-1 and 7.6-2 are resolved.

In DCD, Tier 2, Section 7.6.1.3, the applicant states that there is no HP/LP interface involving safety systems. There is a non-safety HP/LP interface involving the low-pressure FAPCS LPCI line, which interfaces with a high pressure condition in the RWCU/SDC system piping. The RWCU/SDC system piping interfaces with the feedwater line, which maintains the RCPB.

The FAPCS HP/LP interlock logic prevents the opening of the isolation valves on the LPCI discharge line. The interlock logic prohibits the LPCI line isolation valves from being opened whenever the reactor pressure is greater than the reactor pressure permissive setpoint for the interlock logic, thereby protecting the low-pressure FAPCS piping from overpressurization during reactor power operation. The interlock logic is designed to permit LPCI mode initiation when the reactor pressure is below its reactor pressure permissive setpoint allowing the operator to manually open either isolation valve. The interlock logic operates automatically, and its status is provided to the reactor operator in the MCR and the RSS panels.

The LPCI line provides a path to bring in fire water/suppression pool water for reactor shutdown cooling 72 hours after a DBE, if the normal shutdown cooling system is not available. Therefore, the HP/LP interlock logic is non-safety and within the scope of RTNSS. However, the NRC staff finds this item is not included in DCD Chapter 19, Appendix A on RTNSS systems. In RAI 7.6-3, the staff requested the applicant to document this HP/LP interlock logic in DCD Chapter 19, Appendix A. RAI 7.6-3 was being tracked as an open item in the SER with open items. In its response, the applicant stated that the interlock logic exists to protect low pressure piping, but the protection of low pressure piping is not required to meet RTNSS criteria as specified in DCD, Tier 2, Chapter 19 Appendix A. Section 7.6.1.3, Safety Evaluation, was revised to delete references to RTNSS treatment of the "HP/LP Interlock logic." The interlock logic functions are embedded in the DCIS logic such that there is no separate interlock logic. DCD, Tier 2, Sections 7.1.3.2.5, 7.1.6.5, and 7.6 were revised to remove references to the "Interlock System" and replaced them with "Interlock Logic." The staff determined the response was acceptable since the applicant clarified the HP/LP interlock logic and incorporated it into DCD Revision 6. Base on the applicant's response, RAI 7.6-3 resolved.

10 CFR 50.55a(a)(1) requires that structures, systems, and components must be designed, fabricated, erected, constructed, tested, and inspected to quality standards commensurate with

the importance of the safety function to be performed. SRP Appendix 7.1-A states that the applicant should commit to conformance with the RGs, codes and standards referenced in SRP Sections 7.1 through 7.9, applicable BTPs, and SRP Appendix 7-A. With regard to 10 CFR 50.55a(a)(1) conformance, the DCD, Tier 2, Section 7.6.1.3.1 states that the HP/LP interlock logic is non-safety-related. DCD, Tier 2, Section 7.6.1.3 describes the basis for the HP/LP interlock logic being non-safety-related. The testable check valves provide pressure boundary integrity for the RWCU/SDC system. The motor-operated, normally closed, fail-as-is gate valves provide defense-in-depth protection against any leakage passing through the check valves. A safety relief valve is provided upstream of the testable check valves to protect against over-pressurization of the pipe by leakage through the check valves. Based on the HP/LP interlock logic being applied to non-safety-related valves, the NRC staff concurs that the HP/LP interlock logic is non-safety-related.

DCD, Tier 2, Section 7.1.4.4, provides the N-DCIS regulatory requirements conformance summary and DCD, Tier 2, Section 7.1.6, Table 7.1-1, further describes conformance to applicable portions of the regulations. DCD, Tier 2, Table 7.1-1, indicates conformance with 10 CFR 50.55a(a)(1) for network segments PIP A, N-DCIS and PIP B, N-DCIS that implement the HP/LP interlock logic. While DCD, Tier 2, Tables 7.1-1, specifies conformances to some but not all of the RGs identified in SRP Appendix 7.1-A, the NRC staff finds that DCD, Tier 2,Table 7.1-1, specifies conformance to the RGs applicable to HP/LP interlock logic. The NRC staff finds compliance in the design with 10 CFR 50.55a(a)(1) has been adequately addressed for the HP/LP interlock logic.

10 CFR 50.55a(h) requires compliance with IEEE Std 603-1991 and the correction sheet dated January 30, 1995. With regard to 10 CFR 50.55a(h) compliance with IEEE Std 603, DCD, Tier 2, Section 7.6.1.3.1 states that the HP/LP interlock logic is non-safety-related and thus 10 CFR 50.55a(a)(1) is not applicable to the HP/LP interlock logic. As described in the evaluation of 10 CFR 50.55a(a)(1) above, the NRC staff concurs that the HP/LP interlock logic is non-safety-related and 10 CFR 50.55a(h) is not applicable to the HP/LP interlock logic. Although 10 CFR 50.55a(h) and IEEE Std 603 are not applicable to this system, each of the parallel air-operated testable check valves and each of the parallel MOV is powered from either the PIP A or PIP B bus. Similarly, the interlock logic is implemented in the PIP A or PIP B providing separation and isolation, both mechanically and electrically. The NRC staff finds this acceptable.

GDC 2 requires design bases for protection against natural phenomena. GDC 4 requires environmental and dynamic effect design bases. The NRC staff evaluated whether GDC 2 and 4 have been adequately addressed for the HP/LP interlock logic. DCD, Tier 2, Table 7.1-1 identifies that GDC 2 and 4 are applicable to the Q-DCIS and the N-DCIS. In DCD, Tier 2, Sections 7.6 states that the HP/LP interlock logic is classified as non-safety equipment and qualified to the environmental conditions existing at the location of the devices. The evaluation of GDC 2 and GDC 4 in Section 7.1.1.3.6 of this report further addresses these topics applicable to the N-DCIS. Accordingly, based on the applicant's identification of EQ programs consistent with the design bases for the interlock logic, the NRC staff finds that the requirements of GDC 2 and 4 have been adequately addressed.

GDC 13 requires providing instrumentation to monitor variables and systems over their anticipated ranges for normal operation, AOOs, and accident conditions to assure adequate safety. GDC 13 also requires providing appropriate controls to maintain these variables and systems within prescribed operating ranges. GDC 19 requires control room functionality, control room habitability, and remote shutdown capability. The NRC staff evaluated whether GDC 13

and 19 have been adequately addressed for the HP/LP interlock logic. The evaluation of GDC19 is provided in Section 7.1.1.3.6 of this report. DCD, Tier 2, Section 7.6 describes the monitoring capability and controls for the HP/LP interlock logic, The interlock logic operates automatically, and its status is provided to the reactor operator in the MCR. The HP/LP interlock logic is designed to permit LPCI mode initiation when the reactor pressure is below its reactor pressure permissive setpoint allowing the operator to manually open either isolation valve. The NRC staff finds these monitoring capabilities and controls acceptable. Based on the review of DCD, Tier 2, Section 7.6 documentation, the NRC staff finds that the requirements of GDC 13 and 19 have been adequately addressed.

GDC 24 requires that the protection system 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. GDC 24 requires that the interconnection of the protection and control systems be limited so as to assure that safety is not significantly impaired. The NRC staff evaluated whether GDC 24 has been adequately addressed for interlock logic. DCD, Tier 2 ,Table 7.1-1 identifies that GDC 24 applies to all I&C systems, including PIP A and B network segments, which contains the HP/LP interlock logic. The staff evaluation of GDC 24 as described in Section 7.1.1.3.6, Item 13 of this report is applicable to the HP/LP interlock logic, Accordingly, the NRC staff finds that the requirements of GDC 24 have been adequately addressed.

10 CFR 50.34(f)(2)(v) [I.D.3] requires an applicant to provide an automatic indication of the bypassed and operable status of the safety systems. With regard to 10 CFR 50.34(f)(2)(v)[I.D.3] conformance, DCD, Tier 2, Section 7.6.1.3.1 states that the HP/LP interlock logic does not have a bypass feature. Since the HP/LP interlock logic cannot be bypassed, the staff finds that 10 CFR 50.34(f)(2)(v) is not applicable.

10 CFR 52.47(b)(1),requires that the application (for design certification) contain proposed ITAAC that are necessary and sufficient to provide reasonable assurance that, if the inspections, tests, and analyses are performed and the acceptance criteria are met, a plant that references the design certification has been constructed and will operate in accordance with the design certification, the Atomic Energy Act, and the Commission's rules and regulations. With regard to 10 CFR 52.47(b)(1), DCD, Tier 2, Section 7.6.1.3.1 states that ITAAC are provided for the I&C systems and equipment in DCD Tier 1. The HP/LP interlock logic is not included in the ITAAC. As described in the evaluation of 10 CFR 50.55a(a)(1) above, the NRC staff concurs that the HP/LP interlock logic is non-safety-related. In addition, the HP/LP interlock logic is not required by any GDC. Based on the above, the NRC staff finds that ITAAC is not needed for the HP/LP interlock logic and the HP/LP interlock logic meets the requirements of 10 CFR 52.47(b)(1)

GDC 25 requires that the protection system be designed to assure that specified acceptable fuel design limits are not exceeded for any single malfunction of the reactivity control systems, such as accidental withdrawal (not ejection or dropout) of control rods. With regard to GDC 25, DCD, Tier 2, Section 7.6.1.3.2 states that because the HP/LP interlock logic does not involve reactivity control, GDC 25 is not applicable. The staff concurs that the HP/LP interlock logic does not involve reactivity control.

7.6.4 Conclusion

As discussed in Section 7.6.3 above, the NRC staff concludes that the HP/LP interlock logic meets the relevant requirements of 10 CFR 50.55a(a)(1); GDC 1, 2, 4, 13, 19, and 24, and 10 CFR 52.47(b)(1). 10 CFR 50.55a(h), 10 CFR 50.34(f)(2)(v) and GDC 25 are not applicable to the HP/LP logic.

7.7 Control Systems

In DCD, Tier 2, Section 7.7, the applicant described I&C systems for normal plant operations that do not perform plant safety functions. However, these systems do control plant processes that have an impact on plant safety and control. This includes the main reactivity control of the nuclear reactor core with the positioning of the control rods, control of feedwater to the RPV, feedwater temperature, and regulation of reactor steam flow and pressure. These systems both can force the actuation of the safety functions and prevent the need for the safety functions to actuate either through normal operation or through inadvertent operation, or various AOOs.

While not directly essential to the safe shutdown and maintenance of the nuclear reactor and plant in a safe condition, these systems must not prevent the safety function from operating when required. Further, the ability of these systems to meet the acceptance criteria also is dependent on quality software and human factors development which are outside the scope of the evaluation in this section. The control systems described in this section include the following:

- NBS(N) – non-safety subsystems
- RC&IS
- FWCS
- PAS
- SB&PC system
- NMS(N) – non-safety subsystems
- CIS

The non-safety instruments and controls of the RC&IS, FWCS, PAS, SB&PC system, NMS(N), and NBS(N) are part of a group of systems that are collectively grouped with the N-DCIS. The controls for the CIS are not part of the N-DCIS, but have direct controls in the MCR. The relationship of these systems with other non-safety systems and with safety systems is indicated in a simplified network functional diagram of the DCIS in DCD, Tier 2, Figure 7.1-1. DCD, Tier 2, Figure 7.1-3, provides a distributed power-sensor diversity diagram. DCD, Tier 2, Figure 7.1-4, provides a hardware/software (architecture) diversity diagram. The N-DCIS is segmented into five parts that can work independently of one another if failures occur as outlined in the DCD, Tier 2, Sections 7.1.4.8 and 7.1.5.2. One of these five segments is the BOP segment that involves Section 7.7 control systems with a single channel of triple-redundant controllers that execute the functions of the SB&PC system, the PAS, and the FWCS and the Feedwater Temperature Control System (FWTCS). The GENE network segment executes the functions of the RC&IS with dual-redundant controllers.

7.7.0.1 Regulatory Criteria

The objective of the review of DCD, Tier 1, Section 2.2, and DCD, Tier 2, Section 7.7, is to confirm that the control systems comply with the regulations by conforming to the applicable acceptance criteria and guidelines, that the controlled variables can be maintained within prescribed operating ranges, and that effects of operation or failure of these systems are bounded by the accident analyses in DCD, Tier 2, Chapter 15.

Acceptance criteria for control systems are based on meeting the relevant requirements described in SRP Section 7.7 as 10 CFR 50.55a(a)(1); 10 CFR 50.55a(h); 10 CFR 50.34(f)(2)(xxii); 10 CFR 52.47(b)(1); and GDC 1, 10, 13, 15, 19, 24, 28, 29, and 44. The acceptance criteria are also based on conforming to the guidelines of the SRM on SECY-93-087. For non-safety control systems evaluated in this section, 10 CFR 50.34(f)(2)(xxii) is identified as an acceptance criteria only for B&W plants and therefore is not applicable to the ESBWR.

7.7.0.2 Common Control System Acceptance Criteria

The NRC staff reviewed the control systems below in accordance with SRP Section 7.7. The NRC staff also used acceptance criteria in SRP Table 7-1, SRP Appendix 7.1-A, and SRP Appendix 7.1-C as directed by SRP Section 7.7. The NRC staff used the regulatory criteria listed in Section 7.7.0.1 of this report as the basis for the review of the control system discussed in DCD, Tier 2, Section 7.7.

These systems are classified as non-safety, since they are not depended on for safe shutdown of the reactor and maintaining it in a safe condition. However, per SRP HCIB-19 they are considered the first echelon of defense in avoiding situations where the safety reactor protection systems must respond. Therefore, this safety evaluation will note the significant features of these control systems that enhance the overall concept of nuclear power plant safety, support D3, and aid in avoidance of spurious actuation.

7.7.0.3 Evaluation of Control Systems Conformance with Common Acceptance Criteria

The control systems of DCD, Tier 2, Section 7.7, are associated with the N-DCIS and share many basic design and safety attributes. This section will evaluate the acceptance criteria that are common to all or nearly all of these control systems. Exceptions, acceptance criteria that apply to a specific control system, or special features that enhance safety will be discussed under the NRC staff evaluation for the applicable section of specific control systems. Per SRP Section 7.7, the following are the major design considerations that should be emphasized in control systems review and the NRC staff evaluation that are common to all the control systems in Section 7.7 unless otherwise indicated.

(1) Design Basis

SRP Section 7.7 states for design bases that the review should confirm that the control systems include the necessary features for manual and automatic control of process variables within prescribed normal operating limits. This acceptance criteria is system dependent and is reviewed under the NRC staff evaluation for the specific control system under Sections 7.7.1 through 7.7.7 of this report.

(2) Safety Classification

SRP Section 7.7 states for safety classification that the review should confirm that the plant accident analysis in Chapter 15 does not rely on the operability of any control system function to assure safety. The NRC staff reviewed DCD, Tier 2, Chapter 15, and verified that Chapter 15 does not rely on DCD, Tier 2, Section 7.7, control systems to assure safety. In particular, none of the AOOs and accidents identified in DCD, Tier 2, Chapter 15, Tables 15.1-5 and 15.1-6, rely on the control systems to scram the reactor and maintain it in a safe condition. As discussed in the specific control system evaluation below, these control systems often are able to help mitigate an event to avoid the reactor trip system from actuating. In addition, DCD, Tier 2, Sections 7.1.6.6.1.7 and 7.1.6.6.1.19, state that the Q-DCIS protection systems are separate and independent from the non-safety control systems, in accordance with GDC 24, and that any failure of non-safety systems does not affect safety systems or prevent them from performing their safety functions. The conformance of the Q-DCIS to GDC-24 is evaluated in Section 7.1.1.3.6 of this report.

In RAIs 7.7-7 and 7.7-8, the staff requested the applicant to clarify the safety classification of the NBS I&C. ESBWR DCD, Tier 2, Revision 5, Section 7.7, described the both safety and non-safety portions of the NBS I&C and the design of the non-safety portion was not clear. RAIs 7.7-7 and 7.7-8 was being tracked as open items in the SER with open items. In its responses, the applicant revised the DCD, Tier 2, Section 7.7 to discuss only the non-safety portions of the NBS I&C and moved the discussions of the safety portions to the applicable DCD, Tier 2, Chapter 7 Sections. The staff determined the responses were acceptable since the applicant clarified the design of the non-safety portion of the NBS I&C. Based on the applicant's response, RAIs 7.7-7 and 7.7-8 are resolved.

Based on the above, the NRC staff finds that the safety classification of "non-safety systems" has been adequately addressed for the NBS(N), RC&IS, FWCS, PAS, SB&PC, NMS(N), and CIS.

(3) Effects of Control System Operation on Accidents

SRP Section 7.7 states that the review of effects of control system operation on accidents should confirm that the safety analysis includes consideration of the effects of both control system action and inaction in assessing the transient response of the plant for accidents and AOOs. This acceptance criteria is system dependent and is reviewed under the NRC staff evaluation for the applicable subsection of Section 7.7 for the specific control system that follow under Sections 7.7.1 through 7.7.7 of this report.

(4) Effects of Control System Failures

SRP Section 7.7 states that the review of effects of control system failures should confirm that the failure of any control system component or any auxiliary supporting system for control systems does not cause plant conditions more severe than those described in the analysis of AOOs in DCD, Tier 2, Chapter 15. This acceptance criteria is system dependent and is reviewed under the NRC staff evaluation for the specific control system under Sections 7.7.1 through 7.7.7 of this report.

(5) Effects of Control System Failures Caused by Accidents

SRP Section 7.7 states that the review should confirm that the consequential effects of AOOs

and accidents do not lead to control system failures that would result in consequences more severe than those described in the analysis in DCD, Tier 2, Chapter 15. This acceptance criteria is system dependent and is reviewed under the NRC staff evaluation for the specific control system under Sections 7.7.1 through 7.7.7 of this report.

(6) Environment Controls in Control Systems

SRP Section 7.7 states that the review should confirm that I&C systems include environmental controls as necessary to protect equipment from environmental extremes.

Environment Controls in Control Systems							
ESBWR Conformance List for Control Systems of DCD, Tier 2, Section 7.7							
RG/GDC	NBS(N)	RC&IS	FWCS	PAS	SB&PC	NMS(N)	CIS
1.89	1	1	1	1	1	1	1
1.97	C	C	C	C	C	C	C
1.100	2	2	2	2	2	2	2
1.151	C		3		4		C
1.180	C,1	C,1	C,1	1	1	C,1	C,1
1.204	C						
1.209	1	1	1	1	1	1	1
GDC 2	C	C	C	C	C	C	C
GDC 4	C	C	C	C	C	C	C
C = Conforms with the RG or GDC indicated for specified control system							
1 = See DCD, Tier 2, Table 3.11-1							
2 = See DCD, Tier 2, Section 3.9 and Section 3.10							
3 = Receives signals from sensors on RPV instrument lines in the NBS(N); 4 = Not applicable, Receives signals from sensors in NBS(N) and other systems; 5 = CIS instrument lines penetrating containment comply							
GDC 2 and GDC 4							

The NRC staff reviewed DCD, Tier 2, Sections 7.7, 3.9, 3.10, and 3.11, and Table 3.11-1, to identify environmental controls for the control systems of DCD, Tier 2, Section 7.7. DCD, Tier 2, Section 7.7.1.3, states that the NBS(N) instruments are designed to operate under normal and peak operating conditions of system pressure and at ambient pressures and temperatures. Based on the conformance to the RGs and GDC as noted in the table above, the NRC staff finds conformance to environmental controls adequately addressed for the NBS(N), RC&IS, FWCS, PAS, SB&PC, NMS(N), and CIS.

(7) Use of Digital Systems

SRP Section 7.7 states that control system software should be developed using a structured process similar to that applied to safety system software. In Section 7.1.2.3.7 of this report, the NRC staff finds that NEDE-33226P and NEDE-33245P provide a structured process for developing control system software that is appropriately tailored for safety systems and the important non-safety systems of DCD, Tier 2, Section 7.7 and therefore is acceptable. Accordingly the NRC staff finds that the use of digital systems for the control systems evaluated throughout Section 7.7 of this report, including the NBS(N), RC&IS, FWCS, PAS, SB&PC, NMS(N), and CIS, has been adequately addressed.

(8) Independence

See discussion of IEEE Std 603-1991 under Item (2) of Section 7.7.0.4 of this report below.

(9) Diversity and Defense-in-Depth

SRP Section 7.7 states that control system elements credited in the D3 analysis should be reviewed using the criteria for the DPS described in SRP Section 7.8. In RAI 7.7-11, the NRC staff requested that the applicant clarify which non-safety systems perform diverse functions. In response, the applicant revised the DCD to state in DCD, Tier 2, Section 7.1.6.3, that the digital I&C systems are designed for high reliability to minimize the potential for CCFs, by applying principles of D3. Further, DCD, Tier 2, Section 7.1.5.3, states the non-safety portions of the systems that conform to the SRM on SECY-93-087, Item II.Q and BTP HICB-19, are discussed in DCD, Tier 2, Section 7.8, and the NRC staff evaluated this topic in Section 7.8 of this report. The applicant addressed D3 in NEDO-33251 and this document was evaluated by the NRC staff in Section 7.1.3.3 of this report. The NRC staff confirmed the changes were incorporated into DCD Revision 6. The staff determined the response was acceptable since the applicant clarified which non-safety systems perform diverse functions. Based on the applicant's response, RAI 7.7-11 is closed. Further, features that contribute to D3 are discussed in the sections for specific control systems.

(10) Potential for Inadvertent Actuation

SRP section 7.7 states that the control systems design should limit the potential for inadvertent actuation and challenges to safety systems. The NRC staff reviewed control systems of DCD, Tier 2, Section 7.7, to identify design measures that limit the potential for inadvertent actuation. Any examples of such design features are discussed for specific control systems that follows under Sections 7.7.1 through 7.7.7 of this report.

(11) Control of Access

SRP Section 7.7 states that physical and electronic access to digital computer-based control system software and data should be controlled to prevent changes by unauthorized personnel. SRP Section 7.7 further states that the control should address access via network connections and via maintenance equipment. In RAI 7.7-13, the NRC staff requested that the applicant clarify the access controls for control systems. In response, the applicant revised DCD, Tier 2, Subsection 7.1.5.1.2, to specifically provide key-locked control equipment cabinet doors including position switches and electronic protection of control systems including password protection. The NRC staff the changes were incorporated into DCD Revision 6. The staff determined the response was acceptable since the applicant clarified the access controls for control systems. Based on the applicant's response, RAI 7.7-13 is resolved. This is applicable to the control systems evaluated throughout Section 7.7 of this report: NBS(N), RC&IS, FWCS, PAS, SB&PC, NMS(N), and CIS.

7.7.0.4 Evaluation of Control Systems Common Compliance with Regulations

These control systems associated with the N-DCIS share many basic design and quality attributes that contribute to a safer plant. This section will evaluate the compliance with regulations that are common to all or nearly all of these control systems. Exceptions, conformance with regulations that only apply to a specific control system, or special features that enhance plant safety are reviewed under the NRC staff evaluation for the specific control

system under Sections 7.7.1 through 7.7.7 of this report.

Per SRP Section 7.7, the following are the regulations that must be met by all control systems in DCD, Tier 2, Section 7.7 unless otherwise indicated.

(1) Compliance with 10 CFR 50.55a(a)(1)

Regulation 10 CFR 50.55a(a)(1) states, "Structures, systems, and components must be designed, fabricated, erected, constructed, tested, and inspected to quality standards commensurate with the importance of the safety function to be performed." SRP Appendix 7.1-A states that the applicant should commit to conformance with the RGs, codes and standards referenced in SRP Sections 7.1 through 7.9, applicable BTPs, and SRP Appendix 7-A. SRP Appendix 7.1-A further states that the design should conform to all RGs and industry standards committed to by the applicant and that 10 CFR 50.55a(a)(1) applies to all (safety and non-safety) I&C systems including NBS(N), RC&IS, FWCS, PAS, SB&PC, NMS(N), and CIS.

DCD, Tier 2, Section 7.1.4.4, provides the N-DCIS regulatory requirements conformance summary and DCD, Tier 2, Section 7.1.6, Table 7.1-1, further describes conformance to applicable portions of the regulations. DCD, Tier 2, Table 7.1-1, indicates conformance with 10 CFR 50.55a(a)(1) for network segments for GENE and BOP that support and interface with the control systems of DCD, Tier 2, Section 7.7. The applicant's safety evaluation for each of the control systems of DCD, Tier 2, Section 7.7, indicates compliance with 10 CFR 50.55a(a)(1) by conformance and use of the applicable standards. While DCD, Tier 2, Tables 7.1-1, specifies conformances to some but not all of the RGs identified in SRP Appendix 7.1-A, the NRC staff finds that DCD, Tier 2,Table 7.1-1, specifies conformance to the RGs applicable to these non-safety systems. The NRC staff finds compliance in the design with 10 CFR 50.55a(a)(1) has been adequately addressed for NBS(N), RC&IS, FWCS, PAS, SB&PC, NMS(N), and CIS.

(2) Compliance with 10 CFR 50.55a(h) Requiring Conformance to IEEE Std 603-1991

10 CFR 50.55a(h) requires compliance with IEEE Std 603-1991 and the correction sheet dated January 30, 1995. SRP Appendix 7.1-A states that for non-safety systems isolated from safety systems the applicable requirement of 10 CFR 50.55a(h) for IEEE Std 603-1991 is Section 5.6.3, "Independence Between Safety Systems and Other Systems." SRP Table 7.1 indicates that the requirement to provide separation between protection and control functions (Sections 5.6.3 and 6.3.1) apply to all I&C systems. DCD, Tier 2, Table 7.1-1, indicates conformance with 10 CFR 50.55a(h) for network segments for GENE and BOP that support and interface with the control systems of DCD, Tier 2, Section 7.7. The applicant's safety evaluation for each of the control systems of DCD, Tier 2, Section 7.7, indicates compliance with 10 CFR 50.55a(a)(1). Section 7.1.1.3.10 of this report provides an evaluation of IEEE Std 603, Sections 5.6 and 6.3, that is applicable to the control systems. In Section 7.1.1.3.10 of this report, the NRC staff found that Sections 5.6 and 6.3 of IEEE Std 603 have been adequately addressed based on their inclusion in the safety systems design basis and their confirmation in the DAC/ITAAC. Accordingly, the NRC staff finds that the requirements of 10 CFR 50.55a(h) are adequately addressed for the DCD, Tier 2, Section 7.7, control systems NBS(N), RC&IS, FWCS, PAS, SB&PC, NMS(N), and CIS.

(3) Compliance with 10 CFR 52.47(b)(1)

This regulation requires that the application for design certification contain proposed ITAAC that are necessary and sufficient to provide reasonable assurance that, if the ITAAC are performed and the acceptance criteria are met, a plant that references the design certification has been constructed and will operate in accordance with the design certification, the Atomic Energy Act, and the Commission's rules and regulations. Compliance with this regulation and the identification of the DCD Tier ITAAC is reviewed under the NRC staff evaluation for the specific control system under Sections 7.7.1 through 7.7.7 of this report.

(4) Compliance with 10 CFR Part 50, Appendix A, GDC 1, 10, 13, 15, 19, 24, 28, 29, and 44

ESBWR GDC Conformance List for Control Systems of DCD, Tier 2, Section 7.7							
GDC	NBS(N)	RC&IS	FWCS	PAS	SB&PC	NMS(N)	CIS
1 R	C	C	C	C	C	C	C
2	C	C	C	C	C	C	C
4	C	C	C	C	C	C	C
10 R							
12		C				C	
13 R	C	C	C	C	C	C	C
15 R							
19 R	C	C	C	C	C	C	C
20	C						
21	C						
22	C						
23	C						
24 R	C	C	C	C	C	C	C
25						C	
26						C	
27						C	
28 R		C				C	
29 R		C				C	
41							C
42							C
43							C
44 R							
Note: C = Conforms per DCD; R = Required by SRP Section 7.7 (if applicable)							

GDC 1 requires quality standards and maintenance of appropriate records. SRP Appendix-7.1-A states that the applicant should commit to conformance with the applicable RGs, codes and standards referenced in SRP Sections 7.1 through 7.9, the BTPs, and SRP Appendix 7-A. DCD, Tier 2, Table 7.1-1 indicates conformance with GDC 1 for network segments for GENE and BOP that support and interface with the control systems of DCD, Tier 2, Section 7.7. In RAI 7.7.14, the NRC staff requested that the applicant clarify conformance to GDC 1 for control systems. RAI 7.7-14 was being tracked as an open item in the SER with open items. In its response, the applicant indicated that it would revise the safety evaluation for each of the control systems of DCD, Tier 2, Section 7.7, to indicate compliance with GDC 1 by conformance and use of the applicable industry standards. The NRC staff confirmed the applicant incorporated these changes into DCD Revision 6. The NRC staff

determined the response was acceptable since the applicant clarified the conformance to GDC 1 for control systems. Based on the applicant's response, RAI 7.7-14 is resolved. While DCD, Tier 2, Table 7.1-1, specifies conformances to some, but not all of the RGs identified in SRP Appendix 7.1-A, the NRC staff finds that DCD, Tier 2, Table 7.1-1, specifies conformance to RGs applicable to these non-safety systems. The NRC staff finds compliance in the design with GDC 1 has been adequately addressed for NBS(N), RC&IS, FWCS, PAS, SB&PC, NMS(N), and CIS.

GDC 10 requires that the reactor core, associated coolant, control, and protection systems 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. GDC 10 will be addressed in the evaluation for each control system in sections 7.7.1 through 7.7.7 of this report.
GDC 13 requires providing instrumentation to monitor variables and systems over their anticipated ranges for normal operation, AOOs, and accident conditions to assure adequate safety. GDC 13 also requires providing appropriate controls to maintain these variables and systems within prescribed operating ranges. GDC 13 will be addressed in the evaluation for each control system in sections 7.7.1 through 7.7.7 of this report.

GDC 15 requires that the reactor coolant system and associated auxiliary, control, and protection systems be designed with sufficient margin to ensure that the design conditions of the RCPB are not exceeded during any condition of normal operation, including AOOs. GDC 15 will be addressed in the evaluation for each control system in sections 7.7.1 through 7.7.7 of this report.

GDC 19 requires 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. GDC 19 will be addressed in the evaluation for each control system in sections 7.7.1 through 7.7.7 of this report.

GDC 24 requires that the protection system 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. GDC 24 requires that the interconnection of the protection and control systems be limited so as to assure that safety is not significantly impaired. SRP Table 7.1 indicates GDC 24 applies to all control systems. The NRC staff evaluated whether the GDC 24 is adequately addressed for the N-DCIS control systems. DCD, Tier 2, Sections 7.1.6.6.1.7 and 7.1.6.6.1.19, describe conformance with IEEE Std 603, Sections 5.6 and 6.3. These sections state that the Q-DCIS protection systems are separate and independent from the non-safety control systems, in accordance with GDC 24, and that any failure of non-safety systems does not affect safety systems or prevent them from performing their safety functions. IEEE Std 603, Sections 5.6 and 6.3 are evaluated in Section 7.1.1.3.10 of this report, where the NRC staff finds that Sections 5.6 and 6.3 are adequately addressed based on their inclusion in the Q-DCIS design basis and their verification in the DAC/ITAAC. Accordingly, based on the appropriate isolation of the control systems from the safety systems and the inclusion of IEEE Std 603, Sections 5.6 and 6.3, in the design basis for the Q-DCIS and their verification in the DAC/ITAAC, the NRC staff finds that the requirements of GDC 24 have been adequately addressed for N-DCIS control systems (NBS(N), RC&IS, FWCS, PAS, SB&PC, NMS(N), and CIS).

GDC 28 requires that 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 RCPB 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. GDC 28 will be addressed in the evaluation for each control system in sections 7.7.1 through 7.7.7 of this report.

GDC 29 requires that protection and reactivity control systems shall be designed to assure an extremely high probability of accomplishing their safety functions in the event of AOOs. GDC 29 will be addressed in the evaluation for each control system in sections 7.7.1 through 7.7.7 of this report.

GDC 44 requires a system be provided to transfer heat from structures, systems, and components important to safety, to an ultimate heat sink. As described in Section 7.1.1.3.6 of this report, the NRC staff finds that GDC 44 is not directly applicable to the control systems of DCD, Tier 2, Section 7.7.

7.7.1 The Nuclear Boiler System Instrumentation and Control - (Nonsafety Subsystems)

7.7.1.1 Summary of Technical Information

The NBS(N) provides the monitoring and control input for important nuclear reactor related variables during normal plant operating modes and during the plant response to accidents. The NBS sensors used for safety system actuation and control functions are addressed in other sections within this chapter. This section describes the NBS(N) used for indication, actuation, and control of non-safety systems.

The NBS(N) provides RPV water level and dome pressure measurements over the ranges and to the accuracies necessary for adequate operator monitoring of RPV water level during normal, transient, and accident conditions.

The NBS(N) provides indication of the following parameters in support of normal plant operations and power generation as well as during AOOs and events as needed:

- Reactor coolant and RPV temperatures
- RPV water level
  - shutdown range
  - narrow range
  - wide range
  - fuel zone range
- RPV pressure
- SRV discharge line temperature
- Main steam flow rate

The NBS(N) design provides for periodic calibration and testing of the NBS(N) instrumentation during plant operation. Non-safety instruments are powered from the non-safety instrument power supply buses.

The NBS(N) provides the following measurement and monitoring as discussed in DCD, Tier 2, Section 7.7.1.2.2:

(1) Reactor Coolant and Reactor Pressure System Vessel Temperature Monitoring

The reactor coolant temperatures are measured at the mid-vessel inlet to the RWCU/SDC system and at the bottom head drain. Coolant temperature is also determined in the steam-filled parts of the RPV and steam-water mixture by measuring the reactor pressure. In the saturated system, reactor pressure connotes saturation temperature. Core inlet temperature can normally be measured by the redundant core inlet temperature sensors located in each LPRM assembly below the core plate elevation.

The RPV outside surface temperature is measured at the head flange and at the bottom head locations.

(2) Reactor Pressure Vessel Water Level

The reactor pressure vessel water level instruments are differential pressure devices calibrated for the specific vessel pressure and liquid temperature conditions. The method of water level measurement is the condensing chamber reference leg type and uses differential pressure devices as its primary elements. The reactor water level measurement is temperature compensated through the thermocouples installed on the sensing line. Reactor water level instrumentation is used to (1) provide signal input to the FWCS and (2) provide signal inputs for DPS functions as discussed in DCD, Tier 2, Section 7.8.1. Figure 7.7-1 provides a diagram indicating the range and RPV tap points.

- The shutdown range water level instrumentation is used to monitor the RPV water level during shutdown conditions when the head is removed and the reactor system may be flooded for refueling or maintenance.

- The narrow-range water level instrumentation is used to monitor the RPV water level for use with the FWCS for normal operation and abnormal events.

- The wide-range water level instrumentation is used for safety and non-safety applications and for the DPS, and is provided for the range of normal, transient, and accident conditions. The wide-range water level measurement has its own separate sensors and indicators.

- The fuel zone range water level instrumentation is provided for PAM in which the water level may be substantially below the normal range. The maximum point limit uses the RPV taps near the top of the steam outlet nozzle. The fuel zone range water level measurement has its own separate sensors and indicators .

(3) Reactor Pressure Vessel Pressure

Pressure transmitters detect RPV pressure from the instrument lines used for measuring RPV water level to provide indication and status in the MCR.

(4) Safety Relief Valve Leak Detection

Thermocouples are located in the discharge pipes of 10 SRVs. The temperature signals are recorded, and temperatures indicative of a leaking SRV are alarmed in the MCR.

(5) Main Steam Flow Rate

Differential pressure transmitters are used to determine the steam flow rate. Pressure taps from the throat of the RPV steam outlet nozzles, in conjunction with the RPV dome pressure taps, measure differential pressure. Differential pressure is proportional to the main steam flow rate and is used for feedwater control.

7.7.1.2 NRC Staff Evaluation

7.7.1.2.1 Evaluation of NBS(N) Conformance with Acceptance Criteria

The major design considerations per SRP Section 7.7 are listed in Section 7.7.0.3 of this report and discuss the attributes that are common to the control systems of DCD, Tier 2, Section 7.7. This section will discuss and evaluate only those major design considerations and information that are unique to the NBS(N).

Design Basis:

DCD, Tier 2, Section 7.7.1.1.2, does not identify any manual or automatic control functions for the NBS(N). The NBS(N) provides indication of the parameters needed in support of normal plant operations. DCD, Tier 2, Section 7.7.1.5, lists these parameters and states they are displayed in the MCR. In addition, the RPV pressure is indicated at four local instrument racks in the reactor building. Based on the above, the NRC staff finds that the design bases have been adequately addressed for the non-safety NBS(N).

Effects of Control System Operation on Accidents:

DCD, Tier 2, Section 7.7.1.1.2, identifies that the NBS(N) does not have any manual or automatic control functions. The NBS(N) is only a monitoring system. The NBS(N) monitors process parameters that are used by the FWCS and SB&PC system and are indicated in the MCR. The effect of NBS(N) action on transients is to continue to provide process information to the FWCS and SB&PC system and also to the MCR, which is acceptable to the NRC staff. The effect of NBS(N) inaction on transients is bounded by NBS(N) failures evaluated below and found to be acceptable. Accordingly, the NRC staff finds that the effects of NBS(N) system operation on accidents has been adequately addressed.

Effects of Control System Failures:

The NBS(N) monitors process parameters that are used by the FWCS and the SB&PC system so NBS(N) failures (including digital, sense, and transmission failures) are bounded by FWCS failures and SB&PC failures, the dominant failure from the FWCS. DCD, Tier 2, Chapter 15, Sections 15.2.4.2, 15.3.1, and 15.3.2, analyze three bounding feedwater control system failures: runout of one feedwater pump, loss of feedwater heater with failures of Select Control Rod Run-in (SCRRI) and Select Rod Insertion (SRI), and feedwater controller failure with maximum flow demand. These failures bound the failures of the FWCS and thus the NBS(N). Further, the applicant stated in DCD, Tier 2, Section 7.7.1.3, that if a line break occurs in a non-safety portion of a sensing line, the excess flow check valve closes to stop the flow of reactor coolant, and if there is a single failure of the excess flow check valve, a restriction orifice limits the flow of

coolant to within acceptable bounds. Accordingly, the NRC staff the finds that NBS(N) system failures do not cause plant conditions more severe than those described in the analysis of AOOs in Chapter 15. In RAI 7.7-12, the NRC staff requested that the applicant provide analyses that evaluate the effects of control systems failures. RAI 7.7-12 was being tracked as an open item in the SER with open items. In response, the applicant stated that since the outputs from the NBS(N) transmitters are used by other systems such as FWCS, references to DCD, Tier 2, Chapter 15, analysis is made from this FWCS systems. The applicant also stated that although credit was not taken for non-safety systems in the safety functions, failure of these non-safety systems does not prevent safe shutdown of the reactor. The applicant revised the DCD, Tier 2, Section 7.7 to reference DCD, Tier 2, Chapter 15 analyses of specific events that evaluate the effects of control systems failures. As discussed above, the expected and abnormal transients and accident events analyzed in DCD, Tier 2, Chapter 15, Sections 15.2.4.2, 15.3.1, and 15.3.2, bound the failure modes associated with the FWCS digital controls and thus failure in the NBS(N). The staff determined the response was acceptable since the applicant identified the DCD, Tier 2, Chapter 15 analyses that bound the failures of the NBS(N). Based on the applicant's response, RAI 7.7-12 regarding the NBS(N) is resolved.

Effects of Control System Failures Caused by Accidents:

A potential effect of an accident on the NBS(N) would be to damage the instrumentation sensing lines in such a manner as to significantly disrupt the NBS(N) output signals to the FWCS or SB&PC system and thus affecting the FWCS or SB&PC system control functions. The use of multiple divisions and independent sense lines significantly reduces the probability of such effects. In the previous section, "Effects of Control System Failures," the NRC staff the finds that NBS(N) system failures do not cause plant conditions more severe than those described in the analysis of AOOs in DCD, Tier 2, Chapter 15. AOOs and accidents do not lead to more severe NBS(N) failures because the applicant assumed maximum failures of the NBS(N) in the Chapter 15 analyses. Based on the above, the NRC staff finds that the effects of NBS(N) system failures caused by accidents have been adequately addressed.

Potential for Inadvertent Actuation:

The NRC staff reviewed DCD Section 7.7.1 to identify design measures that limit the potential for inadvertent actuation. Examples of such design features are as follows:

The NBS(N) is a measurement system for providing information to other systems such as the FWCS and SB&PC system and does not involve actual control of equipment or processes. Thus, the potential for inadvertent activation is reduced compared to a system like FWCS that provides controls. Inadvertent activation could occur based on incorrect information from the NBS(N), but the probability of this occurring is significantly reduced by the use of multiple independent sensors and transmitters through multiple divisions and use of self-test, diagnostics, and parameter value comparison.

The NBS(N) is designed with redundancy so that failure of any single instrument does not result in the loss of level and pressure indication. The RPV water level, main steam flow rate, feedwater flow, and temperature measurement use multiple signals provided by the NBS(N) that are displayed and alarmed in the MCR.

The core inlet temperatures are to be measured by redundant sensors located in each LPRM assembly below the core plate elevation. This provides both redundant measurements, as well as a radial distribution of the core inlet temperatures. As presented earlier, RPV water level is

measured by four physically separate level (differential pressure) transmitters mounted on separate divisional local racks in the safety envelope within the reactor building. Each transmitter is on a separate pair of instrument lines and is associated with a separate RPS electrical division. Each division has its own set of RPV sensing line nozzle connections. Further, there are four ranges of RPV water level instruments. Based on the above the NRC staff finds that the NBS(N) design limits the potential for inadvertent actuation.

7.7.1.2.2 Evaluation of NBS(N) Compliance with Regulations

The common design attributes and methods for complying with the regulations required by SRP Section 7.7 for control systems of DCD, Tier 2, Section 7.7, are listed and discussed in Section 7.7.0.4 of this report. This section will discuss and evaluate only those regulations with unique methods of compliance for the NBS(N).

Compliance with 10 CFR 52.47(b)(1):

The NRC staff evaluated whether the requirements of 10 CFR 52.47(b)(1) are adequately addressed for the NBS(N). DCD, Tier 1, Section 2.2, does not have a specific table of contents entry for the NBS(N). Instead, since the NBS(N) is supplying parameter readings to other systems and is associate with the N-DCIS network, the NBS(N) is considered to be tested and accepted when the ITAAC of the systems requiring the NBS(N) parameter data are completed. The ITAAC for the systems using NBS(N) data are found in DCD, Tier 1, Sections 2.2.3, 2.2.5, 2.2.9, 2.2.11, 2.2.14, and 2.2.15. Based upon the review of DCD, Tier 2, Section 7.7.1, DCD, Tier 1, Sections 2.2.3, 2.2.5, 2.2.9, 2.2.11, 2.2.14, and 2.2.15, and the ITAAC of the systems using NBS(N) data, the NRC staff finds that the requirements of 10 CFR 52.47(b)(1) are adequately addressed for the NBS(N).

Compliance with GDC 10, 13, 15, 19, 28, and 29:

The NRC staff reviewed DCD, Tier 2, Section 7.7.1, to verify that the applicable GDC specified in SRP Section 7.7 have been adequately addressed for the NBS. DCD, Tier 2, Section 7.7.1.3.2, states that the NBS(N) complies with GDC 13 and 19.

GDC 10 requires that the reactor core, associated coolant, control, and protection systems 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. The NRC staff evaluated whether GDC 10 is adequately addressed for the NBS(N). SRP Appendix 7.1-A for GDC 10 states that the NRC staff review should evaluate the I&C system contributions to design margin for reactor core and coolant systems. The applicant does not credit compliance with GDC 10 for the NBS(N). DCD, Tier 2, Section 7.7.1.1.2, identifies that the NBS(N) does not have any manual or automatic control functions. The NBS(N) provides essential measurements of reactor pressure, RPV water level, reactor coolant, RPV temperatures, main steam flow rate, and SRV discharge temperatures. Accordingly, the NRC staff finds that GDC 10 is not applicable to the NBS(N).

GDC 13 requires providing instrumentation to monitor variables and systems over their anticipated ranges for normal operation, AOOs, and accident conditions to assure adequate safety. GDC 13 also requires providing appropriate controls to maintain these variables and systems within prescribed operating ranges. The NRC staff evaluated whether GDC 13 is adequately addressed for the NBS(N). DCD, Tier 2, Section 7.7.1.1.2, identifies that the

NBS(N) does not have any manual or automatic control functions. DCD, Tier 2, Section 7.7.1.3.2, indicates conformance to GDC 13. The NBS(N) provides essential measurements of reactor pressure, RPV water level, reactor coolant and RPV temperatures, main steam flow, and SRV discharge temperatures. Accordingly, based on information reviewed in DCD, Tier 2, Section 7.7.1, and their verification in the ITAAC of systems that receive inputs from the NBS(N), the NRC staff finds that the requirements of GDC 13 have been adequately addressed for the NBS(N).

GDC 15 requires that the reactor coolant system and associated auxiliary, control, and protection systems shall be designed with sufficient margin to ensure that the design conditions of the RCPB are not exceeded during any condition of normal operation, including AOOs. The NRC staff evaluated whether GDC 15 is adequately addressed for the NBS(N). SRP Appendix 7.1-A for GDC 15 states that the NRC staff review should evaluate the I&C system contributions to design margin for reactor coolant systems. The applicant does not credit compliance with GDC 15 for the NBS. DCD, Tier 2, Section 7.7.1.1.2, does not identify any manual or automatic control functions for the NBS(N). The NBS(N) monitors process parameters that are used by the FWCS and SB&PC system and are indicated in the MCR. Since the NBS(N) does not control any parameter that may affect reactor margins, the NRC staff finds that GDC 15 is not applicable to the NBS(N).

GDC 19 requires control room functionality, control room habitability, and remote shutdown capability. The NRC staff evaluated whether GDC 19 is adequately addressed for the NBS(N). In Section 7.1.1.3.6 the NRC staff evaluated that GDC 19 has been adequately addressed with the exception of the operation of specific I&C systems. SRP Appendix 7.1-A states that the review should evaluate if there exists I&C available to operate the nuclear power unit under normal and accident conditions. DCD, Tier 2, Section 7.7.1.3.2, specifies that the NBS(N) conforms to GDC 19. As described in the DCD, Tier 2, Section 7.7.1.5, the process parameters monitored by the NBS(N) are displayed in the MCR. DCD, Tier 2, Section 7.7.1.1.2, identifies that the NBS(N) does not have any manual or automatic control functions. Based on the above, the NRC staff finds that the NBS(N) provides information to permit actions to be taken to operate the plant safely during normal operation and accidents. Accordingly, the NRC staff finds that the requirements of GDC 19 have been adequately addressed for the NBS(N).

GDC 28 requires that reactivity control systems be designed with appropriate limits on the potential amount and rate of reactivity increase. 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. The NRC staff evaluated whether GDC 28 and GDC 29 are adequately addressed for the NBS(N). The NBS(N) monitors process parameters that are used by the FWCS and the SB&PC system and are indicated in the MCR. Accordingly, the NBS(N) is not a reactivity control system and the NRC staff finds that GDC 28 and 29 are not applicable to the NBS(N).

Based on the above, the NRC staff finds that the NBS(N) adequately addresses the relevant regulatory criteria listed in Section 7.7.0.1 above for a non-safety system and that there is reasonable assurance that this system will be able to accomplish its designed function in a reliable manner when built and tested according to DCD Tier 2 and DCD Tier 1 ITAAC.

7.7.1.3 Conclusion

Based on the above, NRC staff concludes there is reasonable assurance that the NBS(N) conforms to the applicable requirements, which include GDC 1, 10, 13, 19, and 24, 10 CFR

52.47(b)(1), 10 CFR 50.55a(a)(1) and 10 CFR 50.55a(h); adequate high level functional requirements are identified; and sufficient ITAAC of systems using the output from the NBS(N) are included in Tier 1 to verify that the design is completed in compliance with the applicable requirements.

7.7.2 Rod Control and Information System

7.7.2.1 Summary of Technical Information

As described in DCD, Tier 2, Section 7.7.2, the main objective of the RC&IS is to control the Fine Motion Control Rod Drive (FMCRD) motors of the CRD system to permit changes in core reactivity so that reactor power level and power distribution can be controlled. The RC&IS obtains status and control rod position information from the CRD FMCRD instrumentation. It sends purge water valve control signals to and obtains status signals from, the HCUs of the CRD system. The RC&IS sends and receives status and control signals to and from other plant systems and RC&IS modules. The RC&IS also monitors and assists in excess feedwater temperature change protection using the ATLM subsystem.

The RC&IS consists of multiple types of cabinets, or panels, that contain special electronic/electrical equipment modules for performing the RC&IS logic in the reactor building and control building. It also includes a dedicated operator interface (DOI) on the main control panel in the MCR. The RC&IS DOI provides summary and status information to the plant operator with respect to control rod positions, FMCRD, RC&IS status, and HCU status. The RC&IS also provides controls for performing normal rod movement functions, bypassing major RC&IS subsystems, performing CRD surveillance tests (except the FMCRD holding brake testing performed during a refueling outage), and resetting RC&IS trips and most abnormal status conditions. A few abnormal status conditions require reset actions at local control panel equipment. DCD, Tier 2, Section 7.7.2.1.2, lists the functions performed by the RC&IS.

There are nine types of electronic/electrical cabinets/panels that perform the logic functions of the RC&IS:

- rods action control subsystem (RACS) cabinet
- remote communication cabinet (RCC)
- induction motor controller cabinet (IMCC)
- rod brake controller cabinet (RBCC)
- emergency rod insertion control panel (ERICP)
- emergency rod insertion panel (ERIP)
- scram time recording panel (STRP)
- scram time recording and analysis panel (STRAP)
- RAPI auxiliary panels

The RC&IS scope includes the following equipment:

- all the electrical/electronic equipment contained in the RACS cabinet, the RCCs, the remote communication cabinets, the IMCCs, the RBCCs, the STRPs, the STRAP, the ERIPs, and the ERICP (Note: RAPI auxiliary panels are designated as part of the N-DCIS)

- the RC&IS multiplexing network equipment

- the cross-channel communication links between equipment located in the RACS cabinets

- the dedicated RC&IS DOI and the communication links from the RACS cabinets to DOI interface

7.7.2.2 NRC Staff Evaluation

7.7.2.2.1 Evaluation of RC&IS Conformance with Acceptance Criteria

The major design considerations per SRP Section 7.7 are listed in Section 7.7.0.3 of this report and discuss the attributes that are common to the control systems of DCD, Tier 2, Section 7.7. This section will discuss and evaluate only those major design considerations and information that are unique to the RC&IS.

Design Basis:

For "Design Basis," the applicant stated in DCD, Tier 2, Section 7.7.2.1.1, that the RC&IS has no functional safety design basis and is designed so that the functional capabilities of safety systems are not inhibited. DCD, Tier 2, Section 7.7.2.1.2, describes the functions performed by the RC&IS including changes to core reactivity through controls that position the control rods in manual, semiautomatic, and automatic modes of operation. Examples of these functions include the (1) scram-follow function, (2) automatic enforcement of rod movement blocks and enforcement of adherence to predetermined rod patterns, (3) manual and automatic insertion of all control rods by an alternate and diverse method, (4) insertion of selected control rods upon SCRRI/SRI command signals from the DPS, (5) enforcement of fuel operating thermal limits, (6) calculation of a reference feedwater temperature used in feedwater temperature rate of change control, and (7) surveillance test support. Further, the RC&IS provides control rod position and FMCRD and RC&IS status summary information through dedicated operator interface in the MCR. Based on the above and the verification of these controls and functions through DCD, Tier 1, Section 2.2.3, ITAAC, the NRC staff finds that the design bases have been adequately addressed for the RC&IS.

Effects of Control System Operation on Accidents:

For "Effects of RC&IS Operation on Accidents," the NRC staff reviewed DCD, Tier 2, Section 7.7.2 and Chapter 15, for effects of the RC&IS operation on accidents. DCD, Tier 2, Section 7.7.2.1.2, describes many operational functions performed by the RC&IS that attempt to prevent or mitigate transients, but a failure of RC&IS does not prevent safe shutdown of the reactor. Examples include the automatic enforcement of rod movement blocks to prevent potentially undesirable rod movements and a possible scram. These blocks do not affect the hydraulic scram insertion function, the scram-follow function, the ARI function, nor the SCRRI function. Further, the RC&IS operation provides automatic, electric motor run-in of all operable control rods, following detection of activation of the hydraulic insertion of the control rods by a reactor scram. The RC&IS inserts selected control rods upon SCRRI/SRI command signals from the DPS. If the feedwater temperature decreases by more than 30 degrees from the reference feedwater temperature calculated by the ATLM, the RC&IS (via the ATLM) provides a feedwater temperature control valve one-way block, rod withdrawal block, and SCRRI/SRI initiation. The NRC staff reviewed DCD, Tier 2, Chapter 15, Tables 15.1-5, 15.1-6, and 15.1-7, that summarize the creditable bounding AOOs, and other events, transients, and accidents.

The SCRRI and SRI are credited in DCD, Tier 2, Table 15.1-5, with assisting in mitigating the following transients: Loss of Feedwater Heating (LOFWH), Generator Load Reject with Bypass, Turbine Trip with Bypass, Generator Load Rejection with a Single Failure in the Bypass System, and Turbine Trip with a Single Failure in the Bypass System. The Rod Block function is credited with assisting in mitigating the transients that involve control rod withdrawal error. Since these RC&IS protective features are automatic, failure of the RC&IS to perform is concluded to be a failure of one or more components or input information as described below. Failure of the RC&IS does not cause plant conditions more severe than those described in the analysis of AOOs in DCD, Tier 2, Chapter 15. Based on the discussions above and below, the NRC staff finds that the safety analysis includes consideration of the effects of both control system action and inaction in assessing the transient response of the plant for accidents and AOOs. The NRC staff finds this acceptable.

Effects of Control System Failures:

For “Effects of RC&IS Failures,” the NRC staff reviewed DCD, Tier 2, Section 7.7.2 and Chapter 15, for effects of the RC&IS failures. The NRC staff verified that the failure of the RC&IS does not cause plant conditions more severe than those described in the analysis of AOOs in DCD, Tier 2, Chapter 15. The failure of the RC&IS is bounded by considering the worst case of failures involving (1) failure of I&C components or failure of input, (2) an operator error in the manual positioning of the control rods, and (3) failure of an RC&IS indication that causes the operator to make an error in manually positioning the control rods.

The consequences of component or system type failures of the RC&IS are limited since the RC&IS directly controls movement of each control rod or rod gang. A failure that results in inadvertent movement of a control rod affects only one control rod or rod gang. The malfunctioning in positioning any single control rod or rod gang does not impair the effectiveness of a reactor scram. Therefore, no single failure in the RC&IS prevents a reactor scram. Repair, adjustment, or maintenance of the RC&IS enforces all rod blocks until the rod block condition is cleared. The applicant stated that the circuitry described for the RC&IS is independent of the circuitry controlling the scram valves. This separation of the scram and normal rod control functions prevents failures in the RC&IS circuitry from affecting the scram circuitry.

Another potential result of the failure of a component or system of the RC&IS could be the failure to send the “signal to initiate” to have the N-DCIS initiate the SCRRI and SRI functions. Such failures of the RC&IS are bounded and discussed in DCD, Tier 2, Chapter 15. Again, unless other systems act as the MRBM or the operators detect and correctly identify the source of a problem with the RC&IS and take mitigating action in time, the RPS acts to protect the reactor from failure of the RC&IS. With regards to manual positioning errors, DCD, Tier 2, Section 7.7.2.2.7.4, lists 16 types of conditions in which either one channel or both channels of the RC&IS logic receives a signal that will cause it to issue a rod block, preventing further rod movement until the situation is corrected. During startup and below the low-power setpoint, the RWM enforces preplanned, analyzed, and preloaded control rod sequences called reference rod pull sequence (RRPS). ATLM protects against exceeding fuel parameter limits on Minimum Critical Power Ratio (MCPR) and Maximum Linear Heat Generation Rate (MLHGR). MRBM subsystem protects against regional high neutron flux. The safety SRNM and APRM of the NBS have rod blocks before reactor trip setpoints are reached. Other protective rod blocks come from I&C hardware or power failures, unacceptable parameter situations such as CRD charging water low pressure, and operational situations such as refueling platform over the core. The RC&IS enforces all rod blocks until the rod block condition is cleared. The bypass

capabilities of the RC&IS permit clearing certain rod block conditions that are caused by failures or problems that exist in only one channel of the logic. With the proper functioning of the RPS, a failure of the RC&IS is controlled.

DCD, Tier 2, Chapter 15, identifies occurrences and events related to RC&IS and control rod movement as listed in DCD Tier 2, Chapter 15, and Tables 15.0-2, 15.1-3, 15.1-5, 15.1-6, and 15.1-7. The NRC staff finds that these occurrences and events are consistent with the NRC staff identified failures of the RC&IS and, therefore, finds that the failure of the RC&IS does not cause plant conditions more severe than those described in DCD, Tier 2, Chapter 15. In RAI 7.7-12, the NRC staff requested that the applicant provide analyses that evaluate the effects of control systems failures. RAI 7.7-12 was being tracked as an open item in the SER with open items. In response, the applicant revised the DCD, Tier 2, Section 7.7 to reference DCD, Tier 2, Chapter 15 analyses of specific events that evaluate the effects of control systems failures. As discussed above, the expected and abnormal transients and accident events analyzed in DCD, Tier 2, Chapter 15, Subsections 15.2.3.1, 15.2.3.2, 15.3.8 and 15.3.9 bound the effects of RC&IS failures. The staff determined the response was acceptable since the applicant identified the DCD, Tier 2, Chapter 15 analyses that bound the failures of the RC&IS. Based on the applicant's response, RAI 7.7-12 regarding the RC&IS is resolved.

Effects of Control System Failures Caused by Accidents:

For "Effects of RC&IS Failures Caused by Accidents," the NRC staff reviewed DCD, Tier 2, Section 7.7.2 and Chapter 15 for effects of the RC&IS system failures caused by accidents. The RC&IS consists of multiple types of cabinets, or panels, that contain special electronic/electrical equipment modules for performing the RC&IS logic in the reactor building and control building. Accidents could potentially damage the sensors and transmitters providing input to the RC&IS as in the NBS(N) system. Fire or earthquake potential could cause one or more functions to fail and damage the electronic equipment causing an RC&IS function to fail. The potential for such effects is significantly reduced through D3 in the RC&IS sensors, the RC&IS EQ, redundant modules in different cabinets, and a fire protection design. Regardless, in the event of failure of the RC&IS, the applicant states in DCD, Tier 2, Section 7.7.2.2.1, that a failure or malfunction of the RC&IS has no effect on the hydraulic scram function of the CRD. The circuitry for normal insertion and withdrawal of control rods in the RC&IS is independent of the RPS circuitry controlling the scram valves. This separation of the RPS scram and the RC&IS normal rod control functions prevents a failure in the RC&IS circuitry from affecting the scram circuitry. RC&IS failures are bounded by the following DCD, Tier 2, Chapter 15 transients from Table 15.1-7: Control Rod Withdrawal Error During Power Operation with ATLM Failures and Control Rod Withdrawal Error During Startup With Failure of Control Rod Block. Based on the above, the NRC staff finds that the consequential effects of AOOs and accidents do not lead to RC&IS failures that would result in consequences more severe than those described in DCD, Tier 2, Chapter 15. Based on the above, the NRC staff finds that the effects of RC&IS failures caused by accidents have been adequately addressed.

Potential for Inadvertent Actuation:

For "Potential for Inadvertent Actuation," the NRC staff reviewed DCD, Tier 2, Section 7.7.2 to identify design measures that limit the potential for inadvertent actuation. Examples of such design features are as follows:

The RC&IS enforces all rod blocks until the rod block condition is cleared. The bypass capabilities of the RC&IS permit clearing certain rod block conditions that are caused by failures

or problems that exist in only one channel of the logic.

The RC&IS uses a dual redundant architecture of two independent channels for normal monitoring of control rod positions and executing normal control rod movement commands. Under normal conditions, each channel receives separate input signals, and both channels perform the same functions. The outputs of the two channels are continuously compared. For normal functions of enforcing and monitoring control rod positions and emergency rod insertion, the outputs of the two channels must agree. Any sustained disagreement between the two channels results in a rod block. However, when the conditions for generating a rod block signal in a single channel are satisfied, that channel alone (independent of the other channel) issues a rod block signal.

The design allows the RC&IS to continue to operate, when practical, in the presence of component hardware failures. This is achieved because the operator is able to reconfigure the operation of the RC&IS through bypass capabilities while the failures are being repaired. No single power source or single power supply failure results in the loss of the RC&IS functions.

Based on the above, the NRC staff finds that RC&IS design limits the potential for inadvertent actuation. The NRC staff notes that the applicant stated in DCD, Tier 2, Section 7.7.2.2.7.5, that the expected reliability is based upon the expected frequency of an inadvertent movement of more than one control rod due to failure. The expected frequency is less than or equal to one inadvertent movement in 100 reactor operating years.

7.7.2.2.2 Evaluation of RC&IS Compliance with Regulations

The common design attributes and methods for complying with the regulations required by SRP Section 7.7 for control systems of DCD, Tier 2, Section 7.7 are listed and discussed in Section 7.7.0.4 of this report. This section will discuss and evaluate only those regulations with unique methods of compliance for the RC&IS.

For “Compliance with 10 CFR 52.47(b)(1),” the NRC staff evaluated whether the requirements of 10 CFR 52.47(b)(1) are adequately addressed for the RC&IS. The NRC staff reviewed DCD, Tier 2, Section 7.7.2, and DCD Tier 1, Section 2.2.1, in accordance with SRP Sections 7.7 and 14.3.5, to verify that 10 CFR 52.47(b)(1) has been adequately addressed for the RC&IS. DCD, Tier 1, Section 2.2.1, documents the RC&IS ITAAC requirements. While RC&IS has no DAC, the RC&IS methods and functions of controlling the control rod positioning, the general equipment and modes of control, and the actuation initiators of protective actions are specified. Accordingly, based on information reviewed in DCD, Tier 1 Section 2.2.1, DCD, Tier 2, Chapter 7 and Section 7.7.2 information discussed herein, and identified RC&IS I&C and their verification in the ITAAC, the NRC staff finds that the requirements of 10 CFR 52.47(b)(1) have been adequately addressed.

For “Compliance with GDC 10, 13, 15, 19, 28, and 29,” the NRC staff reviewed DCD, Tier 2, Section 7.7.3, to verify that the applicable GDC specified in SRP Section 7.7 have been adequately addressed for the RC&IS. DCD, Tier 2, Section 7.7.1.3.2, states that the RC&IS complies with GDC 13 and 19.

GDC 10 requires that the reactor core, associated coolant, control, and protection systems 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. The NRC staff evaluated whether GDC 10 has been adequately addressed for the RC&IS. SRP

Appendix 7.1-A for GDC 10 states that the NRC staff review should evaluate the I&C system contributions to design margin for reactor core and coolant systems. In DCD, Tier 2, Chapter 15, and Tables 15.1-5 and 15.1-6, identify RC&IS actuations and other actions that reduce the need for the actuation of safety systems to mitigate AOOs. DCD, Tier 2, Section 7.7.2.1.2, includes corresponding actions in the power generation (non-safety) design bases of the RC&IS to maintain the reactor core, reactor coolant system, and the reactivity limits within appropriate margins and to mitigate AOOs. Examples of such design features are as follows:

The control rod block functions provide appropriate margin to protect the reactor core by stopping control rod movement before the RPS is required to initiate a scram. The RC&IS mitigates AOOs by inserting selected control rods to counteract the positive reactivity effects of a loss of feedwater heating event or provide needed power reduction after a load reject event or turbine trip. The ATLM, a subsystem of the RC&IS, helps enforce core thermal limits and feedwater temperature rate of decrease. The RWM forces predefined and approved low rod-worth rod patterns during low-power operations. DCD, Tier 1, Section 2.2.1, includes the ITAAC for the applicant to verify that the as-built RC&IS implements these actions. Accordingly, based on identified RC&IS actions and the verification in the ITAAC, the NRC staff finds that the requirements of GDC 10 has been adequately addressed for the RC&IS.

GDC 13 requires providing instrumentation to monitor variables and systems over their anticipated ranges for normal operation, AOOs, and accident conditions to assure adequate safety. GDC 13 also requires providing appropriate controls to maintain these variables and systems within prescribed operating ranges. The NRC staff evaluated whether GDC 13 has been adequately addressed for the RC&IS. DCD, Tier 2, Section 7.7.2, and DCD, Tier 1, Section 2.2.1, identify I&C provided to monitor, control, and maintain the variables over their anticipated ranges for normal operation, for AOOs, and for accident conditions as appropriate to help assure adequate safety. For the RC&IS, these include those parameters and controls that affect reactivity. The NRC staff reviewed the plant transient response to normal load changes and AOOs such as control rod withdrawal, control rod drop accident, and control withdrawal error during refueling. The NRC staff concludes that the RC&IS is capable of maintaining system variables within prescribed operating ranges and capable of contingency actions if such variables reach limiting conditions. Examples of I&C are status data on RC&IS components, FMCRD status, and control rod position data that are collected and provided to other systems. Other examples are the ATLM subsystem that enforces fuel operating limits and feedwater temperature rate of decrease, the RWM subsystem ensuring that patterns of control rods are consistent with specific control rod pattern restrictions as control rod worth, rod block function, and summary information provided by the RC&IS to the DOI in the control room. DCD, Tier 2, Section 7.7.2.3.2, indicates conformance to GDC 13. Accordingly, based on identified RC&IS I&C and the verification in the ITAAC, the NRC staff finds that the requirements of GDC 13 have been adequately addressed for the RC&IS.

GDC 15 requires that the reactor coolant system and associated auxiliary, control, and protection systems shall be designed with sufficient margin to ensure that the design conditions of the RCPB are not exceeded during any condition of normal operation, including AOOs. The NRC staff evaluated whether GDC 15 has been adequately addressed for the RC&IS. SRP Appendix 7.1-A for GDC 15 states that the NRC staff review should evaluate the I&C system contributions to design margin for reactor coolant systems. DCD, Tier 2, Section 7.7.2.3.3, excludes GDC 15 from conformance for the RC&IS. The main purpose of the RC&IS is to provide reactivity control through positioning of the control rods, to control the FMCRD motors of the CRD in positioning the control rods, to provide the rod block function and to provide status

information on the CRD, HCU, and control rod positions. Therefore, the RC&IS does not directly contribute the design margins for the RCPB. Accordingly, GDC 15 is not applicable to RC&IS.

GDC 19 requires control room functionality, control room habitability, and remote shutdown capability. The NRC staff evaluated whether GDC 19 has been adequately addressed for the RC&IS. In Section 7.1.1.3.6 the NRC staff evaluated that GDC 19 has been adequately addressed with the exception of the operation of specific I&C systems. SRP Appendix 7.1-A states that the review should evaluate if there exists I&C available to operate the nuclear power unit under normal and accident conditions. DCD, Tier 2, Section 7.7.2.3.2, specifies that the RC&IS conforms to GDC 19. The features for manual and automatic control described in DCD, Tier 2, Section 7.7.2, and DCD, Tier 1, Section 2.2.1, identify the RC&IS I&C that facilitate the capability to maintain plant variables within prescribed operating limits and over their anticipated ranges for normal operation, for AOOs, and for accident conditions as appropriate to help assure adequate safety. These include examples such as the automatic, semiautomatic, and manual control rod controls described in DCD, Tier 2, Section 7.7.2.2.7. DCD, Tier 2, Section 7.4.2.5, specifies that the parameters displayed and/or controlled from Division 1 and Division 2 in the MCR also are displayed and/or can be controlled from either of the RSS panels. The RSS is evaluated in Section 7.4.3 of this report. Accordingly, based on identified RC&IS I&C and the verification in the ITAAC, the NRC staff finds that the requirements of GDC 19 have been adequately addressed for the RC&IS.

GDC 28 requires that reactivity control systems be designed with appropriate limits on the potential amount and rate of reactivity increase. The NRC staff evaluated whether GDC 28 has been adequately addressed for the RC&IS. SRP Appendix 7.1-A states that GDC 28 imposes functional requirements on I&C interlock and control systems to the extent they are provided to limit reactivity increases to prevent or limit the effect of reactivity accidents. DCD, Tier 2, Section 7.7.2.3.2, specifies that the RC&IS conforms to GDC 28. DCD, Tier 2, Section 7.7.2.1.2, summarizes the functions of the design performed by the RC&IS, including those that specifically address GDC 28 and that reduce the need for the actuation of safety systems to mitigate AOOs. These include the rod block functions (including RWM and ATLM), rod scram testing function, SCRRI and SRI, and the scram follow-function. In particular, DCD, Tier 2, Section 7.7.2.2.7.4, identifies the control rod block functions performed by the RC&IS. If the feedwater temperature decreases by more than 30˚F from the reference feedwater temperature calculated by ATLM, the RC&IS (via ATLM) provides a feedwater temperature control valve one-way block, rod withdrawal block, and SCRRI/SRI initiation. Also, the RC&IS has special bypass features that allow the operator to perform restricted scram time surveillance testing at any power level, but with no effect on the protective functions for ARI, SCRRI, SCRAM-follow condition, or critical rod block functions, such as provided by MRBM, APRM, or SRNM. DCD, Tier 1, Section 2.2.1, includes the ITAAC for the applicant to verify that the as-built RC&IS implements these actions. Accordingly, based on identified RC&IS actions and their verification in the ITAAC, the NRC staff finds that the requirements of GDC 28 have been adequately addressed for the RC&IS.

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. The NRC staff evaluated whether GDC 29 has been adequately addressed. SRP Appendix 7.1-A identifies that GDC 29 is addressed by conformance, as applicable, to GDC 20-25 and GDC 28. Since the RC&IS is a reactivity control system and not a protection system, GDC 20-23 and 25, which are requirements for protection systems, are not applicable to RC&IS, Accordingly, GDC 29 is addressed by conformance as applicable to GDC 24 and 28. DCD, Tier 2, Table 7.1-1

and Section 7.7.2.3.2, specifies that the RC&IS conforms to GDC 29. Conformance of N-DCIS control systems to GDC 24, including the RC&IS, is evaluated in Section 7.7.0.4 of this report. Conformance of the RC&IS to GDC 28 is evaluated above. Based on the requirements of GDC 24 and 28 having been adequately addressed for the RC&IS, the NRC staff finds that the requirements of GDC 29 have been adequately addressed for the RC&IS.

Therefore, the NRC staff finds the RC&IS, adequately addresses the relevant regulatory criteria listed in Section 7.7.0.1 of this report for a non-safety system and that there is reasonable assurance this system will be able to accomplish its designed function in a reliable manner, when built and tested according to DCD Tier 2 and DCD Tier 1 ITAAC.

7.7.2.3 Conclusion

Based on the above, NRC staff concludes there is reasonable assurance that the RC&IS conforms to the applicable requirements, which include GDC 1, 10, 13, 19, 24, 28, and 29, 10 CFR 52.47(b)(1), 10 CFR 50.55a(a)(1) and 10 CFR 50.55a(h); adequate high level functional requirements are identified, and sufficient ITAAC are included in DCD, Tier 1, Section 2.2.1, to verify that the design is completed in compliance with the applicable requirements.

7.7.3 Feedwater Control System

7.7.3.1 Summary of Technical Information

The FWCS, as described in DCD, Tier 2, Section 7.7.3, regulates the flow of feedwater into the RPV to maintain predetermined water level limits during transients and normal plant operating modes and controls the feedwater temperature. The FWCS is a power generation (control) system that maintains proper RPV water level in the operating range from high (Level 8) to low (Level 3). During normal operation, feedwater flow is delivered to the RPV through three reactor feed pumps (RFPs) which operate in parallel. Each RFP is driven by an adjustable-speed induction motor that is controlled by an adjustable speed drive (ASD) circuit. In normal operation, the fourth RFP is in standby mode and starts automatically if any operating feedwater pump trips while at power.

During normal operation the FWCS sends three speed-demand signals, each of which reflects a voted FWCS processor output, to each feed pump ASD. The ASD performs a midvalue vote and uses it to control the speed/frequency of the feed pump motor. The midvalue vote is also returned to the FWCS as an analog input and compared with the speed demands sent by the FWCS.

Per DCD, Tier 2, Section 7.7.3.2.2, the operator can select any one of three system operation modes for RPV level control from the main control console: (1) single element control, (2) three-element control, or (3) manual feed pump control feedwater temperature control is accomplished by manipulating the heating steam flow to the seventh stage feedwater heaters or directing a portion of the feedwater flow around the high pressure feedwater heaters as shown in DCD, Tier 2, Figure 7.7-7. The two functions are performed by two sets of triple redundant controllers located in separate cabinets as illustrated in DCD, Tier 2, Figure 7.7-3.

Feedwater temperature control has two operational modes per DCD, Tier 2, Section 7.7.3.2.3: (1) Manual, where the feedwater temperature setpoint is controlled by the operator, and (2) Automatic, where the feedwater temperature setpoint is controlled by the PAS. The redundantly measured feedwater temperatures are compared with the temperature setpoint and

the error signal is used by a proportional, integral, derivative (PID) controller. The output signals are used to generate the position demands for both the feedwater heater bypass valves and the seventh stage feedwater heater steam heating valves.

The FWCS consists of the following elements per DCD, Tier 2, Section 7.7.3.5.2:

- the FTDC that contains the software and processors for execution of the control algorithms;
- feedwater flow signals that provide for the measurement of the total flow rate of feedwater into the vessel;
- steam flow signals that provide for the measurement of the total flow rate of steam leaving the vessel;
- feed pump discharge flow signals that provide for the measurement of the discharge flow rate of each feed pump;
- the low flow control valve (LFCV) differential pressure transmitters that provide for the measurement of the pressure drop across the LFCV, for LFCV gain control;
- the LFCV flow transmitters that provide for the measurement of the flow rate through the LFCV, for both LFCV control and low thermal power calculations; and
- feedwater temperature signals that provide the measurement of the feedwater temperature at the point prior to the feedwater piping penetration to the reactor building.

The FWCS includes the following measurement systems described in DCD, Tier 2, Sections 7.7.3.5.3 through 7.7.3.5.5:

- reactor vessel water level measurement
- steam flow measurement
- feedwater flow rate measurement

7.7.3.2 Staff Evaluation

7.7.3.2.1 Evaluation of Feedwater Control System Conformance with Acceptance Criteria

The major design considerations per SRP Section 7.7 are in Section 7.7.0.3 of this report and discuss the attributes that are common to the control systems of DCD, Tier 2, Section 7.7. This section will discuss and evaluate only those major design considerations and information that are unique to the FWCS.

Design Basis:

For “Design Basis,” the FWCS is not a safety system and is not required for safe shutdown of the plant. However, the FWCS can have a significant effect on reactivity and thus reactor power. The applicant stated in DCD, Tier 2, Section 7.7.3.1.2, that the FWCS is designed so that the functional capabilities of safety systems are not inhibited. The design basis of the FWCS has instrumentation and controls to regulate the flow of feedwater into the RPV,

automatically or manually, to maintain the RPV water level such that predetermined limits on water level are met during transients and normal plant operating modes. Further, the FWCS controls feedwater temperature to allow reactor power control without moving control rods. Based on information reviewed in DCD Tier 1, DCD, Tier 2, Section 7.7.3 and Chapter 15, and evaluations that follow, the NRC staff concurs with the classification and finds that the plant accident analysis does not require operability of the FWCS for safe shutdown of the nuclear power plant. The NRC staff finds that the FWCS includes the necessary features for manual and automatic control of process variables within prescribed operating limits. An example is the fact that there is a maximum allowable feedwater temperature setpoint change that cannot be exceeded. Feedwater temperature cannot be decreased when the reactor thermal power exceeds 100 percent. The system does not accept a temperature setpoint outside of the area allowed by the reactor power versus feedwater temperature map which is described in DCD, Tier 2, Subsection 4.4.4.3. Accordingly, based on the above and the verification of these controls and functions through DCD, Tier 1, Section 2.2.3 ITAAC, the NRC staff finds that the design bases have been adequately addressed for the FWCS.

Effects of Control System Operation on Accidents:

For “Effects of FWCS Operation on Accidents,” the NRC staff reviewed DCD, Tier 2, Section 7.7.3 and Chapter 15, for the effects of control system operation on accidents. The FWCS regulates the feedwater flow and feedwater temperature. The FWCS has a primary function in maintaining the proper RPV water level during transients unless unavailable due to isolation of the feedwater lines, loss of power to the feedwater pumps, or major circuit failure. For example, the FWCS controls RPV water level during a postulated inadvertent isolation condenser initiation or a runout of one feedwater pump. The FWCS initiates a runback of feedwater pump feedwater demand to zero and closes the LFCV and RWCU/SDC OBCV when it receives an ATWS trip signal from the ATWS/SLC Logic, as described further in DCD, Tier 2, Section 7.8.1.1. Although no credit is taken for the function in the safety analysis, the feedwater temperature control function also mitigates inadvertent feedwater temperature changes in either direction by manipulating its control valves to maintain the setpoint temperature. In the event of a failure involving the physical control valves, the FWCS will attempt to maintain the feedwater temperature at the setpoint. The temperature difference between feedwater lines A and B is monitored and alarmed if it exceeds the allowable value. The condition where the FWCS cannot maintain the feedwater temperature is bounded by the transient LOFWH. Based on the information above and below, and as described in DCD, Tier 2, Section 7.7.3 and Chapter 15, Tables 15.1-5 and Table 15.1-6, the NRC staff finds that the safety analysis presented in DCD, Tier 2, Chapter 15, includes consideration of the effects of both control system action and inaction in assessing the transient response of the plant for accidents and AOOs.

Effects of Control System Failures:

For “Effects of Feedwater Control System Failures,” the NRC staff reviewed the DCD, Tier 2, Chapter 15 and Section 7.7.3, for the effects of FWCS failures. The failure of the FWCS may affect feedwater flow or feedwater temperature. A total failure of either feedwater flow control subsystem or temperature control subsystem is unlikely because of the use of the triple redundant digital controllers, redundant UPS power supplies, and independent input/output signals to each of the three channels (process controllers) of each controller. The probability of a combined feedwater temperature change and feedwater flow/reactor water level change caused by controller failure is significantly reduced or even precluded by implementing the two control schemes in physically different cabinets and logic processors. No single failure or operator error of the feedwater temperature control subsystem results in more than a 55.6 °C

(100 °F) decrease in the final feedwater temperature.

The worst case of a feedwater pump ASD controller failure in the FWCS system would cause a run-out of one feedwater pump to its maximum flow rate. This event would be detected by high feedwater flow and the FWCS would respond by reducing the demand to the other pumps, automatically compensating for the excessive flow rate from the failed pump.

While unlikely, the total failure of the FWCS and its control of feedwater flow is bounded by (1) failure in a manner that significantly reduces feedwater flow when feedwater is still needed, (2) failure in a manner to oversupply feedwater, and (3) failure in a manner that is still near demand, but no longer responding.

In the first case, RPV water level will decrease and unless the operators detect and identify the problem correctly, and take contingency action, the RPS will actuate. Specifically, if the water falls to Level 3, then the RPS shuts down the reactor. If the water continues to drop and reaches Level 2, the high pressure makeup function of the CRD system initiates (The CRD system is fully independent of other plant delivery or injection systems). The ICS, as part of the ECCS, typically starts operating automatically upon low reactor water level (Level 2) with time delay, and low reactor water Level 1. Also, the GDCS and ADS, as part of the ECCS, operate automatically upon low reactor water Level 1. In DCD, Tier 2, Chapter 15, Table 15.1-6, if the event involves Loss of Non-Emergency AC Power to Station Auxiliaries, an anticipatory scram occurs.

In the second case RPV water level will increase unless the operators detect and correctly identify the problem, and take contingency action. If the RPV water level rises to Level 8, then the RPS shuts down the reactor. Additionally, the main turbine trips, the feedwater pump ASD flow demand is reduced to zero, and LD&IS closes the safety feedwater isolation valves. If the RPV water level rises to Level 9, the feedwater pumps are tripped by the DPS and the ASD controller power supply is interrupted by LD&IS. In DCD, Tier 2, Chapter 15, this event is bounded by Feedwater Controller Failure - Maximum Flow Demand transient.

In the third case uncontrolled feedwater flow will eventually drive the RPV water level either too high or too low, but perhaps over such a long period the possible results may be the same as those in case 1 or 2. However, it is likely that the longer time period significantly increases the probability that the operators will detect and correctly identify the problem, and take contingency action long before the high pressure makeup function of the CRD system initiates or protective functions actuate.

The ESBWR uses feedwater temperature as an additional power controlling parameter as described in DCD, Tier 2, Section 7.7.3.2.3. Loss of feedwater heating increases core inlet subcooling and results in a greater core power due to increased moderation. While unlikely, the total failure of the FWCS and its control of feedwater temperature is still limited by protective actions. If the reactor thermal power versus feedwater temperature combination is outside of the area allowed by the reactor power versus feedwater temperature map, the RC&IS initiates a control rod withdrawal block and feedwater temperature control valve one-way block. If the reactor thermal power versus feedwater temperature combination further departs from the area allowed by the reactor power versus feedwater temperature map (high reactor thermal power, high feedwater temperature or low feedwater temperature), the RPS can shut down the reactor.

A loss of feedwater heating is also monitored independently by both the ATLM and the DPS. If a significant decrease in feedwater temperature is detected by the ATLM or by the DPS, either

will mitigate the event by initiating SCRRI and SRI functions. Although no credit is taken for the function in a safety analysis, the feedwater temperature control system also mitigates inadvertent feedwater temperature changes in either direction by manipulating its control valves to maintain the setpoint temperature. Further, temperature difference between feedwater lines A and B is monitored and alarmed if it exceeds the allowable value.

DCD, Tier 2, Chapter 15, identifies feedwater occurrences and events related to feedwater flow control and feedwater temperature control in DCD, Tier 2, Chapter 15 and Tables 15.0-2, 15.1-3, 15.1-5, 15.1-6, and 15.1-7. Accordingly, the NRC staff finds that these occurrences and events are consistent with the identified flow control and temperature control failures of the FWCS and, therefore, finds that the failure of the FWCS does not cause plant conditions more severe than those described in DCD, Tier 2, Chapter 15. In RAI 7.7-12, the NRC staff requested that the applicant provide analyses that evaluate the effects of control systems failures. RAI 7.7-12 was being tracked as an open item in the SER with open items. In response, the applicant revised the DCD, Tier 2, Section 7.7 to reference DCD, Tier 2, Chapter 15 analyses of specific events that evaluate the effects of control systems failures. As discussed above, the expected and abnormal transients and accident events analyzed in DCD, Tier 2, Chapter 15, Subsections 15.2.4.2, 15.3.1 and 15.3.2 bound the effects of FWCS failures. The staff determined the response was acceptable since the applicant identified the DCD, Tier 2, Chapter 15 analyses that bound the failures of the FWCS. Based on the applicant's response, RAI 7.7-12 regarding the FWCS is resolved. While the focus in these cases is on feedwater flow, RPV water level, and feedwater temperature, detection of a FWCS control problem and response could come from other parameters including power, pressure, steam flow, and the turbine/generator parameters as well as the FWCS self-diagnostics.

Effects of Control System Failures Caused by Accidents:

For "Effects of FWCS Failures Caused by Accidents," the NRC staff reviewed DCD, Tier 2, Section 7.7.3 and Chapter 15, for the effects of FWCS failures caused by accidents. The FWCS consists of multiple types of cabinets, or panels, that contain special electronic/electrical equipment modules for performing the FWCS logic in the reactor building and control building. Accidents could potentially damage the sensors and transmitters providing input to the FWCS as in the NBS(N) system. Fire or earthquake potential could cause one or more functions to fail and damage the electronic equipment causing an FWCS function to fail. The potential for such effects is significantly reduced through (1) D3 in the NBS(N) sensors, (2) FWCS environmental equipment qualification, (3) triple redundant controller modules in different cabinets, (4) the fire protection design, (5) a combined feedwater temperature change, and (6) the fact that feedwater flow/reactor water level change caused by a controller failure is precluded by implementing the two control schemes in physically different cabinets and logic processors. Based on the above, the evaluation and a review of accident consequences and effects of AOOs on the FWCS, the NRC staff finds that the consequential effects of AOOs and accidents do not lead to FWCS failures that would result in consequences more severe than those described in DCD, Tier 2, Chapter 15. Based on the above, the NRC staff finds that the effects of FWCS failures caused by accidents have been adequately addressed.

Diversity and Defense-in-Depth:

For "Diversity and Defense-in-Depth," Section 7.7.0.3 of this report discusses this design consideration. Further, the NRC staff notes that in support of 10 CFR 50.62 and mitigating ATWS events, the FWCS initiates a runback of the feedwater pump's feedwater demand to zero and closes the LFCV and RWCU/SDC overboard flow-control valve when it receives an ATWS

trip signal from the ATWS/SLC logic. With less feedwater for mixing, core inlet subcooling decreases. This introduces negative reactivity from reduced moderator density and voiding to reduce power. 10 CFR 50.62 is evaluated in Section 7.8.3 of this report. DCD, Tier 2, Section 7.7.3.3.3, states that the portions of the FWCS that provide interface support for the DPS conform to the criteria of the SRM on Item II.Q of SECY-93-087.

Potential for Inadvertent Actuation:

For "Potential for Inadvertent Actuation," the NRC staff reviewed DCD Chapter 7.7.3 to identify design measures that limit the potential for inadvertent actuation. Examples of such design features are as follows:

The FWCS is designed with redundancy so that failure of any single instrument does not interfere with the system operation. The FTDC consists of three parallel processing channels, each containing the hardware and software for execution of the control algorithms. Each FTDC channel executes the control software for the control modes. Redundant UPS power the FWCS digital controllers and process measurement equipment. No single power source or single power supply failure results in the loss of FWCS functions. Each parallel processing channel has independent inputs and outputs.

The FTDC self-test and online diagnostic test features are capable of identifying and isolating failures of process sensors, I/O cards, power buses, power supplies, processors and intermediate processor communication paths. These features identify the presence of a fault and determine the location of the failure down to the module level.

Further, in the event that the failure of the triple redundant FWCS causes the RPV water level to drop, when the water level reaches Level 2, the high pressure makeup function of the CRD system initiates as a diverse means. During normal operation, feedwater flow is delivered to the RPV through three RFPs which operate in parallel. In normal operation, the fourth RFP is in standby mode and starts automatically if any operating feedwater pump trips while at power. Also, the fourth RFP can be set in manual mode or can be removed from service for maintenance. The RPV water level, steam flow, and feedwater flow use multiple signals that are displayed and alarmed in the MCR.

During normal operation the FWCS sends three speed-demand signals, each of which reflects a voted FWCS processor output, to each feed pump ASD. The ASD performs a mid-value vote and uses it to control the speed/frequency of the feed pump motor. The mid-value vote is also returned to the FWCS as an analog input and compared with the speed demands sent by the FWCS. If an FTDC channel detects a discrepancy between the field voter output and the FTDC channel output, a "lockup" signal is sent to a "lockup" voter and an alarm is activated in the MCR.

A combined feedwater temperature change and feedwater flow/reactor water level change caused by controller failure is precluded by implementing the two control schemes in physically different cabinets and logic processors.

Based on the above, the NRC staff finds that the FWCS design limits the potential for inadvertent actuation.

7.7.3.2.2 Evaluation of Feedwater Control System Compliance with Regulations

The common design attributes and methods for complying with the regulations required by SRP Section 7.7 for control systems of DCD, Tier 2, Section 7.7 are discussed in Section 7.7.0.4 of this report. This section will discuss and evaluate only those regulations with unique methods of compliance for the FWCS.

For "Compliance with 10 CFR 52.47(b)(1)," the NRC staff evaluated whether the requirements of 10 CFR 52.47(b)(1) are adequately addressed for the control systems of DCD, Tier 2, Section 7.7. The NRC staff reviewed DCD Tier 2, Section 7.7.3, and DCD Tier 1, Section 2.2.3, in accordance with SRP Sections 7.7 and 14.3.5, to verify that 10 CFR 52.47(b)(1) has been adequately addressed for the FWCS. DCD, Tier 1, Section 2.2.3, documents the FWCS ITAAC requirements. While the FWCS has no DAC, the FWCS methods and functions of controlling the feedwater and feedwater temperature, the general equipment and modes of control, and the actuation initiators of protective actions are specified. The NRC staff noted that DCD, Tier 1, Table 2.2.3-1, states, "FWCS is a triple-redundant, fault tolerant digital controller (FTDC)." Based on information in DCD Tier 1, DCD, Tier 2, Chapter 7, information discussed herein and identified FWCS I&C and their verification in the ITAAC, the NRC staff finds that the requirements of 10 CFR 52.47(b)(1) have been adequately addressed.

For "Compliance with GDC 10, 13, 15, 19, 28, and 29," the NRC staff reviewed DCD, Tier 2, Section 7.7.3, to verify that the applicable GDC specified in SRP Section 7.7 have been adequately addressed for the FWCS as a non-safety system of the ESBWR. DCD, Tier 2, Section 7.7.3.3.2, states that the FWCS complies with GDC 13 and 19.

GDC 10 requires that the reactor core, associated coolant, control, and protection systems 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. The NRC staff evaluated whether GDC 10 has been adequately addressed for the FWCS. SRP Appendix 7.1-A for GDC 10 states that the NRC staff review should evaluate the I&C system contributions to design margin for reactor core and coolant systems. In DCD, Tier 2, Chapter 15 and Tables 15.1-5 and 15.1-6, identify FWCS actuations and other actions that reduce the need for the actuation of protection and safety systems to mitigate AOOs. DCD, Tier 2, Section 7.7.3, includes corresponding actions in the design bases of the FWCS to maintain the reactor core, reactor coolant system, and the reactivity limits within appropriate margins and to mitigate AOOs. Examples of such design features are as follows:

The FWCS controls the RPV water level between L8 and L3 during normal operation. Consistent with DCD, Tier 2, Chapter 15, Table 15.1-5, the FWCS mitigates AOOs such as Inadvertent Isolation Condenser Initiation and Runout of One Feedwater Pump events by reducing the output of the remaining feedwater pumps to compensate for the excessive output of the failed pump and to maintain appropriate reactor water level. The FWCS controls feedwater temperature around a setpoint and neither the operator nor the automation system can change the setpoint faster than an allowable rate (nominally 55.6°C (100°F) per hour). The FWCS design does not allow a feedwater temperature decrease when the reactor thermal power exceeds 100 percent of rated thermal power. The FWCS initiates a runback of the feedwater pump demand to zero and closing the LFCV and RWCU/SDC OBCV when an ATWS trip signal is received. DCD, Tier 1, Section 2.2.3, includes the ITAAC for the applicant to verify that the as-built FWCS implements these actions. Accordingly, based on identified FWCS actions and their verification in the ITAAC, the NRC staff finds that the requirements of GDC 10 have been adequately addressed for the FWCS.

GDC 13 requires providing instrumentation to monitor variables and systems over their anticipated ranges for normal operation, AOOs, and accident conditions to assure adequate safety. GDC 13 also requires providing appropriate controls to maintain these variables and systems within prescribed operating ranges. The NRC staff evaluated whether GDC 13 has been adequately addressed for the FWCS, for AOOs, and for accident conditions as appropriate to help assure adequate safety. For the FWCS, these include those parameters and controls that affect reactivity and RPV water level. The NRC staff reviewed the plant transient response to normal load changes and AOOs such as Loss of Feedwater Heating, Feedwater Controller Failure-Maximum Flow Demand, LOFWH With Failure of SCRRI and SRI, and Loss of All Feedwater. The NRC staff concludes that the FWCS is capable of maintaining system variables within prescribed operating ranges and capable of contingency actions if such variables reach limiting conditions. In DCD, Tier 2, Sections 7.7.3.2 and 10.4.7.5, specify status information provided by and for the FWCS, including status data on feedwater flow rate, steam flow rate, RFP discharge flow rates, and monitoring of the temperature and temperature difference between feedwater lines A and B (which, if excessive, provides an indication to the operator). DCD, Tier 2, Section 7.7.3.2.2, specifies manual and automatic reactor water level controls. DCD, Tier 2, Section 7.7.3.2.3, specifies manual and automatic reactor water temperature controls. DCD, Tier 2, Section 7.7.3.3.2, indicates compliance with GDC 13. DCD, Tier 1, Section 2.2.3, includes the ITAAC for the applicant to verify that the as-built FWCS implemented the required automatic functions and operator reactor water level and temperature controls. Accordingly, based on identified FWCS I&C and their verification in the ITAAC, the NRC staff finds that the requirements of GDC 13 have been adequately addressed for the FWCS.

GDC 15 requires that the reactor coolant system and associated auxiliary, control, and protection systems shall be designed with sufficient margin to ensure that the design conditions of the RCPB are not exceeded during any condition of normal operation, including AOOs. The NRC staff evaluated whether GDC 15 has been adequately addressed for the FWCS. SRP Appendix 7.1-A for GDC 15 states that the NRC staff review should evaluate the I&C system contributions to design margin for reactor coolant systems. The NRC staff reviewed DCD, Tier 2, Section 7.7.3, and DCD, Tier 1, Section 2.2.3, for the features of manual and automatic control described in the FWCS that facilitate the capability to maintain plant variables within prescribed operating limits and over their anticipated ranges for normal operation, for AOOs, and for accident conditions as appropriate to assure adequate safety. These include examples such as the automatic and manual controls for the RFPs, RPV water level measurement instrumentation, steam flow measurement instrumentation, and feedwater flow measurement instrumentation. Accordingly, based on identified FWCS I&C and their verification in the ITAAC, the NRC staff finds that the requirements of GDC 15 have been adequately addressed for the FWCS.

GDC 19 requires control room functionality, control room habitability, and remote shutdown capability. The NRC staff evaluated whether GDC 19 is adequately addressed for the FWCS. In Section 7.1.1.3.6 the NRC staff evaluated that GDC 19 has been adequately addressed with the exception of the operation of specific I&C systems. SRP Appendix 7.1-A states that the review should evaluate if there exists I&C available to operate the nuclear power unit under normal and accident conditions. DCD, Tier 2, Section 7.7.3.3.2, specifies that the FWCS conforms to GDC 19. DCD, Tier 2, Section 7.7.3.5, describes parameters provided by the FWCS to the MCR. Examples of major measurement include RPV water level, main steam flow rate, and feedwater flow rate. DCD, Tier 2, Section 7.7.3.2.2, specifies manual and automatic reactor water level controls. DCD, Tier 2, Section 7.7.3.2.3, specifies manual and automatic reactor water temperature controls. DCD, Tier 1, Section 2.2.3, includes the ITAAC for the applicant to verify that the as-built FWCS implements the required automatic functions and

operator reactor water level and temperature controls. Based on the above, including the features for manual and automatic control described in DCD, Tier 2, Section 7.7.3, the NRC staff finds that the requirements of GDC 19 have been adequately addressed for the FWCS.

GDC 28 requires that reactivity control systems be designed with appropriate limits on the potential amount and rate of reactivity increase. The NRC staff evaluated whether GDC 28 has been adequately addressed for the FWCS. SRP Appendix 7.1-A states that GDC 28 imposes functional requirements on I&C interlock and control systems to the extent they are provided to limit reactivity increases to prevent or limit the effect of reactivity accidents. DCD, Tier 2, Section 7.7.3.3.2, does not include GDC 28. However, DCD, Tier 2, Section 7.7.3.2.3, summarizes the feedwater temperature control features that limit potential amount and rate of reactivity increase. These features include: (1) neither the operator nor the automation system can change the setpoint faster than an allowable rate (nominally 55.6°C (100°F) per hour), (2) neither the operator nor the automation system can input a setpoint outside the area allowed by the reactor power versus feedwater temperature operating map (power- feedwater temperature map), and (3) the feedwater temperature controller is unable to decrease feedwater temperature if the reactor thermal power is equal to or greater than 100%. Similarly, DCD, Tier 2, Section 7.7.3.2.2, summarizes the feedwater level controls that limit potential amount and rate of reactivity increase. An example is that if the reactor water level reaches Level 8, the FWCS simultaneously activates a MCR alarm, and sends a zero-speed demand signal to the feed pump ASDs, and trips the main turbine. These and other functions of the design performed by the FWCS address GDC 28 and reduce the need for the actuation of safety systems. DCD, Tier 1, Section 2.2.3, includes the ITAAC for the applicant to verify that the as-built FWCS implemented these actions. Accordingly, based on the identified FWCS actions and their verification in the ITAAC, the NRC staff finds that the requirements of GDC 28 have been adequately addressed for the FWCS.

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. The NRC staff evaluated whether GDC 29 has been adequately addressed. SRP Appendix 7.1-A identifies that GDC 29 is addressed by conformance, as applicable, to applicable GDC 20 thru 25 and GDC 28. Since the FWCS is a reactivity control system and not a protection system, GDC 20-23 and 25, which are requirements for protection systems, are not applicable to FWCS, Accordingly, GDC 29 is addressed by conformance as applicable to GDC 24 and 28. Conformance of N-DCIS control systems to GDC 24, including the FWCS, is evaluated in Section 7.7.0.4 of this report. Conformance of the FWCS to GDC 28 is evaluated above. Further, DCD, Tier 2, Section 7.7.3.2.1, states that each function of the FWCS is implemented on its own dedicated set of the triple redundant FTDCs, including power supplies and input/output signals. The controller is designed for a mean time to failure (MTTF) of no less than 1000 years according to the applicant. Each set of FTDCs consists of three parallel processing channel controllers, each containing the hardware and software for execution of the control algorithms. Each FTDC channel executes the control software for the control modes. Based on the information above and requirements of GDC 24 and 28 having been adequately addressed for the FWCS, the NRC staff finds that the requirements of GDC 29 have been adequately addressed for the FWCS.

Therefore, the NRC staff finds that the FWCS, adequately addresses the relevant regulatory criteria listed in Section 7.7.0.1 above for a non-safety system and that there is reasonable assurance this system will be able to accomplish its designed function in a reliable manner, when built and tested according to DCD Tier 2 and DCD Tier 1 ITAAC.

7.7.3.3 Conclusion

Based on the above, NRC staff concludes there is reasonable assurance that the FWCS conforms to the applicable requirements, which include GDC 1, 10, 13, 15, 19, 24, 28, and 29, 10 CFR 52.47(b)(1), 10 CFR 50.55a(a)(1) and 10 CFR 50.55a(h); adequate high level functional requirements are identified, and sufficient ITAAC are included in DCD Tier 1 to verify that the design is completed in compliance with the applicable requirements.

7.7.4 Plant Automation System

7.7.4.1 Summary of Technical Information

As described in DCD, Tier 2, Section 7.7.4, the (non-safety) PAS provides the capability for supervisory control of the entire plant. It does this by supplying setpoint commands to independent non-safety automatic control systems such as the FWCS and RC&IS. The PAS provides supervisory controls that regulate reactivity during criticality control, provides heatup and pressurization control, regulates reactor power, controls turbine/generator output, controls secondary non-safety systems, and provides reactor startup/shutdown controls. The functions of the PAS are accomplished by suitable algorithms for different phases of reactor operation which include approaches to criticality, heatup, reactor power increase, automatic load following, reactor power decrease, and shutdown. The triple redundant FTDC and redundant system controllers perform the PAS control functional logic.

The N-DCIS accepts one-way communication from the Q-DCIS so that the safety information can be monitored, archived, and alarmed seamlessly with the N-DCIS data. Through the N-DCIS, the PAS receives input from the safety NMS and RPS. Through the N-DCIS, the PAS receives input from the non-safety RC&IS, SB&PC system, PAS, RWCU/SDC, and the TGCS. The output-demand requested signals from the PAS are sent to the RC&IS to position the control rods, to the SB&PC for pressure setpoints, and to the TGCS for load following operation. DCD, Tier 2, Figure 7.7-4, provides a simplified functional block diagram of the PAS.

The PAS interfaces with the operator's control console in the MCR to perform its designed functions. From the operator's control console for automatic plant startup, power operation, and shutdown functions, the operator uses the PAS to issue supervisory control commands to non-safety systems. The operator also uses the PAS to adjust setpoints of lower level controllers to support automation of the normal plant startup, shutdown, and power range operations.

In the automatic mode, the PAS also issues command signals to the turbine master controller, which contains appropriate algorithms for automated sequences of the main turbine and related auxiliary systems. The PAS presents the operator with a series of breakpoint controls on the main control console non-safety VDUs for a prescribed plant operation sequence.

When all the prerequisites are satisfied for a prescribed breakpoint in a control sequence, a permissive is requested and, upon operator acceptance, the prescribed control sequence is initiated or continued. The PAS then initiates demand signals to various system controllers to carry out the predefined control functions. For non-automated operations that are required during normal startup or shutdown (such as a change of reactor mode switch status), automatic prompts are provided. Automated operations continue after the prompted actions are completed manually. The functions associated with reactor power control are performed by the PAS.

For reactor power control, the PAS contains algorithms that can change reactor power by control rod motions. A prescribed control rod sequence is followed when manipulating control rods for reactor criticality, heatup, power changes, and automatic load following. Each of these functions has its own algorithm to achieve its designed objective. When the reactor power control is to be done by feedwater temperature change, the PAS can provide the FWCS feedwater control setpoints to permit reactor power maneuvering without control rod motion. During automatic load-follow operation, the PAS interfaces with the TGCS to coordinate main turbine and reactor power changes for stable operation and performance.

7.7.4.2 Staff Evaluation

7.7.4.2.1 Evaluation of PAS Conformance with Acceptance Criteria

The major design considerations per SRP Section 7.7 are in Section 7.7.0.3 of this report and discuss the attributes that are common to the control systems of DCD, Tier 2, Section 7.7. This section will discuss and evaluate only those major design considerations and information that are unique to the PAS.

Design Basis:

For “Design Basis,” the PAS has no safety design basis. This system is designed so that functionalities of safety systems are not affected by it. The PAS does have a power generation (non-safety) design basis. The non-safety design basis of the PAS is to provide supervisory (automatic and semi-automatic) control that regulates reactivity during criticality control, provides heatup and pressurization control, regulates power, controls turbine/generator output, controls secondary-related non-safety systems, and provides reactor startup/shutdown control. The functions of the PAS are accomplished by suitable algorithms for different phases of reactor operation. Through the N-DCIS, the PAS receives input from the safety systems including NMS and the RPS. Through the N-DCIS, the PAS receives input from the non-safety systems, including RC&IS, SB&PC system, FWCS, RWCU/SDC, and the TGCS. The algorithms then calculate appropriate setpoints that are provided back to various control systems including to (1) the RC&IS to position the control rods, (2) the SB&PC system for pressure setpoints, and (3) the TGCS for load-follow operation. For example, to control reactor power by feedwater temperature change, the PAS provides the feedwater temperature control a new setpoint to allow reactor power maneuvering without moving control rods. Based on information reviewed in DCD, Tier 2, Section 7.7.4, DCD, Tier 2, Chapter 15, and the evaluations that follow, the NRC staff finds that the PAS includes the necessary features for automatic control and semi-automatic control of process variables within prescribed operating limits.

Effects of Control System Operation on Accidents:

For “Effects of PAS Operation on Accidents,” the NRC staff reviewed DCD, Tier 2, Section 7.7.4 and Chapter 15, for the effects of PAS operation on accidents. The PAS does not directly control the physical equipment such as pumps, valves, and control rods, but receives inputs from systems that control the physical equipment and provides setpoints for automatic and semi-automatic plant operations. The normal mode of operation of the PAS is automatic. If any system or component conditions are abnormal during execution of the prescribed sequences, the PAS automatically switches into the manual mode. With the PAS in the manual mode, any in-progress operation stops and alarms are activated in the MCR. Further, with the PAS back in manual mode, the operator can manipulate control rods through the normal controls. A failure

of the PAS does not prevent manual control of reactor power, and does not prevent safe shutdown of the reactor. Inaction by PAS when in automatic mode is effectively an input failure or an I&C component failure and discussed under (4) below. Based on the above, and as described in DCD, Tier 2, Section 7.7.4 and Chapter 15, Tables 15.1-5 and Table 15.1-6, the NRC staff finds that the safety analysis presented in DCD, Tier 2, Chapter 15, includes consideration of the effects of both control system action and inaction in assessing the transient response of the plant for accidents and AOOs.

Effects of Control System Failures:

For "Effects of PAS Failures," the NRC staff reviewed DCD, Tier 2, Chapters 15 and Section 7.7.4 for the effects of PAS failures. The PAS does not control physical equipment directly, but provides control functions through setpoint changes in systems that control the physical equipment. The transients present in DCD, Tier 2, Chapter 15, Tables 15.1-5, 15.1-6, and 15.1-7, are bounding for PAS failures. A PAS failure could be from bad input, or component failure within the PAS. As an example, assume a failure in PAS provided a setpoint to the FWCS that caused a significant increase in feedwater flow. This would be bound by the DCD, Tier 2, Chapter 15, Table 15.1-6, transient Feedwater Controller Failure-Maximum Flow Demand. An incorrect setpoint failure of the PAS does not prevent manual control of reactor power, and does not prevent safe shutdown of the reactor. The NRC staff verified that the failure of any PAS system component for control systems does not cause plant conditions more severe than those described in the analysis of AOOs in DCD, Tier 2, Chapter 15. Based on information reviewed in DCD Tier 1, DCD, Tier 2, Section 7.7.4, and Chapter 15, the NRC staff finds that the occurrences and events discussed in DCD, Tier 2, Chapter 15 are consistent with failures of the PAS and, therefore, the NRC staff finds that failure of the PAS does not cause plant conditions more severe than those described in DCD, Tier 2, Chapter 15. In RAI 7.7-12 and RAI 7.7-12, Supplement 1, the NRC staff requested that the applicant provide analyses that evaluate the effects of PAS control system failures. RAI 7.7-12 was being tracked as an open item in the SER with open items. In its response, the applicant revised the DCD, Tier 2, Section 7.7 to reference DCD, Tier 2, Chapter 15 analyses of specific events that evaluate the effects of control systems failures. The applicant also stated that in the unlikely event of the failure of the triple redundant master controllers and duplicate system controllers causing the PAS to issue incorrect setpoints, the expected and abnormal transients and accident events analyzed in DCD, Tier 2, Chapter 15 bound the effects of the PAS failures as discussed above. The DCD, Tier 2, Chapter 15 events that analyze the effects of the PAS failures are as follows: (1) Subsections 15.2.3.1, 15.2.3.2, 15.3.8, and 15.3.9 bound the effects of failures of the RC&IS controls, (2) Subsections 15.2.4.2, 15.3.1, and 15.3.2 bound the effects of failures of FWCS controls, and (3) Subsections 15.2.5.1, 15.3.3, 15.3.4, 15.3.2, and 15.3.6 bound the effects of failures of the SB&PC system controls. The staff determined the response was acceptable since the applicant identified the DCD, Tier 2, Chapter 15 analyses that bound the failures of the PAS. Based on the applicant's response, RAI 7.7-12 regarding the PAS is resolved.

Effects of Control System Failures Caused by Accidents:

For "Effects of PAS Failures Caused by Accidents," the NRC staff reviewed DCD, Tier 2, Chapters 15 and Section 7.7.4, for the effects of PAS failures caused by accidents. The PAS instrumentation includes (1) MCR instrumentation for the man-machine interface, (2) hardware and software for input/output interfaces and controller functions, and (3) direct non-multiplexed sensor inputs needed by the system. Except for some inputs the PAS equipment is designed for a mild environment. Accidents could potentially damage the sensors and transmitters providing input to the PAS. Fire or earthquake potential could cause one or more functions to

fail and damage the electronic equipment causing a PAS function to fail. The potential for such effects is significantly reduced through D3 in NBS(N) sensors providing input, environmental equipment qualification, triple redundant master controllers and duplicate system controllers modules and a fire protection design. A combined feedwater temperature change and feedwater flow/reactor water level change caused by controller failure is precluded by implementing the two control schemes in physically different cabinets and logic processors. Based on the above, the evaluation of effects of control system failures above, and a review of accident consequences and effects of AOOs on the PAS, the NRC staff finds that the consequential effects of AOOs and accidents do not lead to PAS failures that would result in consequences more severe than those described in DCD, Tier 2, Chapter 15. Based on the above, the NRC staff finds that the effects of PAS failures caused by accidents have been adequately addressed.

Potential for Inadvertent Actuation:

For “Potential for Inadvertent Actuation,” the NRC staff reviewed DCD 2, Section 7.7.4, to identify design measures that limit the potential for inadvertent actuation. Examples of such design features are as follows:

The PAS is designed so that the functionalities of the safety systems are not affected by it. Through the N-DCIS, the PAS receives input from the safety NMS and RPS. The N-DCIS accepts one-way communication from the Q-DCIS so that the safety information can be monitored, archived, and alarmed seamlessly within the N-DCIS.

The PAS hardware comprises triple redundant master controllers and duplicate system controllers. The normal mode of operation of the PAS is automatic. This supports a decrease in the potential for inadvertent actuation by reducing the potential for human error. If any system or component conditions are abnormal during execution of the prescribed sequences, the PAS automatically switches into the manual mode. With the PAS in the manual mode, any operation in progress stops, and alarms are activated in the MCR. Also, with the PAS in manual mode, the operator can manipulate control rods through the normal controls. The FTDC input and output communication interfaces function continuously during normal power operation. Abnormal functioning of these components can be detected during operation. In addition, the FTDC is equipped with self-test and on-line diagnostic capabilities for identifying and isolating failures of input/output signals, buses, power supplies, processors, and inter-processor communications. These can be performed without interrupting the normal control operation of the PAS.

Based on the above, the NRC staff finds that the PAS design limits the potential for Inadvertent actuation.

7.7.4.2.2 Evaluation of Plant Automation System Compliance with Regulations

The common design attributes and methods for complying with the regulations required by SRP Section 7.7 for control systems of DCD, Tier 2, Section 7.7 are listed and discussed in Section 7.7.0.4 of this report. This section will discuss and evaluate only those regulations with unique methods of compliance for the PAS.

For “Compliance with 10 CFR 52.47(b)(1),” the NRC staff evaluated whether the requirements of 10 CFR 52.47(b)(1) are adequately addressed for the PAS. DCD Tier 1, does not provide ITAAC for the PAS. The PAS is not only non-safety, it does not have a direct control over the

physical position control rods, control feedwater flow, and steam flow rate. In addition, the PAS is not required by any regulation. Accordingly, based on a review of DCD, Tier 2, Section 7.7.4, and SRP Sections 14.3 and 14.3.5, the NRC staff finds that not providing ITAAC for PAS is acceptable.

For “Compliance with GDC 10, 13, 15, 19, 28, and 29,” the NRC staff reviewed DCD, Tier 2, Section 7.7.4, to verify that the applicable GDC have been adequately addressed for the PAS as a non-safety system. DCD, Tier 2, Section 7.7.4.3.2, states that the PAS conforms to GDC 13 and 19.

GDC 10 requires that the reactor core, associated coolant, control, and protection systems 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. The NRC staff evaluated whether GDC 10 has been adequately addressed for the PAS. SRP Appendix 7.1-A for GDC 10 states that the NRC staff review should evaluate the I&C system contributions to design margin for reactor core and coolant systems. The PAS functions as a supervisor system with no direct control of physical equipment that controls reactivity or power. The PAS receives input from the following major non-safety systems, the RC&IS (Section 7.7.2), SB&PC system (Section 7.7.5), FWCS (Section 7.7.3), RWCU/SDC (Section 7.4.3), and the TGCS. The output demand request signals from the PAS are to the RC&IS to position the control rods, to the SB&PC system for pressure setpoints, and to the TGCS for load following operation. Thus, since the PAS does not have direct control, the NRC staff finds that GDC 10 is not applicable to the PAS.

GDC 13 requires providing instrumentation to monitor variables and systems over their anticipated ranges for normal operation, AOOs, and accident conditions to assure adequate safety. GDC 13 also requires providing appropriate controls to maintain these variables and systems within prescribed operating ranges. The NRC staff evaluated whether GDC 13 has been adequately addressed for the PAS. DCD, Tier 2, Section 7.7.4.2, identifies I&C provided to monitor, control, and maintain the variables over their anticipated ranges for normal operation during the automatic and non-automatic (semi-automatic) operation of the PAS and while it is in the manual mode. The PAS instrumentation continues to receive input when in manual mode, but any in-progress operation stops and alarms in the MCR. Another example is that the PAS has instrumentation to interface with the operator's control console to aid in its designed functions. From the operator's control console for automatic plant startup, power operation, and shutdown functions, the operator uses the PAS to issue supervisory control commands to non-safety systems. The operator also uses the PAS to adjust setpoints of lower level controllers. The PAS provides supervisory direction to the actual controlling functions. The PAS presents the operator with a series of breakpoint controls on the main control console through non-safety VDUs for a prescribed plant operation sequence. After all prerequisites are satisfied for a prescribed breakpoint on a control sequence, a permissive (i.e., a control system request to proceed) is requested. The prescribed control sequence is initiated only following operator acceptance. If any system or component conditions are abnormal during execution of the prescribed sequences, the PAS automatically switches into the manual mode. DCD, Tier 2, Section 7.7.4.3.2, indicates conformance to GDC 13. Accordingly, based on review of DCD, Tier 2, Chapter 15 and Section 7.7.4, and the commitment to provide instrumentation to monitor variables and systems over their anticipated ranges for normal operation, for AOOs, and for accident conditions as appropriate to ensure adequate safety and provide appropriate controls to maintain these variables and systems within prescribed operating ranges, the NRC staff finds that the requirements of GDC 13 have been adequately addressed for the PAS.

GDC 15 requires that the reactor coolant system and associated auxiliary, control, and protection systems shall be designed with sufficient margin to ensure that the design conditions of the RCPB are not exceeded during any condition of normal operation, including AOOs. The NRC staff evaluated whether GDC 15 has been adequately addressed for the PAS. SRP Appendix 7.1-A for GDC 15 states that the NRC staff review should evaluate the I&C system contributions to design margin for reactor coolant systems. DCD, Tier 2, Section 7.7.4.2, identifies the PAS I&C provided to monitor, control, and maintain the variables over their anticipated ranges. The output demand request signals from the PAS are sent to the RC&IS to position the control rods, to the SB&PC system for pressure setpoints, and to the TGCS for load following operation. The FWCS controls the RPV water level while providing the main reactor coolant, but it does not need setpoints from the PAS. Since the PAS does not directly control parameters that contribute the design margins for the RCPB, GDC 15 is not applicable to the PAS.

GDC 19 requires control room functionality, control room habitability, and remote shutdown capability. The NRC staff evaluated whether GDC 19 is adequately addressed for the PAS. In Section 7.1.1.3.6 the NRC staff evaluated that GDC 19 has been adequately addressed with the exception of the operation of specific I&C systems. SRP Appendix 7.1-A states that the review should evaluate if there exists I&C available to operate the nuclear power unit under normal and accident conditions. DCD, Tier 2, Section 7.7.4.3.2, specifies that the PAS conforms to GDC 19. DCD, Tier 2, Section 7.7.4.2, describes the PAS interface with operator's console to perform PAS designated functions. An example includes parameters provided by the PAS to the MCR. From the operator's control console for automatic plant startup, power operation, and shutdown functions, the operator uses the PAS to issue supervisory control commands to non-safety systems. The operator also uses the PAS to adjust setpoints of lower level controllers to support automation of the normal plant startup, shutdown, and power range operations. DCD, Tier 2, Section 7.7.4.2.2, specifies manual and automatic PAS controls. Based on the above, including the features for manual and automatic control described in DCD, Tier 2, Section 7.7.4, the NRC staff finds that the requirements of GDC 19 have been adequately addressed for the PAS.

GDC 28 requires that reactivity control systems be designed with appropriate limits on the potential amount and rate of reactivity increase. The NRC staff evaluated whether GDC 28 has been adequately addressed for the PAS. SRP Appendix 7.1-A states that GDC 28 imposes functional requirements on I&C interlock and control systems to the extent they are provided to limit reactivity increases to prevent or limit the effect of reactivity accidents. DCD, Tier 2, Section 7.7.4.3.2, does not include GDC 28. DCD, Tier 2, Section 7.7.4.2, describes the output of setpoints that specifically control reactivity and thus reactor power. The algorithms have appropriate limits on control rod motion when manipulating control rods for reactor criticality, heatup, power changes, and automatic load following. Other algorithms provide setpoints for the reactivity control by feedwater temperature change with appropriate restrictions and without moving control rods. In combination, the two reactor power control methods are utilized to form a sequential step-by-step power maneuvering strategy for the control rod pattern/movement and feedwater temperature change. Based on the above and information from DCD, Tier 2, Section 7.7.4, the NRC staff finds that the requirements of GDC 28 have been adequately addressed.

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. The NRC staff evaluated whether GDC 29 has been adequately addressed. SRP Appendix 7.1-A identifies that GDC 29 is addressed by conformance, as applicable, to GDC 20-25 and GDC 28

Since the PAS is a reactivity control system and not a protection system, GDC 20-23 and 25, which are requirements for protection systems, are not applicable to PAS. Accordingly, GDC 29 is addressed by conformance as applicable to GDC 24 and 28. Conformance of N-DCIS control systems to GDC 24, including the PAS, is evaluated in Section 7.7.0.4 of this report. Conformance of the PAS to GDC 28 is evaluated above. Further, DCD, Tier 2, Section 7.7.4.5, states that the PAS hardware comprises triple redundant master controllers and duplicate system controllers. In support of a high probability of accomplishing the PAS design function, the controllers are FTDC with input and output communications interfaces continuously functioning during normal power operation. The FTDC have on-line self-test and diagnostics which can be performed without interrupting the PAS normal control operation. Based on the information above and requirements of GDC 24 and 28 having been adequately addressed for the PAS, the NRC staff finds that the requirements of GDC 29 have been adequately addressed for the PAS.

Therefore, the NRC staff finds the PAS adequately addresses the relevant regulatory criteria listed in Section 7.7.0.1 above for a non-safety system and that there is reasonable assurance that this system will be able to accomplish its design function in a reliable manner, when built and tested according to DCD Tier 2.

7.7.4.4 Conclusion

Based on the above, NRC staff concludes there is reasonable assurance that the PAS conforms to the applicable requirements, which include GDC 1, 13, 19, 24, 28, and 29, 10 CFR 52.47(b)(1), 10 CFR 50.55a(a)(1) and 10 CFR 50.55a(h); adequate high level functional requirements are identified in compliance with the applicable requirements.

7.7.5 Steam Bypass and Pressure Control System

7.7.5.1 Summary of Technical Information

The purpose of the SB&PC system is to control reactor pressure during plant startup, power generation, and shutdown modes of operation.

As described in DCD, Tier 2, Section 7.7.5.2, the control of reactor pressure is accomplished through control of the TCVs through the TGCS and TBVs, so that susceptibility to reactor trip, turbine-generator trip, main steam isolation, and SRV opening is minimized. Triple redundant FTDCs using feedback signals from RPV dome pressure sensors generate command signals for the TBVs and pressure regulation demand signals used by the TGCS to generate demand signals for the TCVs. For normal operation, the TCVs regulate reactor pressure. Whenever the total steam flow demand from the SB&PC system exceeds the effective TCV steam flow demand, the SB&PC system sends the excess steam flow directly to the main condenser through the TBVs. The ability of the plant to load-follow the grid-system demands is accomplished by the aid of control rod actions. In response to the resulting steam production demand changes, the SB&PC system adjusts the demand signals sent to the TGCS so that the TGCS adjusts the TCVs to accept the control steam output change, thereby controlling pressure. DCD, Tier 2, Section 7.7.5.6, describes the major instrument interfaces with the SB&PC system. The SB&PC system also has the capability to start the auxiliary boiler and command the auxiliary boiler to adjust steam production rate upon MSIV closure conditions as required.

7.7.5.2 Staff Evaluation

7.7.5.2.1 Evaluation of Steam Bypass and Pressure Control Conformance with Acceptance Criteria

The major design considerations per SRP Section 7.7 are in Section 7.7.0.3 of this report and discuss the attributes that are common to the control systems of DCD, Tier 2, Section 7.7. This section will discuss and evaluate only those major design considerations and information that are unique to the SB&PC system.

Design Basis:

For "Design Basis," the NRC staff reviewed DCD, Tier 2, Section 7.7.5 and the design basis of the SB&PC system. The SB&PC system is not required to operate during or after any DBA; therefore, the SB&PC system has no safety design basis. The SB&PC system is required for power generation because it controls reactor pressure during plant startup, power operation, and shutdown modes. The SB&PC system design objective is to enable a fast and stable response to system pressure disturbances, and to pressure setpoint changes over the operating range. DCD, Tier 2, Sections 7.7.5.2.2, 7.7.5.2.3, 7.7.5.4 and 7.7.5.6.10, summarize normal, abnormal and special operational features and functions. An example is that during events that lead to a reactor trip, the SB&PC system functions to stabilize the system pressure and thus aids the FWCS feedwater level control in maintaining RPV water level. Based on information reviewed in DCD, Tier 1, Section 2.2.9, DCD, Tier 2, Section 7.7.5, and Chapter 15, the NRC staff finds that the SB&PC system includes the necessary features for manual and automatic control of process variables within prescribed operating limits.

Effects of Control System Operation on Accidents:

For "Effects of SB&PC System on Accidents," the NRC staff reviewed DCD, Tier 2, Section 7.7.5 and Chapter 15 for effects of control system operation on accidents. The NRC staff verified that the safety analysis includes consideration of the effects of both SB&PC system action and inaction in assessing the transient response of the plant for accidents and AOOs. DCD, Tier 2, Sections 7.7.5.1 and 7.7.5.2, summarizes the objective of the SB&PC. The SB&PC system mission is to enable a fast and stable response to system pressure disturbances, and to pressure setpoint changes over the operating range. This is done by modulating TCVs by providing signals to the TGCS and by modulating TBVs for controlling reactor pressure. In addition, the design objective of the SB&PC system is to discharge reactor steam directly to the main condenser in order to regulate reactor pressure whenever the main turbine cannot use all of the steam generated by the reactor. The SB&C system mitigates AOOs by (1) stabilizing system pressure and thereby aiding the feedwater level control systems in maintaining RPV water level and (2) operating with other reactor control systems to avoid reactor trip after significant plant disturbances, such as loss of one feedwater pump, inadvertent opening of a SRV or TBV, main turbine stop/control valve surveillance testing, and MSIV testing. SB&PC system inaction implies a component failure in the SB&PC system logic and is addressed under (4) that follows. Based on the information reviewed in DCD, Tier 2, Section 7.7.5 and Chapter 15, and as described under (4) below, the NRC staff finds that the safety analysis includes consideration of the effects of both control system action and inaction in assessing the transient response of the plant for accidents and AOOs.

Effects of Control System Failures:

For "Effects of SB&PC System Failures," the NRC staff reviewed DCD, Tier 2, Section 7.7.2 and

Chapter 15 for effects of the SB&PC system failures. DCD, Tier 2, Chapter 15, Tables 15.1-5, 15.1-6, and 15.1-7 identifies several occurrences and events related to the SB&PC system that bound the SB&PC system component failure. These transients are Pressure Regulator Failure Opening All Turbine Control Valves and Bypass Valves, Pressure Regulator Failure-Closure of All Turbine Control Valves and Bypass Values, Generator Load Rejection with total Turbine Bypass Failure (at High Power), and Turbine Trip with Total TBV Failure (at High Power). Based on information reviewed in DCD, Tier 2, Section 7.7.5, DCD, Tier 2, Chapter 15, and evaluations herein, the NRC staff finds that the failure of the SB&PC system does not cause plant conditions more severe than those described in DCD, Tier 2, Chapter 15. In RAI 7.7-12, the NRC staff requested that the applicant provide analyses that evaluate the effects of control systems failures. RAI 7.7-12 was being tracked as an open item in the SER with open items. In response the applicant revised the DCD, Tier 2, Section 7.7 to reference DCD Tier 2, Chapter 15 analyses of specific events that evaluate the effects of control systems failures. As described above, the expected and abnormal transients and accident events analyzed in DCD, Tier 2, Chapter 15, Subsections 15.2.5.1, 15.3.3, 15.3.4, 15.3.5, and 15.3.6 bound the effects of the SB&PC system failures. The staff determined the response was acceptable since the applicant identified the DCD, Tier 2, Chapter 15 analyses that bound the failures of the SB&PC. Based on the applicant's response, RAI 7.7-12 regarding the SB&PC is resolved.

Effects of Control System Failures Caused by Accidents:

For "Effects of SB&PC System Failures Caused by Accidents," the NRC staff reviewed DCD, Tier 2, Section 7.7.5 and Chapter 15 for effects of the SB&PC system failures caused by accidents. The SB&PC system instrumentation includes the triple redundant FTDC panel mounted in the MCRBP, communication interfaces to the N-DCIS cabinets, and inputs from other systems. Accidents could potentially damage the sensors, transmitters, or communication providing input to the SB&PC. Fire or earthquake potential could cause one or more functions to fail and damage the electronic equipment causing an SB&PC system function to fail. The potential for such effects is significantly reduced through D3 design features, SB&PC system environmental EQ, triple redundant controller modules in different cabinets, and a fire protection design. Based on the above, the discussion of the effects of control system failures, and a review of accident consequences and effects of AOOs on the SB&PC, the NRC staff finds that the consequential effects of AOOs and accidents do not lead to SB&PC failures that would result in consequences more severe than those described in DCD, Tier 2, Chapter 15, Tables 15.1-5 and 15.1-6. Based on the above, the NRC staff finds that the effects of SB&PC failures caused by accidents have been adequately addressed.

Potential for Inadvertent Actuation:

For "Potential for Inadvertent Actuation," the NRC staff reviewed DCD, Tier 2, Section 7.7.5, to identify design measures that limit the potential for inadvertent actuation. Examples of such design features are as follows:

The SB&PC system is implemented on the triple redundant FTDCs. The SB&PC system has three redundant non-safety AC UPS. The SB&PC system panel is designed so that loss of one power supply or incoming power source does not affect the SB&PC system functional operation and thus plant operation. Triple redundant FTDCs perform the SB&PC system functional logic and process control functions. Because of the triple redundancy, it is possible to lose one complete processing channel without affecting the system function. This also facilitates taking one channel out of service for maintenance, repair, or module replacement while the system is online. In power operation mode, only one of the triple redundant FTDCs can be removed from

service. Controls and valve positions are designed so that steam flow is shut off when the control system electrical power or hydraulic system pressure is lost.

The SB&PC system helps avoid inadvertent actuation of the RPS. During normal operational plant maneuvers the SB&PC system provides responsive, stable performance to minimize RPV water level and neutron flux transients. The SB&PC system provides for automatic control of the reactor pressure during plant startup and heatup. The SB&PC system is also designed to operate with other reactor control systems to avoid a reactor trip after significant plant disturbances. Examples of such disturbances are loss of one feedwater pump, inadvertent opening of SRVs or TBVs, main turbine stop/control valve surveillance testing, and steamline isolation valves testing. To protect the condenser the SB&PC system inhibits opening of the TBVs when it detects high condenser pressure.

Based on the above, the NRC staff finds that the SB&PC system design limits the potential for inadvertent actuation.

7.7.5.2.2 Evaluation of Steam Bypass and Pressure Control Compliance with Regulations

The common design attributes and methods for complying with the regulations required by SRP Section 7.7 for control systems of DCD, Tier 2, Section 7.7 are listed and discussed in Section 7.7.0.4 of this report. This section will discuss and evaluate only those regulations with unique methods of compliance for the SB&PC system.

For “Compliance with CFR 52.47(b)(1).” the NRC staff evaluated whether the requirements of 10 CFR 52.47(b)(1) are adequately addressed for the SB&PC system. The NRC staff reviewed DCD, Tier 2, Section 7.7.5 and DCD, Tier 1, Section 2.2.9, in accordance with SRP Sections 7.7 and 14.3.5, to verify that 10 CFR 52.47(b)(1) has been adequately addressed for the SB&PC. DCD, Tier 1, Section 2.2.9, documents the SB&PC system ITAAC requirements. The SB&PC system methods and functions of controlling reactor pressure are specified. The NRC staff noted that DCD, Tier 1, Section 2.2.9, states that the SB&PC system uses triple-redundant FTDCs. Based on information in DCD, Tier 1, Section 2.2.9, DCD, Tier 2, Chapter 7.7.5, information discussed herein and identified SB&PC system I&C and their verification in the ITAAC, the NRC staff finds that the requirements of 10 CFR 52.47(b)(1) have been adequately addressed.

For “Compliance with GDC 10, 13, 15, 19, 28, and 29,” the NRC staff reviewed DCD, Tier 2, Section 7.7.5, to verify that the applicable GDC specified in SRP Section 7.7 have been adequately addressed for the SB&PC system as a non-safety system. DCD, Tier 2, Section 7.7.5.3.2, states that the SB&PC system conforms to GDC 13 and 19, and 24.

GDC 10 requires that the reactor core, associated coolant, control, and protection systems 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. The NRC staff evaluated whether GDC 10 has been adequately addressed for the SB&PC system. SRP Appendix 7.1-A for GDC 10 states that the NRC staff review should evaluate the I&C system contributions to design margin for reactor core and coolant systems. In DCD, Tier 2, Chapter 15, and Tables 15.1-5 and 15.1-6, identify actuations and other actions that reduce the need for the actuation of protection and safety systems to mitigate AOOs. DCD, Tier 2, Section 7.7.5, includes corresponding actions in the design bases of the SB&PC system to maintain the RPV pressure, reactor coolant system, and reactivity limits within appropriate margins and to mitigate AOOs. The specific objective of the SB&PC system is to control reactor

pressure during plant startup, power generation, and shutdown modes of operation. Further, for normal operation, the TCVs regulate reactor pressure. However, whenever the total steam flow demand from the SB&PC system exceeds the effective TCV steam flow demand, the SB&PC system sends the excess steam flow directly to the main condenser through the TBVs. The ability of the SB&PC system to control reactor pressure supports the FWCS RPV level and provides significant improvement in pressure and RPV water level control during transients. DCD, Tier 1, Section 2.2.9, includes the ITAAC for the applicant to verify that the as-built SB&PC system implements these actions. Accordingly, based on identified SB&PC system actions and their verification in the ITAAC, the NRC staff finds that the requirements of GDC 10 has been adequately addressed for the SB&PC system.

GDC 13 requires providing instrumentation to monitor variables and systems over their anticipated ranges for normal operation, AOOs, and accident conditions to assure adequate safety. GDC 13 also requires providing appropriate controls to maintain these variables and systems within prescribed operating ranges. The NRC staff evaluated whether GDC 13 has been adequately addressed for the SB&PC system. DCD, Tier 2, Sections 7.7.5.2 and 7.7.5.6, specify the SB&PC system manual and automatic controls and status indications. An example is that the MCRP operator interface within the N-DCIS contains controls needed for SB&PC system operation. DCD, Tier 2, Section 7.7.5.3.2, indicates conformance to GDC 13. DCD, Tier 1, Section 2.2.9, includes ITAAC for the applicant to verify that the as-built SB&PC system implements the required automatic functions and operator controls. The NRC staff reviewed monitoring and controls provided for the plant transient response to normal load changes and AOOs under (3) of Section 7.7.5.2.1 of this report and found them acceptable. The NRC staff concludes that the SB&PC system is capable of maintaining system variables within prescribed operating ranges and capable of contingency actions if such variables reach limiting conditions. Accordingly, based on identified SB&PC system monitoring and controls and their verification in the ITAAC, the NRC staff finds that the requirements of GDC 13 have been adequately addressed for the SB&PC system.

GDC 15 requires that the reactor coolant system and associated auxiliary, control, and protection systems shall be designed with sufficient margin to ensure that the design conditions of the RCPB are not exceeded during any condition of normal operation, including AOOs. The NRC staff evaluated whether GDC 15 has been adequately addressed for the SB&PC system. SRP Appendix 7.1-A for GDC 15 states that the NRC staff review should evaluate the I&C system contributions to design margin for reactor coolant systems. The NRC staff reviewed DCD, Tier 2, Section 7.7.5, and DCD, Tier 1, Section 2.2.9, for the features of manual and automatic control described in the SB&PC system I&C that facilitate the capability to maintain plant variables within prescribed operating limits and over their anticipated ranges for normal operation, for AOOs, and for accident conditions as appropriate to assure adequate safety. DCD, Tier 2, Sections 7.7.5.2 and 7.7.5.6, specifies the SB&PC system manual and automatic controls and status indications. Examples are the control signals provided to the TGCS to control the TCVs and the SB&PC system control of the TBVs. DCD, Tier 1, Section 2.2.9, includes the ITAAC for the applicant to verify that the as-built SB&PC system implements the required automatic functions and operator controls. Accordingly, based on the identified the SB&PC system I&C and their verification in the ITAAC, the NRC staff finds that the requirements of GDC 15 have been adequately addressed for the SB&PC system.

GDC 19 requires control room functionality, control room habitability, and remote shutdown capability. The NRC staff evaluated whether GDC 19 has been adequately addressed for the SB&PC system. In Section 7.1.1.3.6 the NRC staff evaluated that GDC 19 has been adequately addressed with the exception of the operation of specific I&C systems. SRP

Appendix 7.1-A states that the review should evaluate if there exists I&C available to operate the nuclear power unit under normal and accident conditions. DCD, Tier 2, Section 7.7.5.3.2 specifies that the SB&PC conforms to GDC 19. DCD, Tier 2, Section 7.7.5.6.3, provides information on the SB&PC system for performance monitoring in the MCR through the N-DCIS. DCD, Tier 2, Sections 7.7.5.2 and 7.7.5.6, specifies the SB&PC system manual and automatic controls and status indications. DCD, Tier 1, Section 2.2.9, includes the ITAAC for the applicant to verify that the as-built SB&PC system implemented the required automatic functions and operator controls. Based on the above, including the features for manual and automatic control described in DCD, Tier 2, Section 7.7.5, the NRC staff finds that the requirements of GDC 19 have been adequately addressed for the SB&PC system.

DCD, Tier 2, Section 7.7.1.1.2, identifies that the SB&PC system controls reactor pressure during plant startup, power operation, and shutdown modes. While pressure does affect reactivity, pressure is not a primary control function compared to functions controlled by RC&IS and FWCS. Accordingly, the SB&PC system is not a reactivity control system and the NRC staff accepts that GDC 28 and 29 are not applicable to the SB&PC system.

Therefore, the NRC staff finds the SB&PC system adequately addresses the relevant regulatory criteria listed in Section 7.7.0.1 above for a non-safety system and that there is reasonable assurance that this system will be able to accomplish its designed function in a reliable manner, when built and tested according to DCD Tier 2 and DCD, Tier 1 ITAAC.

7.7.5.3 Conclusion

Based on the above, NRC staff concludes there is reasonable assurance that the SB&PC system conforms to the applicable requirements, which include GDC 1, 10, 13, 15, 19, and 24, 10 CFR 52.47(b)(1), 10 CFR 50.55a(a)(1), and 10 CFR 50.55a(h); adequate high level functional requirements are identified, and sufficient ITAAC are included in Tier 1 to verify that the design is completed in compliance with the applicable requirements.

7.7.6 Neutron Monitoring System - Nonsafety Subsystems

7.7.6.1 Summary of Technical Information

The non-safety portion of the NMS, (NMS(N)) has two non-safety subsystems, the AFIP subsystem and the MRBM subsystem. The AFIP subsystem is intended as an upgraded replacement for the traversing incore probe (TIP) or automated traversing incore probe (ATIP) used in the current BWR fleet.

7.7.6.1.1Automated Fixed Incore Probe

The purpose of the AFIP subsystem is to provide sufficient axial and radial neutron flux monitoring to support the determination of three-dimension core power distribution, and to provide a automated mode of LPRM calibration by direct interface with the plant computer function of the N-DCIS.

The AFIP subsystem comprises AFIP subsystem sensors and their associated cables, as well as the signal processing electronic unit. The AFIP subsystem sensors, unlike the former TIP and ATIP, are installed permanently within the LPRM assemblies. In each LPRM assembly in the core, there are seven AFIP subsystem sensors evenly distributed axially along the LPRM assembly. Consequently, there are AFIP subsystem sensors at and between all LPRM

locations. The AFIP subsystem sensor cables are routed within the LPRM assembly and then out of the RPV through the LPRM assembly penetration to the vessel. The AFIP subsystem generates signals proportional to the axial power distribution at the radial core locations of the LPRM detector assemblies. The AFIP subsystem signal range is sufficiently wide to accommodate the corresponding local power range from approximately 1 percent to 125 percent of reactor rated power.

The AFIP subsystem data collection and processing sequences are fully automated, with manual control available. The AFIP subsystem signals are used to calibrate the LPRM detectors and to determine the power distribution in the reactor core and the reactor protection parameters.

The power for the AFIP subsystem is supplied from the non-safety instrument 120-VAC supply power source. The power for the AFIP subsystem logic is supplied from redundant, non-safety instrument 120-VAC UPS.

7.7.6.1.2 Multichannel Rod Block Monitor

The purpose of the MRBM subsystem is to monitor signals from the systems that observe the neutron flux and to provide a signal to the RC&IS to block rod movement if the MRBM subsystem signal exceeds a preset rod block setpoint to prevent fuel damage.

The MRBM subsystem logic receives input signals from the LPRMs and the APRMs of the NMS. It also receives control rod status data from the RAPI subsystem of the RC&IS to determine when rod withdrawal blocks are required. The MRBM subsystem uses the LPRM signals to detect local power change during the rod withdrawal. If the MRBM subsystem signal, which is based on averaged LPRM signals, exceeds a preset rod block setpoint, a control rod block demand is issued. The MRBM subsystem monitors the core in 4-by-4 fuel bundle regions where control rods are being withdrawn. The MRBM subsystem algorithm covers the monitoring of multiple regions simultaneously depending upon the size of the gang of rods being withdrawn. Because it monitors more than one region, it is called the multichannel rod block monitor compared to the original single channel rod block monitor. The MRBM subsystem is a dual channel system and it is not a safety system.

The power supply for the MRBM subsystem is from the non-safety 120-VAC uninterruptible buses in two different load groups.

7.7.6.2 Staff Evaluation

7.7.6.2.1 Evaluation of NMS(N) Conformance with Acceptance Criteria

The major design considerations per SRP Section 7.7 are in Section 7.7.0.3 of this report and discuss the attributes that are common to the control systems of DCD, Tier 2, Section 7.7. This section will discuss and evaluate only those major design considerations and information that are unique to the NMS(N).

Design Basis:

For “Design Basis,” the NMS(N) has two non-safety subsystems, the AFIP subsystem and the MRBM subsystem. Once the RPS senses a condition requiring actuation of the reactor protection features, neither the AFIP subsystem nor the MRBM subsystem are required to shut

down the reactor or maintain it in a safe state. Thus, neither the AFIP subsystem nor the MRBM subsystem performs or ensures any safety function; therefore, the AFIP subsystem and MBRM subsystems have no safety design basis. However, these systems are important to overall safe operation of the plant. The AFIP subsystem provides axial and radial neutron flux distribution to support the determination of three-dimension core power distribution, sufficient axial neutron flux monitoring with corresponding axial position, and a totally automated mode of LPRM calibration by direct interface with the plant computer function of the N-DCIS. Other than providing input, the AFIP subsystem has no control function. The MRBM subsystem monitors control rod movement, issues a rod block signal to the RC&IS to block rod movement if the MRBM subsystem signal exceeds a preset rod block setpoint to prevent fuel damage, and provides values to the N-DCIS. Other than this rod block function, the MRBM subsystem has no other control function. The NRC staff finds that the NMS(N) includes the necessary features to support manual and automatic control of process variables within prescribed operating limits. Accordingly, based on the above and DCD, Tier 2, Section 7.7.6 and the verification of these controls and functions through applicable DCD, Tier 1, Section 2.2.5, Table 2.2.5-4, ITAAC, the NRC staff finds that the design bases have been adequately addressed for the NMS(N)

Effects of Control System Operation on Accidents:

For “Effects of NMS(N) System Operation on Accidents,” the NRC staff reviewed DCD, Tier 2, Section 7.7.6 and Chapter 15, for the effects of NMS(N) operation on accidents. The NRC staff verified that the safety analysis includes consideration of the effects of both NMS(N) system action and inaction in assessing the transient response of the plant for accidents and AOOs. Again, the NMS(N) is a monitoring system with no direct control other than issuing rod blocks. The MRBM subsystem provides regional and axial neutron flux monitoring and issues a rod block order to the RC&IS if a MRBM subsystem parameter limit is exceeded as a preemptive function to prevent a reactor scram during a control rod withdrawal error. In DCD, Tier 2, Chapter 15, Table 15.1-6, identifies that during control rod withdrawal error there are four sources that could provide a rod block depending on the reactor power level: SRNM Period, RWM, ATLM , and the MRBM. The control rod withdrawal error events are: (1) Control Rod Withdrawal Error during Power Operation with ATLM Failure, (2) Control Rod Withdrawal Error During Power Operation, (3) Control Rod Withdrawal Error During Startup, and (4) Control Rod Withdrawal Error During Refueling. Credit is taken that one of the rod block sources, as MRBM, is sufficient to mitigate any of these four control rod withdrawal errors. Even though the MRBM subsystem is credited in mitigating these four transients, the safety analysis does not depend on the MRBM subsystem for safe shutdown of the nuclear reactor as the safety function is provided by the SRNM Period rod block. The AFIP subsystem data is used to assist in calculating neutron flux distribution, bundle and sub-bundle powers, to calibrate the LPRM. While the AFIP subsystem may provide useful information on the neutron flux distribution in a transient investigation, there is no rod block from the AFIP subsystem or credit taken in the safety analysis of DCD, Tier 2, Chapter 15. Inaction of the AFIP subsystem or MRBM subsystem would indicated a failed component and is covered under (4) below. Based on the above, a review of DCD, Tier 2, Section 7.7.6 and Chapter 15, and as described under the effects of control system failures below, the NRC staff finds that the safety analysis includes consideration of the effects of both NMS(N) system action and inaction in assessing the transient response of the plant for accidents and AOOs.

Effects of Control System Failures:

For “Effects of NMS(N) System Failures,” the NRC staff reviewed DCD, Tier 2, Chapters 15 and Section 7.7.6, for the effects of NMS(N) failures. The NRC staff verified that the failure of any

NMS(N) system component does not cause plant conditions more severe than those described in the analysis of AOOs in DCD, Tier 2, Chapter 15. The effect of a complete failure of MRBM subsystem removes one of the four different functions that is a potential source of a rod block in case of a control rod withdrawal error. Which function would actually provide the rod block is dependent on reactor power. As discussed under the effects of control system operation on accidents above, there are four control rod withdrawal error events noted in DCD, Tier 2, Table 15.1-6, in which any one of the rod blocks would be sufficient to mitigate the event without requiring a reactor scram. DCD, Tier 2, Table 15.1-6, shows that the bounding condition for a complete failure of MRBM subsystem during reactor startup is the transient labeled, "Control Rod Withdrawal Error During Startup With Failure of Control Rod Block," that is mitigated by the SRNM Period Scram. During power operation, the ATLM is the primary protective rod block on a control rod withdrawal error and the MRBM subsystem is the secondary source for a rod block.

DCD, Tier 2, Table 15.1-6, also shows the control rod withdrawal error event labeled, "Control Rod Withdrawal Error during Power Operation with ATLM Failure," that is mitigated by the MRBM subsystem rod block (assuming above the RWM controlled region). Assuming that both the dual redundant MRBM subsystem and the dual redundant ATLM both fail at the same time is beyond design basis and the single failure criteria. If the MRBM subsystem fails, the ATLM is still available. In general, if the MRBM subsystem fails such that a rod block is not given when required, and the operator does not detect and correctly identify the problem, and take appropriate action, then either an alternate rod block or the RPS would have to respond. A failed MRBM subsystem issuing an erroneous control rod block is in the conservative direction.

A massive failure of the AFIP subsystem logic that would provide some incorrect data would be a problem worse than a failure to provide any data. Again this would not stop a scram. Testing, self-diagnostic, continued operation, data comparison, and defense in depth significantly reduce the probability of such an event. The AFIP subsystem is a passive monitoring system, and does not directly control the control rods or equipment. Also, there are TS criteria for the number of permitted failed AFIP subsystem detectors and their location. Based on the above, DCD, Tier 2, Section 7.7.6 and Chapter 15, Tables 15.1-5 and 15.1-6, the NRC staff finds that the occurrences and events discussed in DCD, Tier 2, Chapter 15, bound any failures of the NMS(N) and, therefore, the NRC staff finds that failures of the NMS(N) do not cause plant conditions more severe than those described in DCD, Tier 2, Chapter 15. In RAI 7.7-12, the NRC staff requested that the applicant provide analyses that evaluate the effects of control systems failures. RAI 7.7-12 was being tracked as an open item in the SER with open items. In response, the applicant stated that the non-safety subsystems of the AFIP subsystem and MRBM subsystem, are assumed to be operational in Chapter 15 analysis. The applicant does not specifically analyze the individual failures of these systems since in applying the single failure criteria, if the ATLM is not available, then the MRBM subsystem would be available; and if the MRBM subsystem failed, then ATLM would be available. However, as discussed above, the applicant does analyze a bounding failure of these systems since the applicant analyzes in DCD, Tier 2, Chapter 15 a control rod withdrawal error during startup with failure of control rod block, In the unlikely failure of all rod blocks, the safety systems would act to prevent or mitigate an accident. The NRC staff determined the response was acceptable since DCD, Tier 2, Chapter 15 includes events that bound the failures of the NMS(N). Based on the above and the applicant's response, RAI 7.7-12 regarding the NMS(N) is resolved.

Effects of Control System Failures Caused by Accidents:

For "Effects of NMS(N) Failures Caused by Accidents," the NRC staff reviewed DCD, Tier 2,

Chapters 15 and Section 7.7.6, for the effects of NMS(N) failures caused by accidents. The NMS(N) consists of cabinets, or panels, that contain special electronic/electrical equipment modules for performing the NMS(N) logic in the reactor building and control building. Accidents could potentially damage AFIP subsystem cabling under the RPV. Even if all cables were destroyed, the reactor scram would not be affected. Sensors and transmitters providing input to the NMS(N) could be damaged. Fire or earthquake potential could cause one or more functions to fail and damage the electronic equipment causing an NMS(N) function to fail. The potential for such effects is significantly reduced through D3 in NMS(N) sensors, NMS(N) environmental EQ, redundant modules in different cabinets, and a fire protection design. Based on the above, DCD, Tier 2, Section 7.7.6, Chapter 15, and failures discussed under the effects of control system failures above, the NRC staff finds that the consequential effects of AOOs and accidents do not lead to NMS(N) failures that would result in consequences more severe than those described in DCD, Tier 2, Chapter 15. Based on the above, the NRC staff finds that the effects of NMS(N) failures caused by accidents have been adequately addressed.

Potential for Inadvertent Actuation:

For “Potential for Inadvertent Actuation,” the NRC staff reviewed DCD Chapter 7.7.6 to identify design measures that limit the potential for inadvertent actuation. Examples of such design features are as follows:

The design has seven gamma thermometer (GT) type neutron detectors per LPRM string and LPRM strings distributed throughout the reactor core. This large number of GT detectors distributed throughout the reactor core allows a limited number of failed GT detectors before the entire AFIP is considered inoperable. The loss of a limited number of detector GTs, while undesirable, can be tolerated in support of D3. There are TS criteria for the number of GT detectors permitted failed and their location.

The MRBM subsystem is effectively a D3 feature. If the MRBM subsystem does not provide a control rod block when rod movements exceed rod movement restrictions, an alternate rod block could be generated by the SRNM fast period, RWM, ATLM, or APRM of the NMS(N) (safety portion). The MRBM subsystem logic can issue a rod block signal used in the RC&IS logic to enforce rod blocks. The logic attempts to anticipate situations from the NMS signals that are approaching or may approach an unsafe condition and attempts to act before the NMS signal requires a reactor scram. The rod blocks prevent fuel damage by ensuring that the MCPR and MLHGR do not violate fuel thermal safety limits. Once a rod block is initiated, manual action is required by the operator to reset the system. Further, the MRBM subsystem is a dual channel system with the power supply from the non-safety 120-VAC uninterruptible buses in two different load groups,

Based on the above, the NRC staff finds that the NMS(N) design limits the potential for inadvertent actuation.

7.7.6.2.2. Evaluation of NMS(N) Compliance with Regulations

The common design attributes and methods for complying with the regulations required by SRP Section 7.7 for control systems of DCD, Tier 2, Section 7.7 are listed and discussed in Section 7.7.0.4 of this report. This section will discuss and evaluate only those regulations with unique methods of compliance for the NMS(N).

For “Compliance with 10 CFR 52.47(b)(1),” the NRC staff reviewed DCD, Tier 2, Section 7.7.6, and DCD, Tier 1, Section 2.2.5, in accordance with SRP Sections 7.7 and 14.3.5, to verify that 10 CFR 52.47(b)(1) has been adequately addressed for the NMS(N) as non-safety subsystems. DCD, Tier 1, Section 2.2.5, documents the Neutron Monitoring System ITAAC requirements. While NMS(N) has no DAC, the DCD, Tier 1, Table 2.2.5-4, defines AFIP and MRBM subsystem as non-safety subsystems of the NMS and verifies the MRBM subsystem main channel bypasses. Accordingly, based on information in DCD, Tier 1, Section 2.2.5, Table 2.2.5-4, and DCD, Tier 2, Chapter 7, information discussed herein and identified NMS(N) I&C and their verification in the ITAAC, the NRC staff finds that the requirements of 10 CFR 52.47(b)(1) have been adequately addressed for these non-safety subsystems.

For “Compliance GDC 10, 13, 15, 19, 28, and 29,” the NRC staff reviewed DCD, Tier 2, Section 7.7.6, to verify that the applicable GDC specified in SRP Section 7.7 have been adequately addressed for the NMS(N) as a non-safety system. DCD, Tier 2, Section 7.7.3.3.2, states that the NMS(N) conforms to GDC 13, 19, 28, and 29.

GDC 10 requires that the reactor core, associated coolant, control, and protection systems 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. The NRC staff evaluated whether GDC 10 has been adequately addressed for the NMS(N). SRP Appendix 7.1-A for GDC 10 states that the NRC staff review should evaluate the I&C system contributions to design margin for reactor core and coolant systems. The AFIP subsystem is a fully automated measurement, data collection, data amplification, and calculation subsystem. The AFIP subsystem collects three-dimensional neutron flux readings and uses these in the calibration of the LPRMs. The subsystem is also a measurement of neutron flux and calculation subsystem to support control rod movement monitoring. Since the NMS(N) does not control any parameter directly that may affect reactor core or associated coolant system margins and NMS(N) is addressed in GDC 13 instrumentation requirements, the NRC staff accepts that GDC 10 is not applicable to the NMS(N).

GDC 13 requires providing instrumentation to monitor variables and systems over their anticipated ranges for normal operation, AOOs, and accident conditions to assure adequate safety. GDC 13 also requires providing appropriate controls to maintain these variables and systems within prescribed operating ranges. The NRC staff evaluated whether GDC 13 has been adequately addressed for the NMS(N). The AFIP subsystem is a fully automated measurement, data collection, data amplification, and calculation subsystem. The AFIP subsystem collects three-dimensional neutron flux readings and uses these in the calibration of the LPRMs. Other than providing input, the AFIP subsystem has no control function. The MRBM subsystem is also a measurement of neutron flux and calculation subsystem to support control rod movement monitoring. Other than this rod block function, the MRBM subsystem has no other control function. DCD, Tier 2, Section 7.7.6.2, specify the automatic and manual controls of the AFIP subsystem and MRBM. DCD, Tier 2, Section 7.7.6.3.2, indicates conformance to GDC 13. DCD, Tier 1, Section 2.2.5, includes ITAAC for the applicant to verify that the as-built NMS(N) implements the required automatic functions and operator controls. Based on the above, DCD, Tier 2, Section 7.7.6, and verification in the ITAAC, the NRC staff finds that that GDC 13 has been adequately addressed.

GDC 15 requires that the reactor coolant system and associated auxiliary, control, and protection systems shall be designed with sufficient margin to ensure that the design conditions of the RCPB are not exceeded during any condition of normal operation, including AOOs. The NRC staff evaluated whether GDC 15 has been adequately addressed for the NMS(N). SRP

Appendix 7.1-A for GDC 15 states that the NRC staff review should evaluate the I&C system contributions to design margin for reactor coolant systems. DCD, Tier 2, Section 7.7.6.3.2, does not state conformance to GDC 15. The AFIP subsystem is a fully automated measurement, data collection, data amplification, and calculation subsystem. The AFIP subsystem collects three-dimensional neutron flux readings and uses these in the calibration of the LPRMs. The MRBM subsystem is also a measurement of neutron flux and calculation subsystem to support control rod movement monitoring. Since the NMS(N) does not control any parameter that may affect RCPB margins, the NRC staff finds that GDC 15 is not applicable to the NMS(N).

GDC 19 requires control room functionality, control room habitability, and remote shutdown capability. The NRC staff evaluated whether GDC 19 has been adequately addressed for the NMS(N). In Section 7.1.1.3.6 the NRC staff evaluated that GDC 19 has been adequately addressed with the exception of the operation of specific I&C systems. SRP Appendix 7.1-A states that the review should evaluate if there exists I&C available to operate the nuclear power unit under normal and accident conditions. DCD, Tier 2, Section 7.7.6.3.2, specifies that the NMS(n) conforms to GDC 19. The AFIP subsystem automatically collects important data and passes it on to the MCR and the Process Computer Function. The AFIP subsystem is a fully automated measurement, data collection, data amplification, and calculation subsystem. The AFIP subsystem collects three-dimensional neutron flux readings and uses these in the calibration of the LPRMs. Other than providing input, the AFIP subsystem has no control function. The MRBM subsystem is also a measurement of neutron flux and calculation subsystem to support control rod movement monitoring. Other than this rod block function the MRBM subsystem has no other control function. There are bypass controls in the MCR for the MRBM. DCD, Tier 2, Section 7.7.6.2, specify the automatic and manual controls of the AFIP subsystem and the MRBM. DCD, Tier 1, Section 2.2.5, includes the ITAAC for the applicant to verify that the AFIP and MRBM subsystem are implemented as non-safety subsystems in the Neutron Monitoring System Based on this above, DCD, Tier 2, Section 7.7.6, and verification by DCD, Tier 1, Section 2.2.5, ITAAC, the NRC staff finds that the requirements of GDC 19 have been adequately addressed.

GDC 28 requires that reactivity control systems be designed with appropriate limits on the potential amount and rate of reactivity increase. The NRC staff evaluated whether GDC 28 has been adequately addressed for the NMS(N). SRP Appendix 7.1-A states that GDC 28 imposes functional requirements on I&C interlock and control systems to the extent they are provided to limit reactivity increases to prevent or limit the effect of reactivity accidents. DCD, Tier 2, Section 7.7.6.3.2, specifies that the NMS(N) conforms to GDC 28. The MRBM subsystem provides a direct protective control function through the MRBM subsystem rod block when rod movement restrictions are violated. The AFIP subsystem is a monitoring and measurement system essential for calibrating the LPRM and providing the data for determining the core power distribution and thus the RPS protective parameters. The MRBM subsystem is an anticipatory defense system to protect the reactor core. In DCD, Tier 2, Chapter 15, and Tables 15.1-5 and 15.1-6, identify actuations and other actions that reduce the need for the actuation of protection and safety systems to mitigate AOOs. DCD, Tier 2, Section 7.7.6, includes functions of the NMS(N) that significantly contribute to the design bases of the NMS(N) to maintain the reactor core and the reactivity limits within appropriate margins and to mitigate AOOs. An example is the rod block protective function of the MRBM. DCD, Tier 1, Section 2.2.5, includes ITAAC to verify that the AFIP and MRBM subsystem are implemented as non-safety subsystems in the Neutron Monitoring System. Accordingly, based on the identified NMS(N) actions and their verification in the ITAAC, the NRC staff finds that the requirements of GDC 28 have been adequately addressed for the NMS(N).

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. The NRC staff evaluated whether GDC 29 has been adequately addressed for NMS(N). SRP Appendix 7.1-A, identifies that GDC 29 is addressed by conformance, as applicable, to GDC 20-25 and GDC 28. Since the NMS(N) is a reactivity control system and not a protection system, GDC 20-23 and 25, which are requirements for protection systems, are not applicable to the NMS(N), Accordingly, GDC 29 is addressed by conformance as applicable to GDC 24 and 28. Conformance of N-DCIS control systems to GDC 24, including the NMS(N), is evaluated in Section 7.7.0.4 of this report. Conformance of the NMS(N) to GDC 28 is evaluated above. DCD, Tier 2, Section 7.7.6.3.2, specifies that the NMS(N) conforms to GDC 29. In addition, DCD, Tier 1, Section 2.2.5, includes ITAAC to verify that the AFIP and MRBM subsystem are implemented as non-safety subsystems in the NMS. Based on the information above and requirements of GDC 24 and 28 having been adequately addressed for the NMS(N), the NRC staff finds that the requirements of GDC 29 have been adequately addressed for the NMS(N).

Therefore, the NRC staff finds the NMS(N) adequately addresses the relevant regulatory criteria listed in Section 7.7.0.1 above for a non-safety system and that there is reasonable assurance that this system will be able to accomplish its designed function in a reliable manner, when built and tested according to DCD Tier 2 and DCD Tier 1 ITAAC.

7.7.6.3 Conclusion

Based on the above, NRC staff concludes there is reasonable assurance that the NMS(N) made up of the AFIP subsystem and the MRBM subsystem, conforms to the applicable requirements, which include GDC 1, 13, 19, 24, 28, and 29, 10 CFR 52.47(b)(1), 10 CFR 50.55a(a)(1), and 10 CFR 50.55a(h); adequate high level functional requirements are identified, and sufficient ITAAC are included in Tier 1 to verify that the design is completed in compliance with the applicable requirements.

7.7.7 Containment Inerting System

7.7.7.1 Summary of Technical Information

The objective of the CIS is to preclude combustion of hydrogen and prevent damage to essential equipment and structures by providing an inerted containment environment. The CIS is designed to establish an inert atmosphere (i.e., less than 4% oxygen by volume) throughout the containment in less than 4 hours and less than 2% oxygen by volume in the next 8 hours following an outage. The CIS is also designed to maintain the containment oxygen concentration below the maximum permissible limit (4 %) during normal power operation to ensure an inert atmosphere. The purpose of the CIS is to provide an inert containment atmosphere (≤ 3% oxygen) during normal operation to minimize hydrogen burn inside the containment in case of an event that would release hydrogen. The CIS is capable of reaching a volumetric oxygen concentration of ≥ 19% within 12 hours after de-inerting begins. Further details are provided in DCD, Tier 2, Sections 7.7.7 and 6.2.5.2. A simplified CIS system diagram is shown in DCD, Tier 2, Figure 6.2-29. Further, the CIS is designed to maintain a positive pressure in the primary containment during normal, abnormal, and accident conditions.

The CIS I&C is provided to monitor the process variables and operate the system processes during startup, normal, and abnormal reactor operation. The CIS is operated from the MCR.

7.7.7.2 Staff Evaluation

7.7.7.2.1 Evaluation of CIS Conformance with Acceptance Criteria

The major design considerations per SRP Section 7.7 are in Section 7.7.0.3 of this report and discuss the attributes that are common to the control systems of DCD, Tier 2, Section 7.7. This section will discuss and evaluate only those major design considerations and information that are unique to the CIS.

Design Basis:

For "Design Basis," the CIS is not a safety system except for the containment isolation function which is outside the scope of this evaluation. The CIS is not required for safe shutdown of the plant. Therefore, the CIS has no safety design basis. Failure of the non-safety I&C components does not adversely affect any safety function. The CIS does have a power generation (non-safety) design basis. The non-safety design basis of the CIS is to establish and maintain an inert atmosphere in the containment, to maintain a positive pressure in the containment, and to perform continuous leakage rate monitoring. The NRC staff finds that the CIS includes the necessary features for manual and automatic control of process variables within prescribed operating limits.

Effects of Control System Operation on Accidents:

For "Effects of CIS Operation on Accidents," the NRC staff reviewed DCD, Tier 2, Sections 6.2.5.2 and 7.7.7 and Chapter 15, for the effects of CIS operation on accidents. During AOOs and accident conditions, the containment inerting function is passive and does not require the operation of the CIS. CIS can be used under post accident conditions for containment atmosphere dilution to maintain inert conditions. CIS in-action indicates a failed component and is discussed below. Based on the above, a review of DCD, Tier 2, Sections 6.2.5.2 and 7.7.7, and Chapter 15, the NRC staff finds the effect of CIS on accidents is adequately addressed.

Effects of Control System Failures:

For "Effects of CIS System Failures," the NRC staff reviewed DCD, Tier 2, Sections 6.2.5.2, Section 7.7.7 and Chapter 15, for the effects of CIS failures. Even if CIS functions failed, a reactor shut down to a safe condition would not be prevented. During AOOs and accident conditions, the containment inerting function is passive and does not require the operation of the CIS. In the case of certain failures, significant portions of the CIS equipment can be operated locally and manually as a backup, as well as from the MCR. Based on the above, a review of DCD, Tier 2, Sections 6.2.5.2 and 7.7.7, and Chapter 15, the NRC staff finds the effects of CIS on accidents is adequately addressed.

Effects of Control System Failures Caused by Accidents:

For "Effects of CIS Failures Caused by Accidents," the NRC staff reviewed DCD, Tier 2, Sections 6.2.5.2 and 7.7.7 and Chapter 15, for the effects of CIS failures caused by accidents. Accidents could potentially damage CIS I&C cabling, controls in cabinets, monitors, sensors, and transmitters. Fire or earthquake potential could cause damage to electronic equipment causing one or more CIS functions to fail. Even if CIS functions failed, a reactor scram would not be prevented. The potential for such effects is significantly reduced through environmental

and a fire protection design. The CIS instrument lines penetrating containment comply with the guidance of RG 1.151. Based on the above, DCD, Tier 2, Sections 6.2.5.2 and 7.7.7, Chapter 15, and failures discussed above the NRC staff finds that the consequential effects of AOOs and accidents do not lead to CIS failures that would result in consequences more severe than those described in DCD, Tier 2, Chapter 15. Based on the above, the NRC staff finds that the effects of CIS failures caused by accidents have been adequately addressed.

Potential for Inadvertent Actuation:

For "Potential for Inadvertent Actuation," the NRC staff reviewed DCD, Tier 2, Sections 6.2.5.2 and 7.7.7, to identify design measures that limit the potential for inadvertent actuation. Examples of such design features are as follows:

In the case of certain failures, significant portions of the CIS equipment can be operated locally as a backup as well as from the MCR. Operator training and operating procedures are the expected method to reduce inadvertent actuation. The CIS cannot adversely affect the safety systems. Unlike many of the other control systems of DCD, Tier 2, Section 7.7, an inadvertent actuation of the CIS is not as serious as it would be for many other systems. This system is used to meet technical specifications requirements for some of the parameters as the maximum permissible limit (4 %) on oxygen in the containment during normal power operation. The NRC staff finds that inadvertent actuation has been adequately addressed for the CIS.

7.7.7.2.2 Evaluation of Containment Inerting System Compliance with Regulations

The common design attributes and methods for complying with the regulations required by SRP Section 7.7 for control systems of DCD, Tier 2, Section 7.7 are listed and discussed in Section 7.7.0.4 of this report. This section will discuss and evaluate only those regulations with unique methods of compliance for the CIS.

For "Compliance with 10 CFR 52.47(b)(1)," the NRC staff reviewed DCD, Tier 2, Sections 6.2.5.2 and 7.7.7 and DCD, Tier 1, Section 2.15.5, in accordance with SRP Sections 7.7 and 14.3.5, to verify that 10 CFR 52.47(b)(1) has been adequately addressed for the CIS. DCD, Tier 1, Section 2.15.5, documents the CIS ITAAC requirements, which include verifying that the containment can be inerted to less than or equal to 4% oxygen by volume and that the drywell temperature indications are retrievable in the main control room. The staff determined that additional ITAAC on control functions are not needed since the CIS has no safety functions and it is not required by regulation. Based on information reviewed in DCD Tier 1, DCD, Tier 2, Chapters 6 and 7, information discussed herein and identified CIS I&C and their verification in the ITAAC, the NRC staff finds that the requirements of 10 CFR 52.47(b)(1) have been adequately addressed.

For "Compliance with GDC 10, 13, 15, 19, 28, and 29," the NRC staff reviewed DCD, Tier 2, Sections 6.2.5.2 and 7.7.7, to verify that the applicable GDC specified in SRP Section 7.7 have been adequately addressed for the CIS as a non-safety system. DCD, Tier 2, Section 7.7.7.3.2, states that the CIS conforms to GDC 13 and 19.

GDC 10 requires that the reactor core, associated coolant, control, and protection systems 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. The NRC staff evaluated whether GDC 10 has been adequately addressed for the CIS. SRP Appendix 7.1-A for GDC 10 states that the NRC staff review should evaluate the I&C system contributions to

design margin for reactor core and coolant systems. The CIS is a system used to assure that the atmosphere in the containment is inerted with nitrogen gas to displace the oxygen and remove the possibility of a hydrogen/oxygen explosion. The CIS does not have any functions associated with reactor reactivity control, the reactor coolant boundary, or cooling water and associated AOOs. GDC 10 is associated with reactor design and is not applicable to the CIS.

DCD, Tier 2, Section 7.7.7.3.2, states that the CIS conforms to GDC 13. The CIS operation is manually or automatically activated from the MCR by aligning corresponding valves through remote manual control switches. The CIS has three control modes: inerting, makeup, and de-inerting. DCD, Tier 2, Section 7.7.7.5.1, specifies the automatic and manual controls for inerting and de-inerting the containment. DCD, Tier 2, Section 7.7.7.5.1, also specifies the automatic control for the makeup mode, which maintains the containment pressure. DCD, Tier 2, Section 7.7.7.5.3, specifies the alarms and status indications in the MCR to support CIS operations. During AOOs and accident conditions, the containment inerting function is passive and does not require the operation of the CIS. DCD, Tier 2, Section 7.7.7.3.2, indicates conformance to GDC 13. Based on the above, DCD, Tier 2, Sections 6.2.5.2 and 7.7.7, the NRC staff finds that the requirements for GDC 13 have been adequately addressed for CIS.

GDC 15 requires that the reactor coolant system and associated auxiliary, control, and protection systems shall be designed with sufficient margin to ensure that the design conditions of the RCPB are not exceeded during any condition of normal operation, including AOOs. The NRC staff evaluated whether GDC 15 has been adequately addressed for the CIS. SRP Appendix 7.1-A for GDC 15 states that the NRC staff review should evaluate the I&C system contributions to design margin for reactor coolant systems. GDC 15 is associated with systems having an influence on the reactor coolant system design and is not applicable to the CIS.

GDC 19 requires control room functionality, control room habitability, and remote shutdown capability. The NRC staff evaluated whether GDC 19 has been adequately addressed for the CIS. In Section 7.1.1.3.6 the NRC staff evaluated that GDC 19 has been adequately addressed with the exception of the operation of specific I&C systems. SRP Appendix 7.1-A states that the review should evaluate if there exists I&C available to operate the nuclear power unit under normal and accident conditions. DCD, Tier 2, Section 7.7.7.3.2, specifies that the CIS conforms to GDC 19. DCD, Tier 2, Section 7.7.7.5.1, describes the CIS logic, interlocks, and general I&C. The CIS operation is manually or automatically activated from the MCR by aligning corresponding valves through remote manual control switches. The CIS has three control modes: inerting, makeup, and de-inerting. DCD, Tier 2, Section 7.7.7.5.1, specifies logic and interlocks for the automatic and manual controls for inerting and de-inerting the containment. DCD, Tier 2, Section 7.7.7.5.1, also specifies the automatic control for the makeup mode, which maintains the containment pressure. DCD, Tier 2, Section 7.7.7.5.2, specifies instrumentation and controls including Drywell pressure sensors, containment temperature and humidity sensors, flow metering devices, oxygen analyzers, and interfaces with other systems. DCD, Tier 2, Section 7.7.7.5.3, specifies the alarms and status indications in the MCR to support CIS operations. During AOOs and accident conditions, the containment inerting function is passive and does not require the operation of the CIS. Based on the above, DCD, Tier 2, Sections 6.2.5.2 and 7.7.7, the NRC staff finds that the requirements for GDC 19 have been adequately addressed for the CIS.

GDC 28 requires that reactivity control systems be designed with appropriate limits on the potential amount and rate of reactivity increase. The NRC staff evaluated whether GDC 28 has been adequately addressed for the CIS. GDC 28 is associated with systems having an influence on reactivity control and is not applicable to the CIS.

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. The NRC staff evaluated whether GDC 29 has been adequately addressed for the CIS. GDC 29 is associated with systems having an influence on the RPS and reactivity control and is not applicable to CIS.

Therefore, the NRC staff finds that the CIS, adequately addresses the relevant regulatory criteria listed in Section 7.7.0.1 above for a non-safety system and that there is reasonable assurance this system will be able to accomplish its designed function in a reliable manner, when built and tested according to DCD Tier 2 and DCD Tier 1, ITAAC.

7.7.7.3 Conclusion

Based on the above, NRC staff concludes there is reasonable assurance that the CIS conforms to the applicable requirements, which include GDC 1, 13, 19, and 24, 10 CFR 50.55a(a)(1), and 10 CFR 50.55a(h); adequate high level functional requirements are identified, and sufficient ITAAC are included in Tier 1 to verify that the design is completed in compliance.

7.7.8 Conclusion on Control System

The NRC staff concludes that design of the control systems of DCD, Tier 2, Section 7.7, evaluated in this section is acceptable and meets the relevant requirements of GDC 1, 10, 13, 15, 19, 24, 28, and 29, 10 CFR 50.34(f), 10 CFR 50.55a(a)(1), and 10 CFR 50.55a(h). This conclusion is based on the review of the design of these non-safety control systems as described in DCD Tier 1, DCD Tier 2, and the NRC staff finding that these control systems are appropriately designed and are of sufficient quality to: 1) minimize the potential for challenges to the safety systems, 2) provide manual and automatic control features capable of maintaining system variables within prescribed operating ranges, 3) protect the instrumentation from threats within the environmental such as freezing in sensing lines, 4) protect the instrumentation from natural phenomenon, 5) provide appropriate isolation from safety systems, 6) provide enhanced reliability through redundancy, diversity, defense against potential CCFs, and minimizing the probability of inadvertent actuation, and 7) provide instrumentation and controls such that plant safety is not dependent upon the response or lack of response or failure of these control systems, but can supplement and support the features of the safety systems.

7.8 Diverse Instrumentation and Control Systems

7.8.1 Regulatory Criteria

The objectives of the review of DCD, Tier 1, Section 2.2 and Tier 2, Section 7.8, are to ensure 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 NRC staff acceptance criteria on D3 and the design of the diverse I&C systems include the ATWS mitigation system, the DPS, and the common mode failure defenses are in compliance with SRP guidance.

Acceptance criteria of the diverse I&C systems are based on meeting the relevant requirements of 10 CFR 50.55a(a)(1), 10 CFR 50.55a(h), GDC 1, 13, 19, and 24, 10 CFR 52.47(b)(1) and 10 CFR 50.62. The acceptance criteria are also based on conforming to the guidelines of IEEE Std 7-4.3.2, as endorsed by RG 1.152 and the SRM on SECY-93-087.

7.8.2 Summary of Technical Information

The ATWS mitigation system and the DPS comprise the diverse I&C systems that are part of the D3 strategy. They provide diverse backup to the RPS and the SSLC/ESF. The ATWS mitigating logic is designed to meet the diverse shutdown requirements of 10 CFR 50.62. The ATWS mitigating logic system is implemented with the Q-DCIS (ATWS/SLC) and the N-DCIS. The non-safety DPS (which is part of the N-DCIS) processes the non-safety portions of the ATWS mitigation logic. It is designed to mitigate the possibility of digital protection system CCFs discussed in the SRM on SECY-93-087, Item II.Q.

The ATWS/SLC mitigation logic provides a diverse means of emergency shutdown using the SLC system for soluble boron injection. ARI, which hydraulically scrams the plant using the air header dump valves of the CRD system, is also used for ATWS mitigation. This logic is implemented in the DPS.

The DPS is a non-safety, triple redundant system powered by redundant non-safety load group power sources. The DPS provides diverse reactor protection using diverse set of scram logics from the RPS. The DPS provides diverse emergency core cooling by independently actuating the ECCS. The DPS performs selected containment isolation functions as part of the diverse ESF function. The scope of the DPS functions is based on the D3 strategy outlined in LTR NEDO-33251.

Mitigation of CCFs is provided by the following:

- manual scram and MSIV isolation by the operator in the MCR in response to diverse parameter indications

- availability of diverse manual initiation of the passive ECCS functions including GDCS squib valve initiation, SRV initiation, DPV initiation, ICS initiation, and SLC system squib valve initiation (manual initiation functions are available in the safety systems and in the DPS)

- core makeup water capability from the condensate and feedwater system, CRD system, and FAPCS in the LPCI mode

- long-term shutdown capability in the two redundant RSS panels which are equipped with Division 1 and 2 controls for manual scram and MSIV closure, Division 1 and 2 safety VDUs, and a non-safety VDU to allow monitoring and control of all plant systems (local displays of process variables in the RSS system are continuously powered and are available for monitoring at any time)

- diverse scram, which is different from the safety RPS, using diverse hardware and software

- diverse ESF initiation logic, which is different from the SSLC/ESF, using diverse hardware and software

- ATWS mitigation using liquid boron injection for emergency plant shutdown through the SLC system

- ATWS mitigation using ARI to hydraulically scram the plant using the three sets of ARI valves of the CRD system

- SCRRI command to the RC&IS

- SRI to hydraulically insert selected control rods with every SCRRI action

- manual initiation capability of the ATWS mitigation functions (ARI/SLC/feedwater runback)

The following scram signals are selected for inclusion in the DPS:

- high RPV dome pressure
- high RPV water level (Level 8)
- low RPV water level (Level 3)
- high drywell pressure
- high suppression pool temperature
- closure of the MSIVs
- RPS scram
- SCRRI/SRI command with power levels remaining elevated

Major diverse ESF functions include the following:

- The ESF functions of the GDCS squib valves, SLC system squib valves, ICS, and ADS (SRVs and DPVs) are included in the DPS. The initiating logic is based on low RPV water level (Level 1).

- The DPS does not provide automatic initiation of the suppression pool equalizing function of the GDCS because it is not required for approximately 30 minutes. Therefore, manual suppression pool equalization capability is provided.

- The DPS also provides the ability to generate diverse manual ECCS actuation from the DPS displays. Manual controls are provided for ADS and GDCS injection sequenced initiation. The DPS does not provide automatic ADS and GDCS injection start on sustained high drywell pressure since this function is not required for 60 minutes.

- For the SRV or DPV opening function, three of the four solenoids on each SRV or DPV are powered by three of the four divisional safety power sources in the ESF ADS. A fourth solenoid on each SRV or DPV is powered by the non-safety load group, with the trip logic controlled by the DPS.

- The ICS logic is configured to allow the availability of each ICS loop flowpath from the four safety divisions and the DPS.

Automatic initiation of the ADS by the DPS is inhibited by the following signals:

- coincident low RPV water level (Level 2) and SRNM ATWS permissive signals (i.e., an SRNM signal from the NMS that is above a specified setpoint)

- coincident high RPV pressure and SRNM ATWS permissive signals that persist for 60 seconds.

The ADS inhibit logic also inhibits the ADS and GDCS injection sequenced initiation from occurring via the DPS logic. The DPS-ADS inhibit logic is also used to inhibit the DPS feedwater isolation on high-high drywell pressure. MCR controls are provided for the above inhibit logic within the DPS under ATWS conditions.

The DPS also provides the following major isolations using 2/4 sensor logic and 2/3 processing logic. The isolation functions performed as part of the diverse ESF are “energize to actuate”:

- The MSIVs are closed upon detection of high steam flow rate, low RPV pressure, or low RPV water level (Level 2). The isolation function is performed by contacts in the 120-VAC MSIV solenoid return circuit. The logic is enabled when the reactor is in run mode.

- The RWCU/SDC isolation valves are closed upon high differential flow rate.

- Isolation of the feedwater lines on a feedwater line break inside containment or LOCA conditions that pose a challenge to containment design pressure. The line break is sensed by differential pressure between feedwater lines coincident with high drywell pressure. A feedwater isolation also occurs on high-high drywell pressure or high dry well pressure coincident with high drywell water level. The DPS trips the feedwater pump adjustable speed drive motor circuit breakers and closes the feedwater containment isolation valve.

- Isolation of CRD high pressure makeup water injection on high drywell pressure coincident with high drywell level, or low level in 2/3 GDCS pools.

The following additional functions are performed by the DPS:

- With logic similar to the SSLC/ESF, the DPS initiates the ICS on high RPV dome pressure, low RPV water level (Level 2), or MSIV closure to provide core cooling.

- With logic similar to the SSLC/ESF, the DPS opens the ICS lower header vent valves after six hours of ICS initiation.

- The DPS trips the feedwater pumps upon high RPV water level (Level 9).

- The DPS opens pool cross-connect valves between the equipment storage pool and the isolation condenser/passive containment cooling expansion pools when a low level condition is detected in either IC/PCCS inner expansion pools. The DPS uses the four non-safety level sensors in each IC/PCCS inner expansion pool which are part of FAPCS.

All safety systems have displays and controls located in the MCR that provide manual system-level actuation of their safety functions and monitoring of parameters that support those safety functions.

In addition to the manual controls and displays for the safety reactor protection and SSLC/ESF functions, the DPS also has displays and manual control functions that are independent of those of the safety protection and SSLC/ESF functions. They are not subject to the same CCF as the safety protection system components. The manual controls permit manual initiation of the SRV, DPV, GDCS, and SLC system valves, and the ICS. The operator is provided with a set of diverse displays separate from those supplied through the safety software platform. The displays that provide independent confirmation of the status of major process parameters include the following:

- reactor pressure
- reactor pressure high alarm
- RPV water level
- RPV water level high alarm
- RPV water level low alarm
- drywell pressure
- drywell pressure high alarm
- drywell water level
- drywell water level high alarm
- suppression pool temperature
- suppression pool temperature high alarm
- SRV solenoid-controlled valves opening
- DPV squib-initiation valves opening
- GDCS squib-initiation valves opening
- GDCS pool level
- GDCS pool level low alarm
- SLC system squib injection valves opening
- ICS operation

In addition to the controls provided by the primary safety systems, the RSS provides manual control of shutdown cooling functions and continuous local display of monitored process parameters.

7.8.3 NRC Staff Evaluation

7.8.3.1 Evaluation of Diverse I&C Systems Compliance with Acceptance Criteria - Major Design Considerations

In accordance with SRP Section 7.8, the following are the major design considerations that are evaluated in the review of the DPS:

(1) Design Basis

The NRC staff evaluated the design bases described in the DCD for the DPS. The NRC staff evaluated whether the design bases addressed the specific design requirements identified in 10 CFR 50.62, as applicable. The NRC staff evaluation of 10 CFR 50.62 is in Section 7.8.3.2 and 7.1.1.3.4, Item (10) of this report, including an evaluation of the design requirements, which finds that 10 CFR 50.62 has been adequately addressed. DCD, Tier 2, Section 7.8.1, provides system description for the systems comprising the ATWS mitigation system and the DPS. The DPS provides backup to the RPS and the SSLC/ESF. The ATWS mitigating logic is designed to

meet the diverse shutdown requirements of 10 CFR 50.62. The ATWS mitigating logic system is implemented with the ATWS/SLC and the N-DCIS.

The NRC staff evaluated whether the design bases identify the conditions that require protective action by the DPS. As identified in DCD, Tier 2, Section 9.3, the failure of control rods to insert in response to a valid trip demand is assumed. ATWS mitigation logic is provided to initiate the ATWS/SLC system if an SRNM power permissive exists. A delay provides sufficient time for completion of the other ATWS mitigation functions of ARI and FMCRD motor-driven run-in to shutdown the reactor. Additionally, DCD, Tier 2, Section 7.8.1, identifies the DPS reactor trip functions that provide a diverse means of reactor shut down. A subset of the RPS scram signals is selected for inclusion in the DPS scope, which provides acceptable diverse protection results. This set of diverse protection logics for reactor scram, combined with the ATWS mitigation features, other diverse backup scram protection, and diverse ESF functions, meets BTP HCIB-19.

The NRC staff evaluated whether the design bases identify the bounding events and the bases in the analyses that are presented or referenced in DCD, Tier 2, Chapter 15. The ATWS/SLC mitigation logic provides a diverse means of emergency shutdown using the SLC system for soluble boron injection. The shutdown functional performance requirements of the SLC system are bounded by the ATWS event performance requirements. ATWS performance requirements and characteristics are provided in DCD, Tier 2, Table 15-5. ARI, which hydraulically scrams the plant using the three sets of air header dump valves of the CRD system, is also used for ATWS mitigation. The ARI functionality is detailed in DCD, Tier 2, Section 7.7.2. DCD, Tier 2, Section 7.8.4, specifies the testing and inspection requirements. Periodic testing is performed on the ATWS/SLC and the DPS logics to verify proper operation of the DPS. Validation and testing for the DPS is detailed in DCD, Tier 1, ITAAC Table 2.2.14-4. The NRC staff finds the design basis consideration for the DPS to be adequately addressed. The NRC staff also finds that the design basis consideration related to 10 CFR 50.62 to be adequately addressed as described in Section 7.8.3.2 of this report.

(2) Quality of Components and Modules

The NRC staff evaluated whether the quality of the DPS components and modules conforms to Generic Letter (GL) 85-06 “Quality Assurance Guidance for ATWS Equipment That Is Not Safety-Related”. DCD, Tier 1, Sections 2.2.14 and 3.8 adequately address the EQ of the DPS safety components. However, the EQ of the non-safety components (ATWS/ARI) in the DPS were not addressed in DCD Revision 5 according to the acceptable guidance for the quality assurance of the DPS, which is included in GL 85-06. DCD, Tier 2, Section 7.8, describes the non-safety ATWS/ARI mitigation system and the DPS as part of the diverse I&C systems. SRP Section 7.8 states that GL 85-06 provides acceptable guidance for the quality assurance of the DPS components. Additionally, SRP Section 7.8 states that the applicant should identify the test, maintenance, surveillance, and calibration procedures and that these procedures should be consistent with the guidance of GL 85-06. DCD, Tier 2, Table 1.9-7, does not identify any differences with SRP Section 7.8. However, the DCD does not incorporate the guidance for the DPS quality, system testing, and surveillance provided in GL 85-06. While DCD, Tier 2, Table 3.2-1, includes for notes Component C-12, Item 10 and component C-41, Item 7 stating, “A quality assurance program that meets or exceeds the guidance of GL 85-06 is applied to all Non-Safety ATWS equipment,” no comparable note is provided for component C-72, the DPS. In RAI 7.8-8, the NRC staff requested the applicant to identify in the DCD how the applicant plans to address the EQ, quality assurance, and procedure guidance of GL 85-06 for the DPS. RAI 7.8-8 was being tracked as an open item in the SER with open items. In its response, the

applicant revised DCD, Tier 2, Table 3.11-1 to add systems and components associated with the DPS and to identify how the EQ program will be applied. In DCD, Tier 2, Section 7.8.3, the applicant specified that the guidance contained in GL 85-06 is applied to the DPS, which includes designing and developing software used in the DPS accordance with the requirements of NEDE-33226P and NEDE-33245P. The NRC staff determined the response was acceptable since the applicant has revised the DCD to properly address the quality assurance of the DPS in accordance with GL 85-06. Based on the applicant's response, RAI 7.8-8 is resolved. In DCD, Tier 2, Revision 6, the applicant added notes to component C-72, the DPS, on Table 3.2-1. The notes specified the requirements to comply with GL 85-06. The NRC staff finds the clarification acceptable.

(3) System Testing and Surveillance

The NRC staff evaluated whether the applicant identified test, maintenance, surveillance, and calibration procedures consistent with the guidance of GL 85-06. GL 85-06 states that measures are to be established to test, as appropriate, non-safety-related-ATWS equipment prior to installation and periodically. The NRC staff also evaluated whether the ATWS mitigation system should be testable at power (up to, but not necessarily including, the final actuation device). DCD, Tier 2, Section 7.8.4, specifies the DPS testing and inspection requirements. NEDE-33226P and NEDE-33245P identifies the factory tests that will be performed on I&C systems prior to installation, including the DPS. The technical specifications in DCD, Tier 2, Chapter 16 identify the periodic tests that are performed on the DPS logics for diverse actuation of safety systems to verify proper operation of the DPS, including channel checks, channel functional tests, channel calibrations, and logic system functional tests. The Availability Controls Manual in DCD, Tier 2, Chapter 19, Appendix A identifies the periodic tests that are performed on the ATWS/SLC and the DPS logics for diverse actuation of non-safety systems to verify proper operation of the DPS, including channel checks, channel functional tests, channel calibrations, and logic system functional tests. The staff find that these periodic tests conform to the guidance of GL85-06 since typical I&C tests and frequencies are identified for the DPS. In DCD, Tier 2, Sections 7.8.3.4 and 7.8.3.5 state that the design conforms to RGs 1.22 and 1.118 and BTP HICB-17 for self-test and surveillance test. The NRC staff finds the system testing and surveillance consideration for the DPS to be adequately addressed.

(4) Use of Digital Systems

The NRC staff evaluated whether IEEE Std 7-4.3.2, as endorsed by RG 1.152, has been adequately addressed for the DPS. SRP Appendix 7.1-D provides guidance on the implementation of IEEE Std 7-4.3.2 concerning the use of digital systems. In Section 7.1.1.3.10 of this report, the NRC staff evaluated in parallel IEEE Std 7-4.3.2 and IEEE Std 603 using the guidance in SRP Appendix 7.1-D. In RAI 7.1-99, Item D, the staff requested that the applicant include in the DAC/ITAAC the IEEE Std 7-4.3.2 criteria not already covered by DAC/ITAAC in DCD, Tier 1, Sections 2.2.15 or 3.2. RAI 7.1-99 was being tracked as an open item in the SER with open items. In its response, the applicant modified DCD, Tier 2, Section 7.1.6.6.1 to describe how IEEE Std 7-4.3.2 criteria are addressed by the IEEE Std. 603 criteria or by NEDE-33226P and NEDE-33245P. DCD, Tier 1, Section 2.2.15 was clarified to state that when the IEEE Std. 603 design criteria are applied to platforms relying on the use of software to perform their safety-related functions, additional criteria from IEEE Std. 7-4.3.2, which augments the IEEE Std. 603 criteria, also apply to the software projects as described under the applicable IEEE Std. 603 criterion. The DCD, Tier 1, Section 3.2 ITAAC for software were rewritten in DCD Revision 6 to refer to individual components of NEDE-33226P and NEDE-33245P. Since NEDE-33226P and NEDE-33245P include applicable IEEE Std 7-4.3.2 requirements, these are

addressed by the revised DCD, Tier 1, Section 3.2 ITAAC. The NRC staff determined the response was acceptable since the DCD was revised to describe how IEEE Std 7-4.3.2 criteria are addressed by the IEEE Std. 603 criteria or by NEDE-33226P and NEDE-33245P and the IEEE Std 7-4.3.2 criteria were included in the revised DAC/ITAAC in DCD, Tier 1, Sections 2.2.15 or 3.2. Based on the applicant's response and DCD changes, RAI 7.1-99, Item D is resolved.

In DCD Revision 6, Tier 2, Section 7.8.3.4, the applicant committed to comply with RG 1.152, that endorsed IEEE Std 7-4.3.2. In DCD, Tier 1, Section 2.2.14, the applicant documented detailed ITAAC requirements for the DPS. The NRC staff finds that the use of digital system concerns has been adequately addressed.

The software development activities are described in NEDE-33226P and NEDE-33245P. DCD, Tier 1, Section 3.2, includes the DAC/ITAAC to confirm that the completion of these activities and products conforms to the processes described in NEDE-33226P and NEDE-33245P and the guidelines of BTP HCIB-14. The NRC staff evaluation of software development activities is provided in Section 7.1.2 of this report.

(5) Power Supply Availability

The NRC staff evaluated whether power sources will be available during and following a loss of offsite power. DCD, Tier 2, Section 15.2.5.2 and Table 15.2-21, provide, details of a scenario involving loss of nonemergency ac power to station auxiliaries (abnormal operational occurrence). Loss of power generation buses produces a reactor trip (scram) signal. The event assumes normal function of the I&C and RPS. NEDO-33251, Appendix A, provides further analysis that assumes that the RPS fails to process trip signals. In this scenario, the DPS, which is available and powered from dc (battery) buses, still functions to shut down the reactor at RPV Level 3. The NRC staff finds that the DPS functionality demonstrates the versatility of the DPS in mitigating an alternating current power supply anomaly. Accordingly, the NRC staff finds the power supply availability consideration for the DPS to be adequately addressed.

(6) Environmental Qualification

The NRC staff evaluated whether the DPS equipment is qualified for the environment that could exist during the events for which the equipment is assumed to respond. The NRC staff reviewed DCD, Tier 2, Section 7.8.3, which stated that the guidance contained in the SRM on SECY-93-087, Item II.Q, BTP HICH-19, and GL 85-06, is applied to all diverse I&C systems and components described in this section. As discussed in section 7.8.3.1, Item (2) of this report, the NRC staff finds that the environmental qualification of the DPS has been adequately addressed. In DCD Revision 6, Tier 2, Section 7.8.3.4, the applicant incorporated the guidance of RG 1.89 and RG 1.209 into the harsh and mild environmental qualification programs, respectively. The harsh and mild environmental qualification programs are evaluated in Section 3.11 of this report. DCD, Tier 2, Table 3.11-1 identifies how DPS equipment is qualified. DCD, Tier 2, Section 7.8.3.4 identifies that conformance of the DPS equipment to RG 1.89 and RG 1.209 is through the qualification programs identified in DCD, Tier 2, Table 3.11-1. Based on the above, the NRC staff finds that the environmental qualification concern has been adequately addressed for the DPS.

(7) System Status

The NRC staff evaluated whether information related to the operation of the DPS is available in the MCR. DCD, Tier 2, Section 7.8.1.3, describes the manual controls and displays in the MCR for the systems operated by the DPS. These are in addition to safety-related controls and displays for the safety-related systems that are initiated by the DPS. The controls and displays for the safety-related systems comply with the applicable requirements of 10 CFR 50.34(f)(2)(v)(I.D.3) and the guidelines of RG 1.47, as discussed in Section 7.1.1.3.4 of this report. The N-DCIS includes controls and displays for non-safety-related systems initiated by the DPS.

Based on the information in DCD, Tier 2, Section 7.8, and the information discussed herein, the NRC staff finds that the system status indication and display has been adequately addressed in the design. Accordingly, the NRC staff finds the system status consideration for the DPS to be adequately addressed.

(8) Independence from the Protection Systems—IEEE Std 603, Sections 5.6 and 6.3

The NRC staff evaluated whether the DPS functions are independent and diverse from the RPS and ESFAS. The NRC staff also evaluated whether ATWS mitigation systems are diverse from the RPS. The RPS uses the RTIF-NMS platform, while the ESFAS uses the SSLC/ESF platform. The ATWS/SLC uses a safety ICP, while the DPS (non-safety) uses a platform diverse from and independent of the safety platforms. This ensures that digital safety and non-safety I&C systems are designed to minimize the potential for CCFs. The safety systems contain multiple redundant divisions to achieve high reliability. In accordance with IEEE Std 7-4.3.2, independence is provided between safety divisions and between safety and non-safety systems to ensure that random single failures do not result in CCF that may affect multiple safety divisions.

As detailed in DCD, Tier 2, Section 7.8.1.2.1, the DPS reactor trip functions provide a diverse means of reactor shutdown and serve as a backup to the RPS. This set of diverse protection logics for reactor scram, combined with the ATWS mitigation features, other diverse backup scram protection, and diverse ESF functions, provides the necessary diverse protections to meet the design requirements specified in the SRM on SECY-93-087 and BTP HICB-19. Further information on diversity is provide in the applicant's D3 assessment provided in NEDO-33251, which is evaluated in Section 7.1.3 of this report.

DCD, Tier 2, Section 7.8.3, provides a description of the DPS conformance with IEEE Std 603. The DPS logic does not communicate with the RPS logic, and the DPS failure modes do not prevent the RPS from performing a reactor trip. The DPS cannot cause the RPS to initiate a reactor trip prematurely. Credible DPS failure modes cannot prevent the SSLC/ESF actuation system from initiating ECCS functions and/or performing barrier isolation functions. Additionally, credible failure modes cannot result in premature operation of these protection systems. The ATWS/SLC logic is designed to mitigate a failure of the normal reactor trip system to function and is diverse from and independent of the RPS. The ATWS/SLC logic platform is designed as a safety system with four independent divisions. The ATWS/ARI function is provided from the non-safety DPS platform. Accordingly, the NRC staff finds the independence from the protection systems consideration for the DPS has been adequately addressed.

(9) Potential for Inadvertent Actuation

The NRC staff evaluated whether the DPS design limits the potential for inadvertent actuation and challenges to safety systems. The DPS is designed as a highly reliable non-safety system that meets the probabilistic risk assessment requirements to minimize failures on demand and to minimize inadvertent operation. Consistent with the guidance in IEEE Std 603, the non-safety DPS is designed to avoid adverse interaction with the protection systems with which the DPS interfaces. In DCD, Tier 2, Sections 7.8.1.2.1 and 7.8.1.2.2 provide descriptions of features in the DPS that minimize inadvertent actuations. Initiation logic for the DPS (for reactor scram and ESF functions) is "energize-to-actuate." System-level operational and functional defenses, as described in DCD, Tier 2, Section 7.8.2.2.1, include the following:

- asynchronous operation of multiple protection divisions. Timing signals are not exchanged among divisions;
- continuous cross-checking of redundant sensor inputs;
- automatic error checking on all multiplexed transmission paths;
- continuous self-test with alarm outputs in all system devices;
- automatic error detection (This permits early safe shutdown or bypass before common mode effects occur.);
- separation and independence requirements that protect against global effects resulting from such factors as EMI and thermal conditions

The NRC staff finds that the DPS incorporate sufficient features to prevent inadvertent system actuation and the potential for inadvertent actuation consideration for the DPS has been adequately addressed.

(10) Manual Initiation Capability

The NRC staff evaluated whether the ATWS mitigation systems and DPS include the capability for initiation from the MCR. In DCD, Tier 2, Sections 7.8.1.1 and 7.8.1.2 provide details of the manual initiation capability for ATWS/SLC, ATWS/ARI, and the DPS. Manual capability is also included to mitigate failure of an ATWS logic processor. A manual bypass switch for this function is provided in the MCR. Switches in the MCR are also used to manually inhibit the ADS under ATWS conditions.

As a backup for the RPS, the DPS also provides the ability to initiate a manual scram from either hardwired switches or the DPS VDU. Additionally, manual initiation capability is provided in the DPS logic circuitry to initiate the diverse ECCS functions of the GDCS, SLC system, ICS, and ADS (SRVs and DPVs). The DPS also provides the ability to generate diverse manual ECCS actuation from the DPS VDU. Accordingly, the NRC staff finds the manual initiation capability consideration for the DPS has been adequately addressed.

(11) Completion of Protective Action

The NRC staff evaluated whether the ATWS mitigation logic and DAS are designed such that, once initiated, the mitigation function will go to completion. DCD, Tier 2, Section 7.8.1.1.1.1, describes the ATWS/SLC mitigation processor logic controls, which provide isolated hardwired contact closure outputs to the SLC system on an initiation signal. Additionally, when an ATWS/ARI signal is received, the DPS generates an additional electrical signal to the RC&IS to initiate electrical insertion of all control rods. These actions are designed to ensure that mitigation functions for all AOOs (including ATWS) will go to completion. Accordingly, the NRC staff finds the completion of protective action consideration for the DPS to be adequately addressed.

(12) Diversity and Defense-in-Depth Analysis

The NRC staff evaluated whether the DPS functions credited with providing diversity are consistent with the assumptions of the applicant D3 analysis. The NRC staff reviewed LTR NEDO-33251 and compared major aspects of the report with the DPS overview in DCD, Tier 2, Section 7.8. In the D3 report, Section 2.6 includes descriptions of the I&C defense echelons and applications of the discrete I&C systems to each echelon. The DPS overview, defense echelons, CCF defenses, and system architecture match the descriptions of the DPS provided in DCD, Tier 2, Sections 7.8.1 and 7.8.2. The NRC staff finds that the DPS is consistent with the applicant's D3 LTR. Accordingly, the NRC staff finds the D3 analysis consideration for the DPS to be adequately addressed. Further information on diversity is provide in the applicant's D3 assessment provided in NEDO-33251, which is evaluated in Section 7.1.3 of this report.

7.8.3.2 Evaluation of Diverse Instrumentation and Control System Compliance with Regulations and the SRM on to SECY-93-087, Item II.Q

GDC 1 requires quality standards and maintenance of appropriate records. The NRC staff evaluated whether GDC 1 and 10 CFR 50.55a(a)(1) have been adequately addressed for the safety ATWS mitigation logic and the non-safety-related DPS per SRP Appendix 7.1-A. SRP Appendix 7.1-A states that the NRC staff review should confirm that the appropriate RGs and endorsed standards are identified as applicable for each I&C system important to safety. The NRC staff evaluation of conformance to RGs and standards for 10 CFR 50.55a(a)(1) and GDC 1 in Section 7.1.1.3.3 and 7.1.1.3.6 of this report is applicable to the safety ATWS mitigation logic. In Section 7.1.1.3.3 of this report, the NRC staff finds that the DCD has properly addressed compliance with the applicable RGs and standards for the safety systems including the ATWS mitigation systems. The In DCD, Tier 2, Sections 7.8.1 and 7.8.3.3, the applicant documented the conformance with SRM on Item II.Q of SECY 93-087. The NRC staff finds that 10 CFR 50.55a(a)(1) and GDC 1 for the ATWS mitigation logic has been adequately addressed.

In DCD Revision 6, Tier 2 Section 7.8.3.4, the applicant updated the documentation with respect to the conformance with the applicable RGs as listed in SRP Appendix 7.1-A. The NRC staff finds the clarification in DCD Section 7.8.3.4 acceptable. In Section 7.8.3.1, Item (2) of this report, the NRC staff finds that the DCD has properly addressed the quality of the DPS.

10 CFR 50.55a(h) requires compliance with IEEE Std 603-1991 and the correction sheet dated January 30, 1995. The NRC staff evaluated whether 10 CFR 50.55a(h) and IEEE Std 603 have been adequately addressed for the safety DPS. The NRC staff evaluation of IEEE Std 603 in

Section 7.1.1.3.10 of this report is applicable to the safety DPS. DCD, Tier 2, Section 7.8.1.1.1 states that a portion of the ATWS/SLC is implemented as safety. In Section 7.1.1.3.1 of this report, the NRC staff finds that the DCD has properly addressed IEEE Std 603 compliance that includes the DPS.

In DCD Revision 6, Tier 1, Section 2.2.15 (Table 2.2.15-1), the applicant added ATWS/SLC as an ICP in the IEEE Std 603 criterion applicability matrix. In DCD, Tier 2, Section 7.8.3.1, the applicant documented the cross reference to the related DCD sections that address conformance to the IEEE Std 603 criterion. Based on these updated information, the NRC staff finds that the requirements of 10 CFR 50.55a(h) and IEEE Std 603 have been adequately addressed.

GDC 2 requires design bases for protection against natural phenomena. GDC 4 requires environmental and dynamic effect design bases. The NRC staff evaluated whether GDC 2 and 4 has been adequately addressed for the safety ATWS/SLC mitigation logic. SRP Appendix 7.1-A states that GDC 2 and 4 apply to all I&C safety systems. SRP Appendix 7.1-A for GDC 2 states that the design bases for protection against natural phenomena for I&C systems important to safety should be provided for the I&C system. SRP Appendix 7.1-A for GDC 4 states that the environmental and dynamic effects (e.g., missiles) design bases for I&C systems important to safety should be provided for each system in Chapter 7 of the DCD. DCD, Tier 2, Section 7.8.1.1.1, states that a portion of the ATWS/SLC is implemented as safety. However, neither DCD, Tier 2, Table 7.1-1 nor Section 7.8.3.2 specify that GDC 2 and 4 are applicable to the safety-related ATWS/SLC mitigation logic. In RAI 7.1-99, Part G, the NRC staff requested the applicant to address the applicability of the GDC to the ATWS/SLC. RAI 7.1-99 was being tracked as an open item in the SER with open items. In its response, the applicant revised DCD, Tier 2, Table 7.1-1 and Section 7.8.3.2 to specify that GDC 2 and 4 are applicable to the safety-related ATWS/SLC mitigation logic. The NRC staff determined the response was acceptable since the applicant clarified that the ATWS/SLC Mitigation Logic conforms to GDC 2 and 4. Based on the applicant's response, RAIs 7.1-99 Item G is resolved.

DCD, Tier 2, Table 3.2-1, identifies that the safety SLC safety electrical modules and cables, which includes the ATWS/SLC mitigation logic, are designed as seismic Category I systems. In DCD, Tier 2, Sections 3.10 and 3.11 describe the EQ programs for safety electrical and digital I&C equipment, which are evaluated in Chapter 3 of this report. In DCD, Tier 1, Table 3.8-1, Items 1 and 3 include ITAAC for the applicant to verify the EQ of safety electrical and digital I&C equipment. The evaluation of GDC 2 and GDC 4 in Section 7.1.1.3.6 of this report further addresses these topics and is applicable to the ATWS/SLC mitigation logic. Accordingly, based on the applicant's identification of EQ programs consistent with the design bases for the ATWS/SLC mitigation logic and their verification in the ITAAC, the NRC staff finds that the requirements of GDC 2 and 4 have been adequately addressed for the safety-related ATWS/SLC mitigation logic.

GDC 24 requires that the protection system 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. GDC 24 requires that the interconnection of the protection and control systems be limited so as to assure that safety is not significantly impaired. The NRC staff evaluated whether GDC 24 has been adequately addressed for the DPS. Appendix 7.1-A to the SRP states that GDC 24 is addressed for safety systems by conformance to IEEE Std 603, Sections 5.1, 5.6, 5.12, 6.3, 6.6, and 8, particularly Sections 5.6

and 6.3. DCD, Tier 2, Table 7.1-1, identifies that GDC 24 applies to the DPS. DCD, Tier 2, Section 7.8, describes the conformance of the DPS to IEEE Std 603, Sections 5.6 and 6.3, which are evaluated Section 7.1.1.3.10 in this report. For the non-safety DPS, DCD, Tier 2, Sections 7.1.6.6.1.7 and 7.1.6.6.1.19, describes conformance with IEEE Std 603, Sections 5.6 and 6.3. These sections state that the Q-DCIS protection systems are separate and independent of the non-safety control systems, in accordance with GDC 24, and that any failure of non-safety systems does not affect safety protection systems or prevent them from performing their safety functions. Sections 5.6 and 6.3 of IEEE Std 603 are evaluated in Section 7.1.1.3.10 of this report. DCD, Tier 1, Table 2.2.15-2, includes the DAC/ITAAC for verifying that the applicable I&C systems design was completed in compliance with IEEE Std 603, including Sections 5.6 and 6.3. Accordingly, the NRC staff finds that the requirements of GDC 24 have been adequately addressed for the DPS.

The NRC staff evaluated whether GDC 13 and 19 have been adequately addressed for the DPS. GDC 13 requires providing instrumentation to monitor variables and systems over their anticipated ranges for normal operation, AOOs, and accident conditions to assure adequate safety. GDC 13 also requires providing appropriate controls to maintain these variables and systems within prescribed operating ranges. GDC 19 requires control room functionality, control room habitability, and remote shutdown capability. The evaluation of GDC 19 is provided in Section 7.1.1.3.6 of this report with the exception of support functions necessary for operating the reactor. SRP Section 7.8 identifies that GDC 13 and 19 are addressed by the review of the DPS status information, manual initiation capabilities, and control capabilities. DCD, Tier 2, Section 7.8.5, specify the status information of the safety ATWS mitigation logic. DCD, Tier 2. Section 7.8.1.1, specifies the automatic and manual initiation and control capabilities of the safety ATWS/SLC mitigation logic. DCD, Tier 2, Section 7.8.1.2, specifies the automatic initiation and controls of the DPS. DCD, Tier 2, Section 7.8.1.2, specifies the status information and manual initiation and control capabilities of the DPS. In combination with the following identified interrelated processes to complete the design of the monitoring capability and control room controls for the DPS, the NRC staff finds these monitoring capabilities and controls acceptable. NEDE-33226P and NEDE-33245P, as part of a software life cycle process, define a process by which plant performance requirements under various operational conditions will be specified, implemented, and tested. DCD, Tier 1, Section 3.2, includes the DAC/ITAAC for verifying that the software plans were developed and implemented consistent with this process and produce acceptable design outputs. DCD, Tier 1, Section 3.3, includes the DAC/ITAAC for implementing an HFE design process, which includes the design and verification of controls and information displays for monitoring variables and systems in the control room. These verifications are applicable to the DPS and include verifications of the controls for manual initiation and control of the DPS functions necessary to support actions to operate the nuclear power unit safely under normal conditions and to maintain it in a safe condition under accident conditions. Accordingly, based on the identified monitoring capabilities and control room controls, the defined processes for completing their design and their verification in the DAC/ITAAC, the NRC staff finds that the requirements of GDC 13 and 19 have been adequately addressed for the DPS.

The NRC staff evaluated whether 10 CFR 50.62 has been adequately addressed for the DPS. 10 CFR 50.62 requires that BWR plants have, (1) an ARI system that is diverse from the RPS and the ARI must be designed to perform its function in a reliable manner and be independent from the RPS [10 CFR 50.62(c)(3)], (2) an SLC system whose initiation must be automatic and which must be designed to perform its function in a reliable manner [10 CFR 50.62(c)(4)], and (3) an automatic recirculation pump trip (RPT) [10 CFR 50.62(c)(5)]. 10 CFR 50.62(c)(5) is not applicable to the ESBWR because the design does not have a recirculation pump. SRP

Table 7.1 identifies that 10 CFR 50.62 applies to the DPS (DCD Section 7.8). DCD, Tier 2, Table 7.1-1, identifies that 10 CFR 50.62 is applicable to the relevant safety and non-safety I&C systems.

For 10 CFR 50.62(c)(3), DCD, Tier 2, Section 7.8.1.1, describes the diverse ATWS mitigation logic which includes an ARI, SCRRI/SRI, and a diverse scram. DCD, Tier 2 Section 7.8.1, states that the ARI uses the three sets of air header dump valves of the CRD system to hydraulically scram the plant. DCD, Tier 2, Figure 4.6-8, shows that these valve are redundant to the scram air header dump valves. DCD, Tier 2, Section 7.8.1.1.2, states that the ARI logic resides in the DPS, which is separate and independent from the Q-DCIS with diverse hardware and software. The RPV pressure and level input sensors for the ARI logic are independent and separate from the sensors used in the Q-DCIS. Based on the above, the NRC staff finds that the diverse ATWS mitigation logic includes the ARI functions required by 10 CFR 50.62(c)(3).

For 10 CFR 50.62(c)(4), DCD, Tier 2, Section 7.8.1.1.1, describes the safety ATWS mitigation logic, which includes the automatic initiation of SLC boron injection and feedwater runback. DCD, Tier 2, Section 7.8.1.1.1, also states that the safety ATWS mitigation logic processors are separate and diverse from RPS circuitry and use discrete programmable logic devices for ATWS mitigation logic processing. DCD, Tier 2, Section 7.8.3, states that the safety ATWS mitigation logic is diverse from and independent of the RPS. Based on the above, the NRC staff finds that the safety ATWS mitigation logic includes the SLC functions required by 10 CFR 50.62(c)(4).

As noted above, 10 CFR 50.62(c)(5) requires an automatic RPT due to the BWR use of forced core flow circulation. Because the design uses natural circulation, there are no recirculation pumps to be tripped. The automatic FWRB feature is implemented to provide a reduction in water level, core flow, and reactor power, similar to the RPT in a forced circulation plant.

The NRC staff evaluated the design features that provide diversity of each ATWS mitigation logic from the RPS and its functioning a reliable manner. The design uses the FMCRD design with both hydraulic and electrical means to achieve shutdown. The use of this design eliminates the CCF potentials of the locking-piston CRD by eliminating the scram discharge volume, and by having an electrical motor run-in diverse from the hydraulic scram feature. This feature allows rod run-in, if scram air header pressure is not exhausted because of a postulated common cause electrical failure and simultaneous failure of the ARI system, and thus satisfies the intent of 10 CFR 50.62.

The ATWS mitigation functions use diverse control logics from the primary protection system. The safety portions of the ATWS mitigation logic, which provides an alternate means of emergency plant shutdown via soluble boron injection by the SLC system, uses independent logic controllers instead of a software-based platform.

DCD, Tier 2, Section 7.8.1, “System Description,” discusses CCF defenses. The DPS triple redundant design employs a different hardware and software platform from the primary protection system platforms (i.e., RTIF-NMS, ECCS/ESF, and ICP). The DPS is diverse from and independent of the primary protection systems. As part of the D3 evaluation, a review to assess a digital protection system CCF impact on events discussed in DCD, Tier 2, Chapter 15, has been performed. NEDO-33251 documents the coverage of the DPS with respect to the DCD, Tier 2, Chapter 15, events and discusses the backup functions provided by the DPS for mitigation of DCD, Tier 2, Chapter 15 events. Accordingly, the NRC staff finds that the ATWS mitigation design includes an appropriate set of functions. As described in Section 7.8.3.1,

Item (8) above, in this report, the NRC staff finds 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 HICB 7-11. Based on the above, the NRC staff finds that ATWS mitigation logic is acceptably diverse from the RPS and provides reasonable assurance of functioning in a reliable manner.

Based on the diverse ATWS mitigation logic including the ARI functions required by 10 CFR 50.62(c)(3), the safety ATWS mitigation logic including the SLC functions required by 10 CFR 50.62(c)(4), and both ATWS mitigation logics having acceptable diversity from the RPS and providing reasonable assurance of functioning in a reliable manner, the NRC staff finds that 10 CFR 50.62 has been adequately addressed for the DPS.

The NRC staff evaluated whether the guidelines of the SRM on SECY-93-087, Item II.Q, have been adequately addressed for the DPS. The SRM on SECY-93-087, Item II.Q, is evaluated in Section 7.1.1.3.7 of this report, which is applicable to the DPS. DCD, Tier 2, Table 7.1-1, identifies that the SRM on SECY-93-087, Item II.Q, applies to the DPS. NEDO-33251 provides the primary assessment of conformance to the guidelines of SRM to SECY-93-087, Item II.Q, along with BTP HCIB-19. The NRC staff evaluation of the D3 assessment is documented in Section 7.1.3 of this report, which finds that

- The applicant has analyzed each postulated CCF for each event that is evaluated in the accident analysis section of DCD Chapter 15, and the applicant has demonstrated adequate diversity within the DCIS design for each of these events.

- The proposed DPS has sufficient quality to perform the necessary function under the associated event conditions.

- A set of displays and controls located in the MCR can provide for manual system-level actuation of critical safety functions. The displays and controls are independent and diverse from the Q-DCIS.

The NRC staff evaluation of the I&C system in response to the SRM on SECY-93-087 is documented in Sections 7.1.1.3.7 and 7.1.3 of this report.

The NRC staff evaluated whether the requirements of 10 CFR 52.47(b)(1) have been adequately addressed. DCD, Tier 1, Section 2.2.14, contains the ITAAC that are necessary and sufficient to provide reasonable assurance that, if the ITA are performed and the acceptance criteria are met, a plant that references the design certification has been constructed and will operate in accordance with the design certification, the Atomic Energy Act, and the Commission's rules and regulations.

7.8.4 Conclusion

Based on the review of information in DCD, Tier 1, Sections 2.2.14 and 2.2.15, and DCD, Tier 2, Section 7.8, and NEDO-33251, the NRC staff concludes that the DPS design meets the applicable regulatory requirements of 10 CFR 50.55a(a)(1), 10 CFR 50.55a(h), GDC 1, 13, 19, and 24, 10 CFR 52.47(b)(1), 10 CFR 50.62, and the SRM on SECY-93-087.

7.9 COL Action Items Identified as Unresolved

No unresolved COL action items have been identified.